kaspersky

Kaspersky Industrial CyberSecurity for Nodes

Подготовительные процедуры и руководство по сертификации

Версия программы: 3.2.0.273

kaspersky

Уважаемый пользователь!

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

Дата редакции документа: 06.12.2023

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

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

kaspersky

Содержание

kaspersky

Об этом документе

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

Подготовительные процедуры изложены в разделах "Подготовка к установке приложения", "Установка приложения", "Подготовка приложения к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

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

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Industrial CyberSecurity for Nodes, а также поддержка организаций, использующих Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

О Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes – средство антивирусной защиты и средство контроля подключения съемных машинных носителей информации, 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;
- контроль подключения съемных машинных носителей информации.

В сертифицированной версии программы не поддерживаются следующие функции:

- защита от сетевых угроз.

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

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

- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование внешних устройств в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время

обмена файлами с подключаемым по USB флеш-накопителем или внешним устройством другого типа.

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

Работа компонентов контроля основана на правилах:

- Контроль запуска программ использует правила контроля запуска программ.
- Контроль устройств использует правила доступа к устройствам и правила доступа к шинам подключения.
- Функция проверки целостности проектов ПЛК использует правила проверки целостности проектов ПЛК.

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

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

- **Постоянная защита файлов**. Компонент позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте Kaspersky Industrial CyberSecurity for Nodes, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках. Постоянная защита файлов перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.
- **Контроль Wi-Fi**. Компонент отслеживает попытки подключения защищаемого компьютера к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям.
- **Управление сетевым экраном**. Этот компонент обеспечивает возможность управления брандмауэром Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует возможность настройки параметров сетевого экрана извне.
- **Защита от шифрования**. Компонент позволяет обнаруживать активность вредоносного шифрования сетевых файловых ресурсов защищаемого компьютера со стороны удаленных компьютеров корпоративной сети.
- **Портативный сканер**. Этот компонент исследует изолированные устройства и проводит проверки состояния безопасности.
- **Мониторинг файловых операций**. Kaspersky Industrial CyberSecurity for Nodes обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения указывают на нарушение безопасности на защищаемом компьютере.
- **Мониторинг доступа к реестру**. Компонент позволяет отслеживать действия, выполняемые с указанными ветвями и ключами реестра в областях мониторинга, заданных в параметрах задачи.
- **Анализ журналов**. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

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

Чтобы поддерживать Kaspersky Industrial CyberSecurity for Nodes в актуальном состоянии, требуется обновление баз и модулей программы, используемых в работе программы. По умолчанию программа

обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули программы.

Для защиты компьютеров используются следующие задачи:

- **Полная проверка**. Kaspersky Industrial CyberSecurity for Nodes выполняет тщательную проверку операционной системы, включая системную память, объекты, загружаемые при старте операционной системы, резервное хранилище операционной системы, а также все жесткие и съемные диски.
- **Выборочная проверка**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, выбранные пользователем.
- **Проверка важных областей**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, загрузка которых осуществляется при запуске операционной системы, системную память и объекты, которые могут быть заражены руткитами.
- **Обновление**. Kaspersky Industrial CyberSecurity for Nodes загружает обновленные базы и модули программы. Обновление обеспечивает актуальность защиты компьютера от вирусов и других программ, представляющих угрозу.

Удаленное управление через Kaspersky Security Center

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

Служебные функции программы

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

- **Журналы**. В процессе работы программы для каждого компонента и задачи программы формируется отчет. Отчет содержит список событий, произошедших во время работы Kaspersky Industrial CyberSecurity for Nodes, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.
- **Хранилища**. Если в ходе проверки компьютера на вирусы и другие программы, представляющие угрозу, программа обнаруживает зараженные или возможно зараженные файлы, она блокирует эти файлы. Kaspersky Industrial CyberSecurity for Nodes перемещает возможно зараженные файлы в карантин – специальное хранилище. Копии вылеченных и удаленных файлов Kaspersky Industrial CyberSecurity for Nodes сохраняет в резервном хранилище. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Industrial CyberSecurity for Nodes помещает в список необработанных файлов.Вы можете проверять файлы, восстанавливать файлы в папку их исходного размещения, самостоятельно помещать файлы на карантин, а также очищать хранилище данных.
- **Уведомления**. Служба уведомлений позволяет пользователю быть в курсе событий о текущем состоянии защиты компьютера и о работе Kaspersky Industrial CyberSecurity for Nodes. Уведомления могут отображаться на экране или доставляться по электронной почте.
- **Kaspersky Security Network**. Участие пользователя в Kaspersky Security Network (KSN) позволяет повысить эффективность защиты компьютера за счет оперативного получения информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.
- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

- **Список заблокированных сетевых сеансов**. Вы можете заблокировать сетевые сеансы, пытающиеся получить доступ к общим сетевым папкам компьютера, при обнаружении вредоносной активности с их стороны.
- **Доверенная зона**. Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Industrial CyberSecurity for Nodes будет применять по умолчанию в задачах проверки по требованию и постоянной защиты файлов и в других задачах, если вы укажете их в параметрах исключений.
- **Поддержка**. Все зарегистрированные пользователи Kaspersky Industrial CyberSecurity for Nodes получают доступ к обновлению баз данных и модулей программы, а также к консультациям специалистов Службы технической поддержки "Лаборатории Касперского" по электронной почте по вопросам, связанным с установкой, настройкой и использованием программы.

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы приложения, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Перед установкой Kaspersky Industrial CyberSecurity for Nodes необходимо удалить с устройства другие антивирусные программы, чтобы избежать возможных конфликтов между программами.

Программные требования к защищаемым устройствам

Настольные операционные системы:

- Windows XP Professional SP2 32-разрядная / 64-разрядная.
- Windows XP Professional SP3 32-разрядная.
- Windows Vista® SP2 32-разрядная / 64-разрядная.
- Windows 7 SP1 Professional / Enterprise / Ultimate 32-разрядная / 64-разрядная.
- Windows 8 Professional / Enterprise 32-разрядная/ 64-разрядная.
- Windows 8.1 Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2015 версии 1507 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2016 версии 1607 32-разрядная / 64-разрядная.
- Windows 10 RS4 версии 1803 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS5 версии 1809 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2019 версии 1809 32-разрядная / 64-разрядная.
- Windows 10 19H1 версии 1903 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H1 версии 2004 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H2 версии 2009 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H1 версии 21H1 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H2 версии 21H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 22H2 версии 22H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.

- Windows 10 LTSC 2021 версии 21H2 32-разрядная / 64-разрядная.
- Windows 11 21H2 версии 21H2 Home / Pro / Education / Enterprise 64-разрядная.
- Windows 11 22H2 версии 22H2 Home / Pro / Education / Enterprise 64-разрядная.

Серверные операционные системы:

- Windows Server 2003 SP1 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2003 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2003 R2 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2008 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2008 R2 SP1 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2012 Foundation / Standard / Essentials / Datacenter 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Essentials / Datacenter 64-разрядная.
- Windows Server 2016 версии 1709 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2016 версии 1803 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 версии 1809 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 версии 1903 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 версии 1909 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 версии 2004 Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2019 версии 20H2 Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2022 версии 21H2 Standard / Datacenter 64-разрядная.

Встраиваемые системы:

- Windows XP Embedded SP2 WEPOS 32-разрядная / 64-разрядная.
- Windows XP Embedded SP3 POS Ready 2009 32-разрядная.
- Windows 7 Embedded SP1 POS Ready 32-разрядная / 64-разрядная.
- Windows 8.0 Embedded Industry Pro 32-разрядная / 64-разрядная.
- Windows 8.1 Embedded Industry Pro 32-разрядная / 64-разрядная.
- Windows 10 версии 1803 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 версии 1809 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 версии 1903 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 версии 21H1 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 версии 21H2 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 версии 22H2 IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 11 версии 21H2 IoT Enterprise 64-разрядная.
- Windows 11версии 22H2 IoT Enterprise 64-разрядная.

kaspersky

Аппаратные требования к защищаемым устройствам

Таблица 1. Аппаратные требования к защищаемым устройствам

Тип ОС	Наименование ОС	Минимальные требования	Рекомендованные требования
Для рабочих станций	Windows 7 / 8 x86 Windows XP x86/ x64	• Процессор: 1.4 ГГц одноядерный не ниже Pentium IV (x64). • Оперативная память: 512 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows 7 / 8 / 10 / 11 x64	• Процессор: 1.4 ГГц одноядерный не ниже Pentium IV (x64). • Оперативная память: 1 ГБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
Для серверов	Windows Server 2003 x86/x64 Windows Server 2008 x86	• Процессор: 1.4 ГГц одноядерный не ниже Pentium IV (x64). • Оперативная память: 512 МБ. • Объем свободного места на диске: 4 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64	• Процессор: 1.4 ГГц одноядерный. • Оперативная память: 1 ГБ. • Объем свободного места на диске: 4 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4ГБ.
Встраиваемые	Windows Embedded XP Windows Embedded POSReady 2009	• Процессор: 1.4 ГГц одноядерный не ниже Pentium IV (x64). • Оперативная память: 512 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4ГБ.
	Windows Embedded 7 / 8	• Процессор: 1.4 ГГц одноядерный не ниже Pentium IV (x64). • Оперативная память: 1 ГБ. • Объем свободного места на диске: 2 ГБ	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4ГБ.

В случае установки на это же устройство программы Kaspersky Endpoint Agent потребуется дополнительное пространство:

- Оперативная память: 50 МБ.
- Место на жестком диске: 250 МБ.

Поддерживаемые индустриальные системы

Kaspersky Industrial CyberSecurity for Nodes 3.2 защищает следующие программируемые логические контроллеры:

- SIMATIC™ S7-300 (Siemens™);
- SIMATIC S7-400 (Siemens);
- SIMATIC S7-400H в режиме работы с резервированием (Siemens);
- Schneider Electric Modicon M340;
- Schneider Electric Modicon M580;
- устройства на базе CODESYS V3;
- ОВЕН ПЛК210;
- Fastwel CPM723-01;
- Прософт-Системы Regul R500;
- Siemens SIMATIC S7-1500;
- Siemens SIMATIC S7-1200;
- Siemens серии SIPROTEC 4.

Ограничение функциональности в устаревших версиях Windows

- В Windows XP версии SP2 невозможно заблокировать удаленные устройства и настроить параметры списка заблокированных сетевых сеансов. В этой версии Windows параметр **Блокировать доступ к общим сетевым ресурсам для сетевых сеансов, проявляющих вредоносную активность** неактивен.
- При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Industrial CyberSecurity for Nodes на устройства под управлением Windows XP или Windows Server 2003 необходимо использовать исполняемый файл setup.exe из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.
- Для управления программой Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center на компьютере под управлением Windows XP или Windows Server 2003 необходимо использовать Агент администрирования Kaspersky Security Center (klnagent) версии 10.5.

Аппаратные и программные требования для Kaspersky Security Gateway

Общие аппаратные и программные требования:

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

Настольные операционные системы:

- Windows Vista SP 2 32-разрядная / 64-разрядная.
- Windows 7 Professional 32-разрядная / 64-разрядная.
- Windows 7 Enterprise / Ultimate 32-разрядная / 64-разрядная.
- Windows 7 Professional SP1 и выше 32-разрядная / 64-разрядная.
- Windows 7 Enterprise / Ultimate SP1 и выше 32-разрядная / 64-разрядная.
- Windows 8 Pro 32-разрядная / 64-разрядная.
- Windows 8 Enterprise 32-разрядная / 64-разрядная.
- Windows 8,1 Pro 32-разрядная / 64-разрядная.
- Windows 8,1 Enterprise 32-разрядная / 64-разрядная.
- Windows 10 Pro 32-разрядная / 64-разрядная.
- Windows 10 Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS1/RS2/RS3/RS4.

Серверные операционные системы:

- Windows Server 2008 Standard SP1 и выше.
- Windows Server 2008 Enterprise SP1 и выше.
- Windows Server 2008 R2 Standard.
- Windows Server 2008 R2 Enterprise.
- Windows Server 2008 R2 Standard SP1.
- Windows Server 2008 R2 Enterprise SP1.
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter 64-разрядная.
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter 64-разрядная.
- Windows Server 2016.

Функциональные требования и ограничения

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

В этом разделе

kaspersky

Установка программы

Ниже приведен список ограничений при установке программы:

- Для корректной работы Kaspersky Industrial CyberSecurity for Nodes в Windows требуется поддержка SHA-2.
- При установке программы на экране может появиться предупреждение, если указанный путь к папке установки Kaspersky Industrial CyberSecurity for Nodes содержит более 150 символов. Это предупреждение не влияет на процесс установки: вы можете установить и запустить Kaspersky Industrial CyberSecurity for Nodes.
- Если вы хотите установить компонент поддержки протокола SNMP, перезапустите службу SNMP, если она запущена.
- Если вы хотите установить и запустить Kaspersky Industrial CyberSecurity for Nodes на устройстве со встроенной операционной системой, установите компонент Диспетчер фильтров.
- Установка Средств администрирования Kaspersky Industrial CyberSecurity for Nodes невозможна средствами групповых политик Microsoft Active Directory®.
- Если исключить узел Антивирусная защита из списка устанавливаемых компонентов программы, он исчезнет из списка доступных компонентов после завершения установки. Для установки компонентов узла Антивирусная защита запустите мастер установки из инсталляционного пакета, поскольку инсталляционный пакет содержит полный список компонентов.
- Если установлена Консоль администрирования Kaspersky Industrial CyberSecurity for Nodes, мастер установки может предложить перезагрузить компьютер. В этом случае перезагрузка не обязательна. Достаточно завершить сеанс пользователя, установившего Консоль администрирования, и повторно выполнить вход в систему.
- При установке программы на устройства с устаревшей версией операционной системы, для которой невозможно регулярное получение обновлений, нужно проверить следующие корневые сертификаты:
  - DigiCert Assured ID Root CA
  - DigiCert_High_Assurance_EV_Root_CA
  - DigiCertAssuredIDRootCA

  Если указанные корневые сертификаты не установлены, программа может работать некорректно. Рекомендуется установить сертификаты как можно скорее.

Мониторинг файловых операций

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

Следующие папки и файлы исключены из области мониторинга:

- Служебные файлы NTFS с идентификатором файла от 0 до 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\

- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

Программа исключает папки верхнего уровня.

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

Управление сетевым экраном

Ниже приведен список ограничений при управлении сетевым экраном:

- Требуется указать несколько адресов. В противном случае невозможна работа с IPv6.
- Текущие правила политики сетевого экрана поддерживают основные сценарии взаимодействия между защищаемыми устройствами и Сервером администрирования. Для использования функций Kaspersky Security Center в полном объеме необходимо настроить правила для портов. Информация о номерах портов, протоколах и их функциях приведена в Базе знаний Kaspersky Security Center.
- После установки программы и настройки правил для задачи программа контролирует изменение правил и групп правил брандмауэра Windows, когда задача Управление сетевым экраном запущена. Чтобы обновить статус и добавить необходимые правила, перезапустите задачу Управление сетевым экраном.
- При запуске задачи Управление межсетевым экраном запрещающие правила и правила, контролирующие исходящий трафик, автоматически удаляются из параметров сетевого экрана операционной системы.

kaspersky

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Должна быть обеспечена возможность периодического контроля целостности ПО программы и БД ПКВ.
16. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
17. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

kaspersky

Типовые схемы развертывания

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

Решение Kaspersky Industrial CyberSecurity включает следующие утилиты и программы:

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

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

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

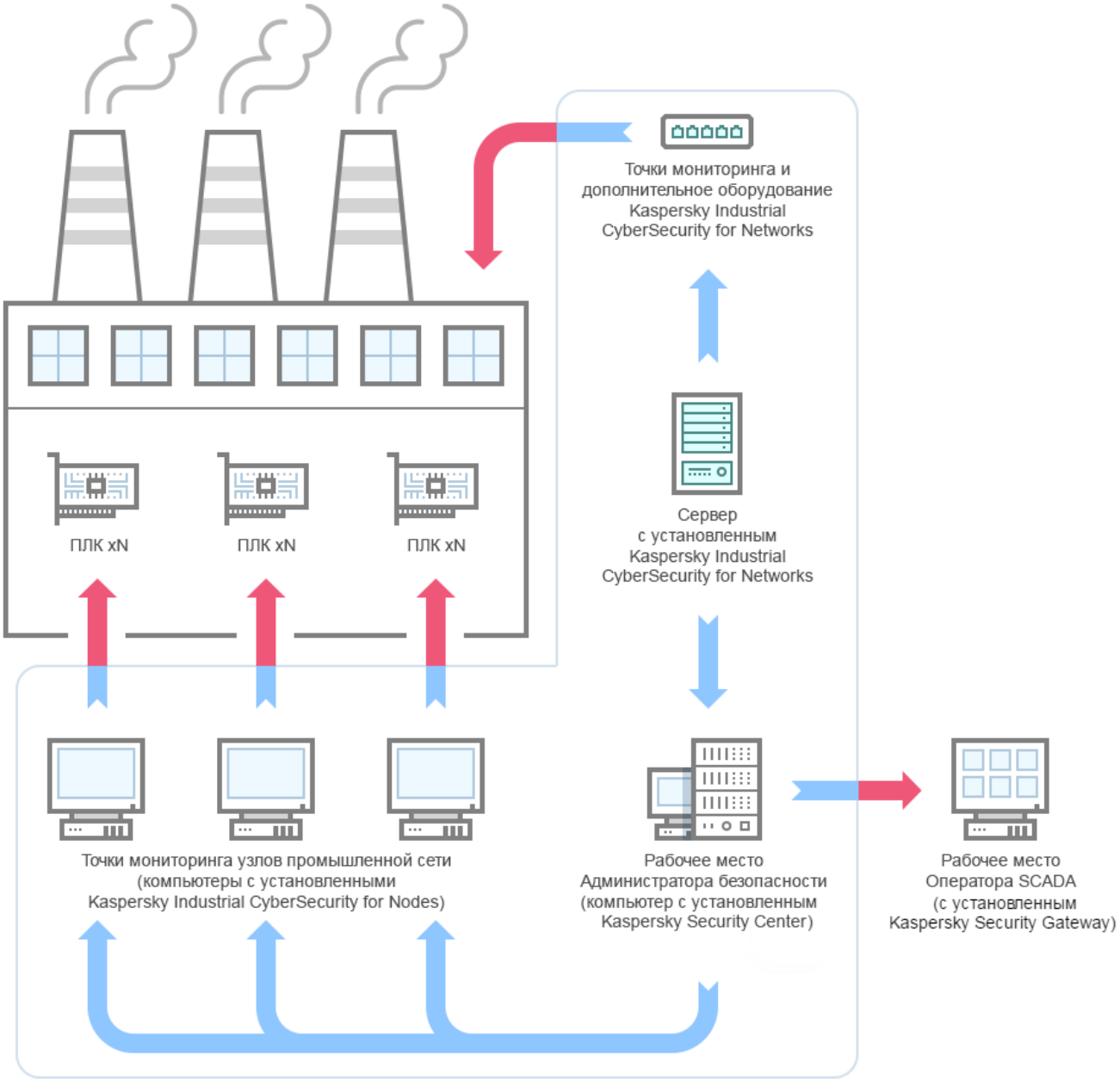
Вы можете управлять программами Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes, развернутыми в одной выделенной сети, с помощью единой Консоли администрирования Kaspersky Security Center. Вы также можете настроить передачу диагностических данных, полученных от программ Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes, из Kaspersky Security Center в систему SCADA с помощью программы Kaspersky Security Gateway (см. раздел "Использование Kaspersky Security Gateway" на стр. 873).

Kaspersky Industrial CyberSecurity for Nodes включает:

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

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

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


Точки мониторинга и
дополнительное оборудование
Kaspersky Industrial
CyberSecurity for Networks
Сервер
с установленным
Kaspersky Industrial
CyberSecurity for Networks
ПЛК xN
ПЛК xN
ПЛК xN
Точки мониторинга узлов промышленной сети
(компьютеры с установленными
Kaspersky Industrial CyberSecurity for Nodes)
Рабочее место
Администратора безопасности
(компьютер с установленным
Kaspersky Security Center)
Рабочее место
Оператора SCADA
(с установленным
Kaspersky Security Gateway)

kaspersky

Kaspersky Endpoint Agent

Использование компонента возможно только при наличии соответствующей лицензии.

Kaspersky Endpoint Agent можно установить на отдельные устройства в ИТ-инфраструктуре организации. Программа осуществляет постоянный контроль процессов, запущенных на этих устройствах, открытых сетевых соединений и изменяемых файлов. Kaspersky Endpoint Agent поддерживает взаимодействие со следующими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, целевых атак):

- Kaspersky Endpoint Detection and Response Optimum (поддерживает Kaspersky Endpoint Agent 3.9 и выше).

  Взаимодействие осуществляется при наличии соответствующей лицензии.

- Kaspersky Anti Targeted Attack Platform (поддерживает Kaspersky Endpoint Agent 3.8 и выше).

  Взаимодействие осуществляется в рамках Kaspersky Anti Targeted Attack Platform при наличии соответствующей лицензии.

- Kaspersky Sandbox (поддерживает Kaspersky Endpoint Agent 3.7 и выше).

  Взаимодействие осуществляется в рамках Kaspersky Anti Targeted Attack Platform при наличии соответствующей лицензии.

Kaspersky CyberSecurity for Nodes поддерживает Kaspersky Endpoint Agent версии 3.11 и выше.

Перед установкой Kaspersky Endpoint Agent на устройства с операционной системой Windows XP следует провести пилотное тестирование, чтобы исключить риски, которые могут повлиять на работу критически важных программ.

Вы можете запросить указанные версии этих программ у менеджера по технической поддержке (TAM).

kaspersky

В этом разделе

Программные и аппаратные требования

Программные требования к защищаемым компьютерам

Перед установкой программы требуется выключить использование TLS 1.0 и TLS 1.1 в операционной системе. О том, как это сделать, читайте в статье.

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 SP1 Home / Professional / Enterprise / Ultimate 32-разрядная / 64-разрядная.
- Windows 8.1.1 Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS3 (версия 1703) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS4 (версия 1803) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.

- Windows 10 RS5 (версия 1809) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1809, LTSC 2019) 32-разрядная / 64-разрядная.
- Windows 10 19H1 (версия 1903) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 19H2 (версия 1909) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H1 (версия 2004) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H2 (версия 2009) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 21H1) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 21H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H2 (версия LTSC 2021) 32-разрядная / 64-разрядная.
- Windows 10 (версия 22H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 11 (версия 21H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 11 (версия 22H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.

Поддерживаемые серверные операционные системы:

- Windows Server 2008 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2016 (версия 1709) Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2016 (версия 1803) Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 (версия 1809) Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 (версия 1903) Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2019 (версия 1909) Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2019 (версия 2004) Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2019 (версия 20H2) Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2022 (версия 21H2) Standard / Datacenter 64-разрядная.

Поддерживаемые встраиваемые операционные системы:

- Windows 7 SP1 Embedded (POSReady 7) 32-разрядная / 64-разрядная.
- Windows 10 (версия 1703) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1803) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1809) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1903) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1909) IoT Enterprise 32-разрядная / 64-разрядная.

- Windows 10 (версия 2004) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 2009) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 21H1) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 21H2) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 22H2) IoT Enterprise 32-разрядная / 64-разрядная.
- Windows 11 (версия 21H2) IoT Enterprise 64-разрядная.
- Windows 11 (версия 22H2) IoT Enterprise 64-разрядная.

Следующие операционные системы поддерживаются только для сценариев интеграции с Kaspersky Industrial CyberSecurity for Networks:

- Windows XP SP2 Professional 32-разрядная / 64-разрядная.
- Windows XP SP3 Professional 32-разрядная.
- Windows Vista SP2 32-разрядная / 64-разрядная.
- Windows 8.0 Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 (версия 1507, LTSC 2015) 32-разрядная / 64-разрядная.
- Windows 10 (версия 1607, LTSC 2016) 32-разрядная / 64-разрядная.
- Windows Server 2003 SP2 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2003 SP3 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2003 R2 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2012 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows XP Embedded SP2 (WEPOS) 32-разрядная / 64-разрядная.
- Windows XP Embedded SP3 (POSReady 2009) 32-разрядная.
- Windows Embedded 8.0 Industry Pro 32-разрядная / 64-разрядная.
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная.

Следующие операционные системы поддерживаются только для сценариев интеграции с Kaspersky Anti Targeted Attack Platform и сценариев интеграции с Kaspersky Endpoint Detection and Response Optimum:

- Windows 11 (версия 23H2) Home / Professional / Education / Enterprise 64-разрядная.
- Windows 11 (версия 23H2) IoT Enterprise 64-разрядная.

kaspersky

Аппаратные требования к защищаемым компьютерам

Таблица 2. Аппаратные требования к компьютерам для установки Kaspersky Endpoint Agent

Тип ОС	Наименование ОС	Минимальные требования	Рекомендованные требования
Для рабочих станций, встраиваемые ОС	Windows 7 / 8 x86	• Процессор: 1.4 ГГц (одноядерный). • Оперативная память: 1 ГБ. • Объем свободного места на диске: 500 МБ.	• Процессор: 2.4 ГГц (четырехъядерный). • Оперативная память: 2 ГБ. • Объем свободного места на диске: 1 ГБ.
	Windows 7 / 8 / 10 x64 Windows XP x86	• Процессор: 1.4 ГГц (одноядерный). • Оперативная память: 1 ГБ. • Объем свободного места на диске: 500 МБ.	• Процессор: 2.4 ГГц (четырехъядерный). • Оперативная память: 4 ГБ. • Объем свободного места на диске: 1 ГБ.
	Windows 11 x64	• Процессор: 1 ГГц (двухъядерный). • Оперативная память: 4 ГБ. • Объем свободного места на диске: 500 МБ.	• Процессор: 2.4 ГГц (четырехъядерный). • Оперативная память: 8 ГБ. • Объем свободного места на диске: 1 ГБ.
Для серверов	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64	• Процессор: 1.4 ГГц (одноядерный). • Оперативная память: 512 МБ. • Объем свободного места на диске: 500 МБ.	• Процессор: 2.4 ГГц (четырехъядерный). • Оперативная память: 2 ГБ. • Объем свободного места на диске: 1 ГБ.
	Windows Server 2022 x64	• Процессор: 1.4 ГГц (одноядерный). • Оперативная память: 2 ГБ. • Объем свободного места на диске: 500 МБ.	• Процессор: 2.4 ГГц (четырехъядерный). • Оперативная память: 4 ГБ. • Объем свободного места на диске: 1 ГБ.

Ограничения для сценариев интеграции с Kaspersky Endpoint Detection and Response Optimum

Интеграция с Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Detection and Response Optimum доступна в рамках указанных приложений при наличии соответствующей лицензии.

- Если установлен Агент администрирования Kaspersky Security Center (klnagent) версии 10.5 и выше, но ниже версии 12.1, сценарии интеграции с Kaspersky Endpoint Detection and Response Optimum поддерживаются со следующими ограничениями:
  - Информация о цепочке развития угрозы в сетевой список не передается.
  - Информация о результатах выполнения задач не передается в Kaspersky Security Center.
- Если установлен klnagent версии 12.1 и выше, все сценарии интеграции с Kaspersky Endpoint Detection and Response Optimum поддерживаются без ограничений.
- Для управления программой Kaspersky Endpoint Agent с помощью Kaspersky Security Center Web Console требуется один из браузеров:
  - Google Chrome для Windows;
  - Mozilla Firefox для Windows;
  - Google Chrome для Linux;
  - Mozilla Firefox для Linux.
- В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции:
  - загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения);
  - функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения);
  - обнаружение уязвимостей программ сторонних производителей (при использовании Системного администрирования).

Совместимость программы Kaspersky Endpoint Agent 3.16 с предыдущими версиями Kaspersky Endpoint Agent

Если на устройстве установлен и используется Endpoint Sensor версии 3.6.X в составе Kaspersky Endpoint Security, необходимо отключить Endpoint Sensor перед установкой Kaspersky Endpoint Agent во избежание возможных конфликтов между программами.

Доступна установка программы Kaspersky Endpoint Agent 3.16 на устройство с программой Endpoint Sensor версии 3.5 и ниже, установленной в составе Kaspersky Endpoint Security. Программы работают независимо и без конфликтов.

Обновление Kaspersky Endpoint Agent возможно для версий программы, установленных в составе программ Endpoint Protection Platform и установленных отдельно. Обновление Kaspersky Endpoint Agent, установленной отдельно, доступно только для версий 3.8 и выше. Обновление выполняется путем установки новой версии.

Интеграция программы Kaspersky Endpoint Agent 3.16 с другими программами и решениями "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.16 поддерживает интеграцию со следующими программами и решениями «Лаборатории Касперского»:

- Kaspersky Security Center версий 13.2, 14, 14.2.
- Kaspersky Security Center Cloud Console.

В сертифицированной версии программы использование Kaspersky Security Center Cloud Console приводит к выходу программы из безопасного состояния.

- Kaspersky Sandbox 2.0.

  Взаимодействие осуществляется в рамках Kaspersky Anti Targeted Attack Platform при наличии соответствующей лицензии.

- Kaspersky Anti Targeted Attack Platform 5.1.

  Взаимодействие осуществляется в рамках Kaspersky Anti Targeted Attack Platform при наличии соответствующей лицензии.

- Kaspersky Endpoint Detection and Response Optimum 1.1.

  Взаимодействие осуществляется при наличии соответствующей лицензии.

Ограничения Kaspersky Endpoint Agent 3.16

В Kaspersky Endpoint Agent 3.16 известны следующие ограничения.

Ограничения установки:

- Для корректной работы Kaspersky Endpoint Agent необходима поддержка SHA-2 в Windows. При попытке установки на операционную систему без поддержки SHA-2 появится предупреждение об отсутствии поддержки, и дальнейшая установка будет невозможна.
- При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.
- В Kaspersky Security Center версии 13.2 и выше для установки Kaspersky Endpoint Agent на компьютеры под управлением Windows XP необходимо использовать стандартный дистрибутив Kaspersky Endpoint Agent 3.16, а не инсталляционный пакет, созданный в Kaspersky Security Center.
- Установщик не может остановить службу soyuz до тех пор, пока не завершится инициализация службы. Например, установщик возвращает ошибку "Неверный пароль" при попытке удалить или изменить конфигурацию программы сразу после завершения установки, так как служба soyuz не завершила инициализацию и не может быть остановлена.
- Невозможно восстановить или удалить Kaspersky Endpoint Agent с устройства, если нарушена целостность модуля agent.exe (утилита командной строки Kaspersky Endpoint Agent).
- Невозможно запустить Установщик Kaspersky Endpoint Agent на устройстве с операционной системой, к которой применяется активная политика CodeIntegrity.
- После установки, восстановления или удаления Kaspersky Endpoint Agent, рекомендуется выполнить перезагрузку ОС в ближайшее доступное время. Это необходимо, потому что часть настроек программы может быть завершена только в момент запуска операционной системы.

- При попытке запуска Установщика Kaspersky Endpoint Agent с правами учетной записи пользователя, в имени которого содержатся китайские иероглифы, работа Установщика завершается ошибкой. Рекомендуется выполнять установку программы с правами учетной записи Local System, например, запускать установку средствами Kaspersky Security Center.
- В Kaspersky Endpoint Agent реализована функция запуска и исполнения службы Kaspersky Endpoint Agent (soyuz.exe) с признаком PPL (Protected Process Light). Эта функция обеспечивается драйвером klelaml.sys. Нарушение целостности драйвера klelaml.sys приводит к сбою при загрузке операционной системы. В этом случае рекомендуется использовать системные утилиты восстановления Windows. Отсутствие драйвера klelaml.sys при включенном признаке PPL для процесса soyuz.exe не приводит к сбою операционной системы, но вызывает аварийное завершение Kaspersky Endpoint Agent. В этом случае рекомендуется запустить Установщик программы для выполнения восстановления в тихом режиме с ключом REINSTALL=Drivers.klelam.
- В свойствах программы Kaspersky Endpoint Agent в Консоли администрирования (в разделе **Общие**) данные о статусе установки программы отображаются некорректно.
- Если операционная система активирована по корпоративной лицензии (Volume License), то после установки Kaspersky Endpoint Agent из-за установки сетевых драйверов программы может потребоваться повторная активация операционной системы.
- При удалении или обновлении Kaspersky Endpoint Agent с установленным драйвером сниффера L2 возможны разрывы сетевых соединений.

Функциональные ограничения:

- Компонент запрета открытия документов не запрещает открытие документа, подпадающего под критерии применяющегося правила, если документ открыт с использованием OLE-автоматизации.
- Если при настройке параметров исключения из сетевой изоляции для критерия "Приложение" указано больше одной программы, Kaspersky Endpoint Agent разрешит подключение только для первой программы из списка. Сетевые подключения для остальных указанных программ будут проигнорированы. Ограничение воспроизводится при изоляции устройств, работающих под управлением операционных систем Windows 7 и Windows Server 2008 R2.
- Для объектов, помещенных на карантин программой Kaspersky Endpoint Agent, не поддерживается отправка на анализ в "Лабораторию Касперского" из карантина Kaspersky Security Center.
- В секциях параметров для управления доступом на основе ролей (RBAC) в Консоли администрирования, в разделе с правами управления плагином Kaspersky Endpoint Agent отображаются флажки, соответствующие правам "Чтение" и "Выполнение операций с выборками устройств", которые не применяются к блокам параметров в Kaspersky Security Center. Если вы установите эти флажки, права "Чтение" и "Выполнение операций с выборками устройств" не будут ограничены для указанных пользователей.
- К некоторым событиям Kaspersky Endpoint Agent, которые публикуются в Консоли администрирования Kaspersky Security Center, не применяются фильтры при построении выборок событий.
- В свойствах объекта, помещенного на карантин в репозиторий Сервера администрирования, в поле **User** записывается имя рабочей группы, а не имя пользователя.
- Если при запуске групповых задач выставлено расписание запуска **При запуске программы**, в истории выполнения задачи статус выполнения задачи обновляется с отсрочкой. По этой причине в некоторых случаях в истории выполнения задачи не будут отображаться статусы выполнения задачи.
- Запуск задачи Аудит безопасности доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Ограничения телеметрии:

- Перед отправкой событий телеметрии на KATA Central Node программа Kaspersky Endpoint Agent сохраняет данные в очередь событий. Kaspersky Endpoint Agent прекращает размещать события в очереди, если размер очереди необработанных событий достигает 1ГБ.
- При работе программы Kaspersky Endpoint Agent на устройствах с операционной системой Windows 7 программа исключает из телеметрии данные о сетевых соединениях, относящихся к процессам с идентификаторами PID=4 и PID=0.
- Если программа Kaspersky Endpoint Agent используется на одном устройстве с программой Kaspersky Endpoint Security и в программе Kaspersky Endpoint Security установлен компонент, обеспечивающий файловое шифрование (FLE), то программа Kaspersky Endpoint Agent не регистрирует события телеметрии о загрузке модулей (LoadImage) и не отправляет их компоненту KATA Central Node.
- В операционных системах Windows XP и Windows Vista в событиях телеметрии, отправляемых на сервер сбора телеметрии, может отсутствовать некоторая информация о файлах. Это связано с тем, что возможность получения некоторой информации о файлах появилась в более поздних версиях операционных систем MS Windows.
- В операционных системах Windows 11 22H2 и выше по умолчанию включена функция Безопасность на основе виртуализации, из-за чего телеметрия консольного ввода на сервер Kaspersky Anti Targeted Attack Platform может не отправляться.

Ограничения сканирования IOC:

- При проверке индикаторов компрометации, поиск которых предполагает разбор текстовых строк, по условию "is" учитывается наличие пробелов, а также необходимость экранировать описание индикатора в IOC-файле символами CDATA. Например, чтобы обнаружить объект с копирайтом "Copyright (C) 1998-2017 John Smith" по условию "is", необходимо указать описание индикатора в следующем формате: <Content type="string"><![CDATA[Copyright (C) 1998-2017 John Smith]]></Content>. Для упрощения описания индикаторов можно также использовать условие "contains".
- Kaspersky Endpoint Agent может дважды отображать данные о сработавшем объекте при выводе результатов задачи поиска IOC.
- При проверке объектов по IOC-документу FileItem Kaspersky Endpoint Agent пропускает объекты, доступ к которым ограничен, например файлы, с которыми на момент проверки работают другие программы. Для таких объектов Kaspersky Endpoint Agent возвращает ложно-отрицательный результат проверки.
- При поиске индикаторов, включающих перебор модулей, загруженных в адресное пространство, Kaspersky Endpoint Agent пропускает случаи, в которых система загружает 64-разрядные модули в 32-разрядные процессы. Например, загрузка wowcpu64.dll в system32 или загрузка ntdll в system32 не будут обнаружены. Ограничение воспроизводится в операционных системах Windows Server 2008 R2 и Windows 7 x64.

Ограничения локализации:

- При несовпадении локализации Kaspersky Endpoint Agent и плагина управления Kaspersky Endpoint Agent в Kaspersky Security Center некоторые параметры могут некорректно отображаться в выводах команд "show" в командную консоль.
- Утилита командной строки agent.exe не поддерживает работу с кириллическими символами. Например, если в списке узлов Kaspersky Sandbox в параметрах Kaspersky Endpoint Agent указан узел, адрес которого содержит кириллические символы, вывод команды `--sandbox=show` может содержать ошибки.

- Установщик Kaspersky Endpoint Agent и плагина управления Kaspersky Endpoint Agent автоматически выбирает локализацию программы на основе региональных параметров операционной системы на устройстве, где выполняется установка программы или плагина управления:
  - если в операционной системе используется локаль RU-RU, устанавливается русская версия Kaspersky Endpoint Agent или плагина управления Kaspersky Endpoint Agent;
  - если в операционной системе используется любая локаль, отличная от RU-RU, устанавливается английская версия Kaspersky Endpoint Agent или плагина управления Kaspersky Endpoint Agent.

  Локализация программы влияет на язык текстов, используемых при описании модулей программы в системе и при публикации событий работы программы в журнал событий Windows, и на отчеты Kaspersky Security Center. Локализация плагина управления Kaspersky Endpoint Agent влияет на язык текстов, используемых в интерфейсе программы в Консоли администрирования (интерфейс политик, групповых задач и свойств программы). Локализацию программы нельзя настроить вручную.

  Обратите внимание, что при несовпадении региональных параметров на управляемых устройствах и на устройстве с установленным плагином управления Kaspersky Endpoint Agent, локализация интерфейса Kaspersky Endpoint Agent в Консоли администрирования и локализация событий, публикуемых программой в отчеты Kaspersky Security Center, могут не совпадать. Также локализация интерфейса программы в Консоли администрирования и локализация событий, публикуемых программой в отчеты Kaspersky Security Center, могут отличаться от локализации интерфейса Консоли администрирования и интерфейса совместимых EPP в Консоли администрирования.
- В интерфейсе Консоли администрирования Kaspersky Security Center и Kaspersky Security Center Web Console в разделах, связанных с управлением программой Kaspersky Endpoint Agent, для некоторых элементов управления текст отображается в усеченном виде.

kaspersky

Установка и удаление Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent на устройство, как обновить предыдущую версию программы и как удалить программу с устройства.

В этом разделе

Подготовка к установке Kaspersky Endpoint Agent

Перед установкой Kaspersky Endpoint Agent на устройство или обновлением предыдущей версии программы проверьте следующие условия:

- выполнение аппаратных и программных требований (см. раздел "Программные и аппаратные требования" на стр. 41);
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

Установка Kaspersky Endpoint Agent

Установка Kaspersky Endpoint Agent может быть выполнена:

- локально с помощью Мастера установки (см. раздел "Установка Kaspersky Endpoint Agent с помощью Мастера установки" на стр. 52);
- локально с помощью командной строки (см. раздел "Установка, восстановление и удаление программы с помощью командной строки" на стр. 53);
- удаленно с помощью Kaspersky Security Center (см. раздел "Установка Kaspersky Endpoint Agent с помощью Kaspersky Security Center" на стр. 56);
- удаленно с помощью редактора управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).

При удаленной установке параметры установки можно передать при помощи конфигурационного файла install_props.json. Для это необходимо предварительно разместить файл install_props.json в одной папке с файлом endpointagent.msi.

Кодировка файла: UTF-8. В содержимом файла поддерживаются два синтаксиса, приведенные в примерах ниже.

Используйте параметры EULA=1 и PRIVACYPOLICY=1, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Пример 1:

```
[Setup]
EULA=1
PRIVACYPOLICY=1
UNLOCK_PASSWORD=<пароль>
```

Пример 2:

```
{
"EULA":"1",
"PRIVACYPOLICY":"1",
"UNLOCK_PASSWORD":"<пароль>"
}
```

Локальная установка и удаление Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent локально на устройстве.

В этом разделе

Установка Kaspersky Endpoint Agent с помощью Мастера установки

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

► *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,*

скопируйте файл endpointagent.msi, входящий в комплект поставки, на устройство пользователя и запустите его.

Запустится мастер установки программы.

После установки программы Kaspersky Endpoint Agent на устройство, мастер установки может быть запущен на этом устройстве в одном из следующих режимов:

- **Восстановление** (восстановить поврежденные модули программы).
- **Удаление** (удалить программу с устройства).

Удаление Kaspersky Endpoint Agent с помощью Мастера установки и удаления

Вы можете удалить Kaspersky Endpoint Agent стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

Установка, восстановление и удаление программы с помощью командной строки

Kaspersky Endpoint Agent можно установить и удалить при помощи msi-пакета, задавая при этом значения свойств MSI стандартным образом. Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Установка Kaspersky Endpoint Agent

Ниже приведен пример установки программы в неинтерактивном режиме с параметрами по умолчанию. После запуска установки программы в неинтерактивном режиме ваше участие в процессе установки не требуется.

Установка Kaspersky Endpoint Agent в неинтерактивном режиме требует принятия Лицензионного соглашения и Политики конфиденциальности. Используйте параметры `EULA=1` и `PRIVACYPOLICY=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Пример:

```
msiexec /i endpointagent.msi EULA=1 PRIVACYPOLICY=1 USE_AZURE_SUPPORT=1
ENABLE_L2_SNIFFER=1 /qn
```

Таблица 3. Параметры команды для установки Kaspersky Endpoint Agent

Параметр	Описание
`EULA`	Обязательный параметр. Параметр передает согласие или отказ от условий Лицензионного соглашения. Значения: • 0 – отказ; • 1 – согласие. Если передано значение 0, то установка программы не выполняется.
`PRIVACYPOLICY`	Обязательный параметр. Параметр передает согласие или отказ от условий Политики конфиденциальности. Значения: • 0 – отказ; • 1 – согласие. Если передано значение 0, то установка программы не выполняется.

Параметр	Описание
USE_AZURE_SUPPORT	Параметр устанавливает признак использования идентификатора физического оборудования в виде значения параметра EnableAzureSupport HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment для операционных систем на платформе x86 или HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\SOYUZ\4.0\Environment для операционных систем на платформе x64. Значения: • 0 – Kaspersky Endpoint Agent при отправке событий на сервер сбора телеметрии в качестве значения sensor_id в отправляемых запросах серверу передает идентификатор ОС хоста из реестра. Значение по умолчанию. • 1 – Kaspersky Endpoint Agent при отправке событий на сервер сбора телеметрии в качестве значения sensor_id в отправляемых запросах серверу передает идентификатор BIOS хоста.
ENABLE_L2_SNIFFER	Параметр указывает на установку драйвера снифферa L2, с помощью которого Kaspersky Endpoint Agent отправляет расширенную телеметрию L2 в адрес Kaspersky Industrial CyberSecurity for Networks. Значения: • 0 – во время установки Kaspersky Endpoint Agent драйвер снифферa L2 не устанавливается. Значение по умолчанию. • 1 – во время установки Kaspersky Endpoint Agent драйвер снифферa L2 устанавливается. Если вы устанавливаете Kaspersky Endpoint Agent поверх предыдущей версии программы и ранее драйвер снифферa L2 был установлен, то, независимо от значения параметра, драйвер снифферa L2 будет остановлен, обновлен и заново запущен.

Восстановление Kaspersky Endpoint Agent

Ниже приведен пример восстановления программы в неинтерактивном режиме. После запуска восстановления программы в неинтерактивном режиме ваше участие в процессе восстановления не требуется.

Пример:

```
msiexec /i endpointagent.msi REINSTALL=ALL /qn
```

kaspersky

Удаление Kaspersky Endpoint Agent

Ниже приведен пример удаления программы в неинтерактивном режиме. После запуска удаления программы в неинтерактивном режиме ваше участие в процессе удаления не требуется.

Пример:

```
msiexec /i {99237667-507D-4F5E-9D2D-2BE6F69EE32F} REMOVE=ALL /qn
```

Если программа защищена паролем:

```
msiexec /i {99237667-507D-4F5E-9D2D-2BE6F69EE32F} REMOVE=ALL
UNLOCK_PASSWORD=<пароль> /qn
```

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

Если при установке, восстановлении или обновлении Kaspersky Endpoint Agent был установлен драйвер сниффера L2, то после удаления программы он тоже удаляется.

kaspersky

Установка Kaspersky Endpoint Agent с помощью Kaspersky Security Center

Kaspersky Endpoint Agent можно установить с помощью задачи удаленной установки в Kaspersky Security Center. Установка состоит из следующих этапов:

1. Создание инсталляционного пакета (см. раздел "Создание инсталляционного пакета Kaspersky Endpoint Agent" на стр. 56).
2. Создание задачи удаленной установки (см. раздел "Создание задачи удаленной установки Kaspersky Endpoint Agent" на стр. 58).

Kaspersky Security Center также поддерживает и другие способы установки программ на группы управляемых устройств. Подробнее об установке с помощью задачи удаленной установки и о других способах установки см. в *Справке Kaspersky Security Center*.

При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

В этом разделе

Создание инсталляционного пакета Kaspersky Endpoint Agent

Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файла с расширением KUD, входящего в состав дистрибутива программы.

► *Чтобы создать инсталляционный пакет в Консоли администрирования Kaspersky Security Center:*

1. В Консоли администрирования Kaspersky Security Center перейдите в папку **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Просмотреть актуальные версии программ "Лаборатории Касперского"**.

   Появится список текущих версий программ "Лаборатории Касперского".
3. Выберите инсталляционный пакет Kaspersky Endpoint Agent.
4. Нажмите на кнопку **Загрузить программу и создать инсталляционный пакет**.

   Инсталляционный пакет отображается в списке инсталляционных пакетов.

5. Чтобы изменить свойства инсталляционного пакета, в контекстном меню инсталляционного пакета выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета Kaspersky Endpoint Agent. Вы можете указать:

   - папку для установки программы;
   - значение параметра восстановления программы;
   - значение параметра совместимости с Azure WVD;
   - значение параметра для установки драйвера сниффера L2;

     > Если инсталляционный пакет используется для установки Kaspersky Endpoint Agent поверх предыдущей версии программы и ранее драйвер сниффера L2 был установлен, то, независимо от значения параметра, драйвер сниффера L2 будет остановлен, обновлен и заново запущен.

   - параметры файла ключа для активации программы.

Новый инсталляционный пакет теперь доступен в списке инсталляционных пакетов. Вы можете использовать этот инсталляционный пакет для задачи удаленной установки (см. раздел "Создание задачи удаленной установки Kaspersky Endpoint Agent" на стр. 58).

► *Чтобы создать инсталляционный пакет в Веб-консоли Kaspersky Security Center:*

1. В главном окне Веб-консоли Kaspersky Security Center перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета.

3. На первой странице мастера выберите параметр **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех программ, которые совместимы с текущей версией Kaspersky Security Center.

4. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

   Откроется окно с информацией об инсталляционном пакете.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить и создать инсталляционный пакет** отображается кнопка **Загрузить дистрибутив**. В этом случае вам необходимо выполнить следующие действия:

   a. Нажмите на кнопку **Загрузить дистрибутив**, чтобы загрузить дистрибутив на свой компьютер.

      Дождитесь окончания загрузки файла.

   b. Закройте окно мастера создания инсталляционного пакета и заново запустите мастер.

   c. На первой странице мастера выберите параметр **Создать инсталляционный пакет из файла**.

   d. На второй странице мастера укажите путь к файлу дистрибутива на вашем компьютере.

e. Следуйте дальнейшим указаниям мастера.

6. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.
7. После завершения загрузки нажмите на кнопку **Закрыть**.

   Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.
8. Чтобы изменить свойства инсталляционного пакета, нажмите на имени инсталляционного пакета.

   Откроется окно свойств инсталляционного пакета Kaspersky Endpoint Agent. Вы можете указать:

   - папку для установки программы;
   - значение параметра восстановления программы;
   - значение параметра совместимости с Azure WVD;
   - значение параметра для установки драйвера сниффера L2;

     Если инсталляционный пакет используется для установки Kaspersky Endpoint Agent поверх предыдущей версии программы и ранее драйвер сниффера L2 был установлен, то, независимо от значения параметра, драйвер сниффера L2 будет остановлен, обновлен и заново запущен.

   - параметры файла ключа для активации программы.

Новый инсталляционный пакет теперь доступен в списке инсталляционных пакетов. Вы можете использовать этот инсталляционный пакет для задачи удаленной установки (см. раздел "Создание задачи удаленной установки Kaspersky Endpoint Agent" на стр. 58).

При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

Создание задачи удаленной установки Kaspersky Endpoint Agent

Для удаленной установки Kaspersky Endpoint Agent с помощью Kaspersky Security Center предназначена задача Удаленная установка программы. Для установки программы задача использует инсталляционный пакет программы (см. раздел "Создание инсталляционного пакета Kaspersky Security Center с пользовательскими OVAL- или XCCDF-правилами" на стр. 262).

► *Чтобы создать задачу удаленной установки в Консоли администрирования Kaspersky Security Center:*

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **Задачи**.

   Откроется список задач.

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

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

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

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите инсталляционный пакет Kaspersky Endpoint Agent (см. раздел "Создание инсталляционного пакета Kaspersky Endpoint Agent" на стр. 56).

Вы можете изменить свойства инсталляционного пакета в Kaspersky Security Center.

Шаг 3. Дополнительно

Совместно с Kaspersky Endpoint Agent может быть установлен Агент администрирования. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Если вы хотите установить Агент администрирования совместно с Kaspersky Endpoint Agent, выберите инсталляционный пакет Агента администрирования.

Шаг 4. Параметры

Настройте следующие дополнительные параметры программы:

- **Принудительно загрузить инсталляционный пакет**. Выберите средства установки программы:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования устанавливается средствами операционной системы. Далее Kaspersky Endpoint Agent устанавливается средствами Агента администрирования.
  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в *Справке Kaspersky Security Center*.
  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.
- **Поведение устройств, управляемых другими Серверами**. Выберите способ установки Kaspersky Endpoint Agent. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.
- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите устройства, на которые будет установлена программа Kaspersky Endpoint Agent.

Шаг 7. Выбор учетной записи для запуска задачи

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

Шаг 8. Настройка расписания запуска задачи

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

Шаг 9. Определение названия задачи

Введите название задачи, например, `Установка Kaspersky Endpoint Agent.`

Шаг 10. Завершение создания задачи

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

► *Чтобы создать задачу удаленной установки Веб-консоли Kaspersky Security Center:*

1. В главном окне Веб-консоли Kaspersky Security Center перейдите в раздел **Устройства** → **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Программа** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка программы**.
3. В поле **Название задачи** введите короткое описание, например, `Установка Kaspersky Endpoint Agent`.
4. В разделе **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлена программа Kaspersky Endpoint Agent в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Agent (см. раздел "Создание инсталляционного пакета Kaspersky Endpoint Agent" на стр. 56).
2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Endpoint Agent. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.
3. В блоке **Принудительно загружать инсталляционный пакет** выберите средства установки программы:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования устанавливается средствами операционной системы. Далее Kaspersky Endpoint Agent устанавливается средствами Агента администрирования.
   - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на управляемые устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в *Справке Kaspersky Security Center*.
   - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на управляемые устройства будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на управляемом устройстве не установлен Агент администрирования, но управляемое устройство находится в той же сети, что и Сервер администрирования.
4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.
5. В поле **Количество попыток установки** установите ограничение попыток установить программу. Если установка Kaspersky Endpoint Agent завершается с ошибкой, задача автоматически запускает установку повторно.
6. Если требуется, снимите флажок **Не устанавливать программу, если она уже установлена**. Это позволит, например, установить программу более ранней версии.
7. Если требуется, снимите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки дистрибутива программы, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.
8. Если требуется, установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка Kaspersky Endpoint Agent выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

9. Если требуется, установите флажок **Предлагать пользователю закрыть работающие программы**. Установка Kaspersky Endpoint Agent требует ресурсов компьютера. Для удобства пользователя мастер установки программы предлагает закрыть работающие программы перед началом установки. Это позволит избежать замедление в работе других программ и возможных сбоев в работе компьютера.
10. В блоке **Поведение устройств, управляемых другими Серверами** выберите способ установки Kaspersky Endpoint Agent. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера.

Шаг 5. Выбор учетной записи для запуска задачи

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

Шаг 6. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Установка программы будет выполнена в тихом режиме.

См. также

Создание инсталляционного пакета Kaspersky Endpoint Agent 56

kaspersky

Установка средств администрирования Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить плагин управления Kaspersky Endpoint Agent для управления Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center (см. раздел "Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center" на стр. 122) или веб-плагин управления Kaspersky Endpoint Agent для управления Kaspersky Endpoint Agent в Kaspersky Security Center Web Console.

В этом разделе

Установка и обновление плагина управления Kaspersky Endpoint Agent

Для управления Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center (см. раздел "Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center" на стр. 122) вам потребуется установить плагин управления Kaspersky Endpoint Agent.

► *Чтобы установить плагин управления Kaspersky Endpoint Agent,*

скопируйте файл klcfginst.msi, входящий в комплект поставки, на устройство с установленной Консолью администрирования Kaspersky Security Center и запустите его.

Запустится мастер установки программы.

Обновление предыдущей установленной версии плагина управления Kaspersky Endpoint Agent

Обновление доступно только для плагинов управления Kaspersky Endpoint Agent версий 3.7 и выше.

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, политики, групповые и локальные задачи переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

  Чтобы применить ранее недоступные параметры, после обновления плагина необходимо внести и сохранить любое изменение в нужную политику или задачу.

- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

  При создании новой политики на основе старой флажок для согласия с условиями Положения о KSN снят. В уже созданной политике состояние флажка для согласия с Положением о KSN остается прежним.

Вы можете использовать новый плагин для управления предыдущими версиями программы Kaspersky Endpoint Agent. При этом Kaspersky Endpoint Agent предыдущих версий не поддерживает и не применяет параметры, появившиеся в новой версии плагина.

Установка и обновление веб-плагина управления Kaspersky Endpoint Agent

Для управления Kaspersky Endpoint Agent с помощью Kaspersky Security Center Web Console вам потребуется установить веб-плагин управления Kaspersky Endpoint Agent.

Вы можете установить веб-плагин следующими способами:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.
- Из списка доступных дистрибутивов в Kaspersky Security Center Web Console.

  Подробная информация об установке веб-плагинов управления доступна в справке Kaspersky Security Center https://help.kaspersky.com/KSC/14.2/ru-RU/176101.htm.
- Загрузив дистрибутив в Kaspersky Security Center Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Agent в интерфейсе Web Console (Параметры Консоли → Веб-плагины). Дистрибутив веб-плагина вы можете загрузить, например, с веб-сайта "Лаборатории Касперского".

Обновление предыдущей установленной версии веб-плагина управления Kaspersky Endpoint Agent

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, политики, групповые и локальные задачи переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

  > Чтобы применить ранее недоступные параметры, после обновления плагина необходимо внести и сохранить любое изменение в нужную политику или задачу.
- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

  > При создании новой политики на основе старой флажок для согласия с условиями Положения о KSN снят. В уже созданной политике состояние флажка для согласия с Положением о KSN остается прежним.

Вы можете использовать новый плагин для управления предыдущими версиями программы Kaspersky Endpoint Agent. При этом Kaspersky Endpoint Agent предыдущих версий не поддерживает и не применяет параметры, появившиеся в новой версии плагина.

kaspersky

Обновление предыдущей версии Kaspersky Endpoint Agent

Обновление Kaspersky Endpoint Agent возможно для версий программы, установленных в составе программ Endpoint Protection Platform и установленных отдельно. Обновление Kaspersky Endpoint Agent, установленной отдельно, доступно только для версий 3.8 и выше. Обновление выполняется путем установки новой версии.

При обновлении Kaspersky Endpoint Agent действующая лицензия автоматически применится к Kaspersky Endpoint Agent 3.16. Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности (см. раздел "Функциональные ограничения после окончания срока действия лицензии" на стр. 76).

В процессе установки Kaspersky Endpoint Agent 3.16 на устройство с установленной предыдущей версией Kaspersky Endpoint Agent все данные, которые можно перенести, сохраняются и используются, а предыдущая версия программы автоматически удаляется.

Если вы устанавливаете Kaspersky Endpoint Agent 3.16 на устройство с установленной предыдущей версией Kaspersky Endpoint Agent, для подключения к Kaspersky Security Center и перенесения данных предыдущей версии в новую версию необходимо создать учетную запись. Для учетной записи используется логин по умолчанию AutoIOC_Admin и пароль, заданный пользователем.

При обновлении предыдущей версии Kaspersky Endpoint Agent, защищенной паролем, необходимо передать установщику этот пароль одним из следующих способов:

- При установке локально через интерфейс Мастера установки (см. раздел "Установка Kaspersky Endpoint Agent с помощью Мастера установки" на стр. 52) или в интерактивном режиме через командную строку указать пароль на соответствующем шаге.
- При установке локально через командную строку в неинтерактивном режиме (см. раздел "Установка, восстановление и удаление программы с помощью командной строки" на стр. 53) указать пароль в качестве значения ключа `UNLOCK_PASSWORD`.
- При установке удаленно через Kaspersky Security Center (см. раздел "Установка Kaspersky Endpoint Agent" на стр. 50) передать текущий пароль в параметрах инсталляционного пакета.

При обновлении Kaspersky Endpoint Agent в составе EPP можно передать пароль в качестве значения ключа `UNLOCK_PASSWORD` в конфигурационном файле install_props.json.

Кодировка файла: UTF-8. В содержимом файла поддерживаются два синтаксиса, приведенные в примерах ниже.

Используйте параметры EULA=1 и PRIVACYPOLICY=1, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Пример 1:

```
[Setup]
EULA=1
PRIVACYPOLICY=1
UNLOCK_PASSWORD=<пароль>
```

Пример 2:

```
{
"EULA":"1",
"PRIVACYPOLICY":"1",
"UNLOCK_PASSWORD":"<пароль>"
}
```

Пароль программы, передаваемый через конфигурационный файл install_props.json, хранится в файле в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется ограничить доступ к файлу install_props.json и удалить его с устройства после установки или обновления программы.

Начиная с версии 3.10 в Kaspersky Endpoint Agent нет возможности настроить использование службы Kaspersky Managed Protection (далее KMP). Если в предыдущей установленной версии Kaspersky Endpoint Agent было включено использование службы KMP, то после обновления программы до версии 3.10 и выше служба KMP продолжает работать. После обновления вы можете отключить службу KMP только при помощи Плагина управления Kaspersky Endpoint Agent или Веб-плагина Kaspersky Endpoint Agent версий ниже 3.10.

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, политики, групповые и локальные задачи переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

  Чтобы применить ранее недоступные параметры, после обновления плагина необходимо внести и сохранить любое изменение в нужную политику или задачу.

- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

  При создании новой политики на основе старой флажок для согласия с условиями Положения о KSN снят. В уже созданной политике состояние флажка для согласия с Положением о KSN остается прежним.

Вы можете использовать новый плагин для управления предыдущими версиями программы Kaspersky Endpoint Agent. При этом Kaspersky Endpoint Agent предыдущих версий не поддерживает и не применяет параметры, появившиеся в новой версии плагина.

Восстановление Kaspersky Endpoint Agent

Установщик Kaspersky Endpoint Agent, запущенный вами в режиме Восстановление, проверяет и восстанавливает целостность всех поврежденных модулей программы и ключей системного реестра, созданных при установке программы.

Вы можете запустить установщик в режиме восстановления одним из следующих способов:

- локально с помощью Мастера установки Kaspersky Endpoint Agent (см. раздел "Установка Kaspersky Endpoint Agent с помощью Мастера установки" на стр. 52);
- локально с помощью командной строки (см. раздел "Установка, восстановление и удаление программы с помощью командной строки" на стр. 53);
- удаленно с помощью Kaspersky Security Center, выполнив одно из следующих действий (подробнее см. в *справке Kaspersky Security Center*):
  - установив флажок **Выполнять восстановление, если программа уже установлена** при создании инсталляционного пакета;
  - указав параметр `REINSTALL=ALL` при создании пользовательского инсталляционного пакета.

Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления, а *программа не требует восстановления*, то установщик не выполняет никаких изменений на устройстве.
Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления, а *программа не установлена на устройстве*, то будет запущена установка программы.
Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления локально с помощью командной строки или удаленно с помощью с помощью Kaspersky Security Center, а *параметры установленной программы отличаются от параметров, указанных при запуске установщика*, то запустится режим изменения параметров установленной программы.

Изменения в системе после установки Kaspersky Endpoint Agent

При установке Kaspersky Endpoint Agent служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Endpoint Agent;
- регистрирует в системном реестре ключи Kaspersky Endpoint Agent;
- регистрирует службы и драйверы Kaspersky Endpoint Agent.

Папки Kaspersky Endpoint Agent на защищаемом устройстве

При установке Kaspersky Endpoint Agent на устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Endpoint Agent, содержащая исполняемые файлы Kaspersky Endpoint Agent:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\
- Папка, содержащая драйверы Kaspersky Endpoint Agent(x86):
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\<версия_ОС>\<имя драйвера>
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\x64\<версия ОС>\<имя драйвера>
- Папки, содержащие файлы IOC:
  - В 32-х разрядной версии Microsoft Windows:
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.1
  - В 64-х разрядной версии Microsoft Windows:
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.1
- Папки, содержащие служебные файлы Kaspersky Endpoint Agent:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Images
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kata
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kmp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Syslog
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Hunts
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Settings
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\DSKM
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp\Tasks

    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Bases
- Папка, содержащая служебные файлы для работы с Kaspersky Security Network.
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Ksn
- Папка, содержащая файлы, помещенные на карантин:
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
- Папка, содержащая файлы, восстановленные из карантина:
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Restored
- Папка, содержащая файлы конфигурации политики Kaspersky Security Center:
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Policy
- Папки, содержащие служебные файлы для работы с Kaspersky Sandbox:
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox\Queue
- Папка, содержащая файлы обновляемых компонентов:
    - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Update
- Папка, содержащая файлы ярлыков для меню Пуск:
    - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Kaspersky Endpoint Agent

Службы и драйверы Kaspersky Endpoint Agent

Следующие службы Kaspersky Endpoint Agent регистрируются и запускаются под системной учетной записью (SYSTEM):

- SOYUZ.exe – это основная служба Kaspersky Endpoint Agent, которая управляет задачами и рабочими процессами программы, обеспечивает взаимодействие между Kaspersky Endpoint Agent и компонентом Central Node.
- ANGARA.dll (исполняется в proton.exe) – это служба, которая обеспечивает взаимодействие между Kaspersky Endpoint Agent и EPP в сценариях интеграции с Kaspersky Sandbox.

Следующие драйверы Kaspersky Endpoint Agent регистрируются на устройстве:

- klsnsr.sys – это драйвер для работы с трассировкой событий Windows (ETW).
- klncap.sys – это анализатор сетевых пакетов ETW.

    При установке на устройство с ОС Microsoft Windows XP вместо klncap.sys регистрируется драйвер klncapxp.sys.

kaspersky

Ключи системного реестра

В результате установки Kaspersky Endpoint Agent создаются следующие ключи системного реестра:

Ключи системного реестра указаны в представлении для 32-разрядных приложений.

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdDisplayName]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdVersion]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ConnectorVersion]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ConnectorFlags]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\NagentMinVer]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ConnectorPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString3]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString3KPD]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\ProductCode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\NoPPL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\BFESDDL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EnableKillChain]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\SvmUpdateMode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\MsiPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\AgentPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EventsExpirationTimeout]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallTime]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLocalization]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallPlatformType]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\Version]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\StartMenu]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\UninstallShortcut2]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\RelNotes]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\License]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Ksn]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Kmp]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\angara]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncapxp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\soyuz]

kaspersky

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Endpoint Agent.

В сертифицированной версии Kaspersky Endpoint Agent допускается только активация файлом ключа. Иные способы активации приводят к выходу приложения из безопасного состояния.

В этом разделе

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Agent.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

kaspersky

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Agent прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Agent). Чтобы продолжить использование Kaspersky Endpoint Agent в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа .

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

kaspersky

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

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

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения программного решения, в состав которого входит Kaspersky Endpoint Agent, или после заказа пробной версии этого программного решения.

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

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно обратиться к продавцу лицензии.

kaspersky

Активация Kaspersky Endpoint Agent

Этот раздел содержит информацию об активации Kaspersky Endpoint Agent.

В этом разделе

Управление активацией Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent одним из следующих способов:

- Во время установки программы:
  - указав файл ключа на отдельном шаге Мастера установки (см. раздел "Установка Kaspersky Endpoint Agent с помощью Мастера установки" на стр. 52);
  - предварительно разместив файл ключа в одной папке с файлом endpointagent.msi при установке в неинтерактивном режиме (см. раздел "Установка, восстановление и удаление программы с помощью командной строки" на стр. 53) (в том числе при удаленной установке (см. раздел "Установка Kaspersky Endpoint Agent" на стр. 50));
  - указав путь к файлу ключа при помощи параметра `LICENSEKEYPATH` при установке в неинтерактивном режиме (см. раздел "Установка, восстановление и удаление программы с помощью командной строки" на стр. 53) (в том числе при удаленной установке (см. раздел "Установка Kaspersky Endpoint Agent" на стр. 50)).

    При наличии в папке нескольких файлов ключа, Kaspersky Endpoint Agent будет активирован при помощи файла ключа с самой поздней датой окончания срока действия лицензии.
    Если установщик Kaspersky Endpoint Agent не обнаружит файл ключа пригодный для активации Kaspersky Endpoint Agent, то программа будет установлена без активации.

При обновлении Kaspersky Endpoint Agent действующая лицензия автоматически применится к Kaspersky Endpoint Agent 3.16. Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности (см. раздел "Функциональные ограничения после окончания срока действия лицензии" на стр. 76).
Если срок действия лицензии обновляемой версии истек, вы можете добавить лицензионный ключ прямо во время обновления. Можно передать файл ключа одним из указанных способов (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 75).

- После установки программы:
  - при помощи задачи активации программы в Консоли администрирования Kaspersky Security Center (см. раздел "Создание задачи активации Kaspersky Endpoint Agent" на стр. 155) или Kaspersky Security Center Web Console (см. раздел "Создание задач активации Kaspersky Endpoint Agent" на стр. 210);
  - через командную строку (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 237) локально на устройстве.

Вы можете использовать Kaspersky Security Center в качестве прокси-сервера при активации Kaspersky Endpoint Agent (см. раздел "Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent" на стр. 132).

Информацию о действующей лицензии можно просмотреть в Kaspersky Security Center в разделе **Лицензии Лаборатории Касперского**, в свойствах устройства (см. раздел "Просмотр информации о действующей лицензии" на стр. 77) или через командную строку (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 237).

Подробную информацию об управлении ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

После окончания срока действия лицензии программа продолжит работу в режиме ограниченной функциональности (см. раздел "Функциональные ограничения после окончания срока действия лицензии" на стр. 76).

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов Kaspersky Endpoint Agent:

- Прекращается выполнение заданий от компонента Central Node и отправка результатов компоненту Central Node.

  Программа отправляет компоненту Central Node сообщение об изменении статуса активации Kaspersky Endpoint Agent.

  При этом соединение с компонентом Central Node не разрывается. Kaspersky Endpoint Agent продолжает принимать от компонента Central Node задания на создание задач и изменение параметров, но не запускает эти задачи и не включает сетевую изоляцию и функцию Запрет запуска.
- Прекращается отправка телеметрии.
- Недоступно построение графа цепочки развития угрозы.
- Невозможно включить сетевую изоляцию.

  Если сетевая изоляция была включена на момент окончания срока действия лицензии, программа отключает сетевую изоляцию в соответствии с заданными параметрами автоматического отключения сетевой изоляции.
- Невозможно включить функцию Запрет запуска.

  Если функция Запрет запуска была включена на момент окончания срока действия лицензии, программа прекращает блокирование объектов, которые подпадают под заданные правила запрета.

- Останавливаются и становятся недоступными для запуска следующие задачи: Получить файл, Выполнить программу, Завершить процесс, Удалить файл.
- Останавливаются и становятся недоступными для запуска стандартные задачи поиска IOC.
- Прекращается использование KSN/KPSN.

При попытке использования перечисленных функциональных компонентов программы после окончания срока действия лицензии программа записывает критическое событие `LicenseViolation` в журнал событий Windows и в журнал Сервера администрирования Kaspersky Security Center. При работе через командную строку, программа возвращает код `8` (`AccessDenied`).

Просмотр информации о действующей лицензии

Информацию о действующей лицензии можно посмотреть в Kaspersky Security Center в разделе **Лицензии "Лаборатории Касперского"** или в свойствах устройства в разделе **Ключи**. Подробную информацию об управлении ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

► *Чтобы посмотреть информацию о действующей лицензии в Консоли администрирования Kaspersky Security Center:*

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите вкладку **Устройства**.
3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
4. В контекстном меню устройства выберите пункт **Свойства**.

   Откроется окно свойств устройства.
5. Выберите раздел **Программы**.

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
6. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:
   - Двойным щелчком мыши по названию программы.
   - В контекстном меню программы выберите пункт **Свойства**.
   - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".
7. Выберите раздел **Ключи**.

Информация о действующей лицензии отобразится в рабочей области окна.

► *Чтобы посмотреть информацию о действующей лицензии в Kaspersky Security Center Web Console:*

1. На закладке **Устройства** выберите **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства перейдите на закладку **Программы**.
4. В списке программ нажмите на **Kaspersky Endpoint Agent**.
5. В открывшемся окне свойств программы перейдите на закладку **Общие** и откройте раздел **Лицензия**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Данные программы Kaspersky Endpoint Agent

Не используйте Kaspersky Endpoint Agent на устройствах, передача данных с которых запрещена политикой вашей организации.

Для обеспечения основных функций, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского" Kaspersky Endpoint Agent хранит и обрабатывает данные локально.

На устройствах с Kaspersky Endpoint Agent хранятся данные, подготовленные для автоматической отправки на серверы решений Kaspersky Sandbox, KATA и в Kaspersky Security Center. Файлы хранятся на устройствах с Kaspersky Endpoint Agent в открытом незашифрованном виде в папке, которая по умолчанию используется для хранения файлов перед отправкой.

Администратору решения, в состав которого входит Kaspersky Endpoint Agent, необходимо обеспечить безопасность устройств с Kaspersky Endpoint Agent и серверов решения с перечисленными выше данными самостоятельно. Администратор решения несет ответственность за доступ к данной информации.

В этом разделе содержится следующая информация о персональных данных, хранящихся на устройствах с Kaspersky Endpoint Agent, а также передаваемых в Kaspersky Security Center или на серверы "Лаборатории Касперского":

- состав хранимых данных;
- место хранения;
- срок хранения;
- доступ пользователей к данным.

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

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

Конкретный состав данных зависит от решения, в составе которого используется Kaspersky Endpoint Agent.

kaspersky

В этом разделе

Служебные данные

К служебным данным Kaspersky Endpoint Agent относятся:

- данные, попадающие в конфигурационные файлы в результате настройки параметров администратором;
- данные, обрабатываемые при автоматическом реагировании на угрозы;
- данные, обрабатываемые при интеграции с Kaspersky Sandbox;
- данные, обрабатываемые при интеграции с компонентом KATA Central Node;
- данные, обрабатываемые при интеграции с Kaspersky Industrial CyberSecurity for Networks.

Служебные данные хранятся в файле %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>. Данные в подпапке Settings зашифрованы с помощью Шифрующей файловой системы (EFS). Данные хранятся до удаления Kaspersky Endpoint Agent.

Эти данные могут автоматически передаваться в Kaspersky Security Center.

По умолчанию доступ к файлам имеют только пользователи с правами System (полный доступ) и Administrator (чтение и исполнение). Папка %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия> и подпапка Restored также доступны пользователям с правами User (только чтение).

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

Kaspersky Endpoint Agent хранит следующие данные, обрабатываемые при автоматическом реагировании и интеграции с Kaspersky Sandbox:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Пароль доступа к Kaspersky Endpoint Agent.
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent.
   - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
   - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
   - Учетные данные для авторизации на прокси-сервере.
   - Адреса пользовательских источников обновлений.
   - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
2. Кеш Kaspersky Endpoint Agent:
   - Время записи результата проверки в кеш.
   - MD5-хеш задачи проверки.
   - Идентификатор задачи проверки.
   - Результат проверки объекта.
3. Очередь запросов на проверку объекта:
   - Идентификатор объекта в очереди.
   - Время помещения объекта в очередь.
   - Статус обработки объекта в очереди.
   - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
   - Системный идентификатор (SID) пользователя операционной системы, с правами учетной записью которого создана задача на проверку объекта.
   - MD5-хеш задачи на проверку объекта.
4. Информация о задачах, для которых Kaspersky Endpoint Agent ожидает результат проверки от Kaspersky Sandbox:
   - Время получения задачи на проверку объекта.
   - Статус обработки объекта.
   - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
   - Идентификатор задачи на проверку объекта.
   - MD5-хеш задачи на проверку объекта.
   - Системный идентификатор (SID) пользователя операционной системы, под учетной записью которого создана задача.
   - XML-схема автоматически созданного IOC.

- MD5 и SHA256-хеши проверяемого объекта.
- Ошибки обработки.
- Имена объектов, на проверку которых создана задача.
- Результат проверки объекта.

Kaspersky Endpoint Agent хранит локально следующие данные при интеграции с компонентом KATA Central Node:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent:
     - Пароль доступа к Kaspersky Endpoint Agent.
     - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
     - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
     - Учетные данные для авторизации на прокси-сервере.
     - Адреса пользовательских источников обновлений.
     - Открытый ключ сертификата для интеграции с KATA Central Node.
     - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
     - Данные о лицензии.
2. Данные, необходимые для интеграции с компонентом KATA Central Node:
   - Обновляемые схемы фильтрации телеметрии.
   - Очередь пакетов событий телеметрии.
   - Кеш идентификаторов IOC-файлов, полученных от компонента KATA Central Node.
   - Объекты для передачи на сервер в рамках задачи Получить файл.
   - Отчеты о результатах задачи Получить список файлов, процессов.

Kaspersky Endpoint Agent хранит локально следующие данные при интеграции с сервером Kaspersky Industrial CyberSecurity for Networks:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Параметры Kaspersky Endpoint Agent:
     - Пароль доступа к Kaspersky Endpoint Agent.
     - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
     - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
     - Учетные данные для авторизации на прокси-сервере.
     - Адреса пользовательских источников обновлений.

- Открытый ключ сертификата для интеграции с Kaspersky Industrial CyberSecurity for Networks.
- Данные о лицензии.

2. Данные, необходимые для интеграции с Kaspersky Industrial CyberSecurity for Networks:
   - Обновляемые схемы фильтрации телеметрии.
   - Очередь пакетов событий телеметрии.

Данные о событиях Журнала событий Windows

Данные о событиях Журнала событий Windows хранятся в файле %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx в открытом незашифрованном виде. Данные хранятся до удаления Kaspersky Endpoint Agent.

Эти данные могут автоматически передаваться в Kaspersky Security Center.

По умолчанию доступ на чтение к файлам имеют только пользователи с правами System и Administrator. Kaspersky Endpoint Agent не управляет правами доступа к этой папке и ее файлам. Доступ определяет системный администратор.

Данные о событиях могут содержать следующую информацию:

- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы (userID).
- Об ошибках выполнения задач проверки объектов.
- О задачах на проверку объектов.
- Об обнаружениях Kaspersky Sandbox.
- О событиях Kaspersky Sandbox.
- Об IOC-файлах Kaspersky Endpoint Agent, сформированных при автоматическом реагировании.
- О результатах проверки объектов.
- О сертификатах серверов Kaspersky Sandbox.
- Об очереди объектов на проверку.
- Об изменении параметров Kaspersky Endpoint Agent.
- Об изменении политик Kaspersky Security Center.
- Об изменении статуса задачи на проверку объектов.
- О политиках Kaspersky Security Center.
- Об объектах на карантине.
- О действиях по автоматическому реагированию на обнаруженные угрозы.
- Об ошибках взаимодействия с серверами программы.
- Об объектах, заблокированных по правилам Запрета запуска.
- О результатах выполнения задач Удалить файл.
- О результатах выполнения задач Завершить процесс.

- О результатах выполнения задач Выполнить программу.
- О результатах выполнения задач Получить файл.
- О действующей лицензии Kaspersky Endpoint Detection and Response Optimum.
- О статусе активации программы.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

Данные в результатах выполнения задач поиска IOC

Kaspersky Endpoint Agent автоматически передает данные из результатов выполнения задач поиска IOC в Kaspersky Security Center для построения цепочки развития угрозы.

Данные хранятся в базах данных Kaspersky Security Center. По умолчанию данные хранятся 7 дней.

Данные в результатах выполнения задач поиска IOC могут содержать следующую информацию:

- IP-адрес из ARP-таблицы.
- Физический адрес из ARP-таблицы.
- Тип и имя записи DNS.
- IP-адрес защищаемого устройства.
- Физический адрес (MAC) защищаемого устройства.
- Идентификатор записи в журнале событий.
- Имя источника данных в журнале.
- Имя журнала.
- Пользователь.
- Время события.
- MD5-хеш файла.
- SHA256-хеш файла.
- Полное имя файла (включая путь).
- Размер файла.
- Удаленный IP-адрес, с которым было установлено соединение в момент проверки.
- Удаленный порт, с которым было установлено соединение в момент проверки.
- IP-адрес локального адаптера.
- Порт, открытый на локальном адаптере.
- Протокол в виде числа (в соответствии со стандартом IANA).
- Имя процесса.

- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор (PID) процесса.
- Windows идентификатор (PID) родительского процесса.
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Имя службы.
- Описание службы.
- Путь и имя DLL-службы (для svchost).
- Путь и имя исполняемого файла службы.
- Windows идентификатор (PID) службы.
- Тип службы (например, драйвер ядра или адаптер).
- Статус службы.
- Режим запуска службы.
- Имя учетной записи пользователя.
- Наименование тома.
- Буква тома.
- Тип тома.
- Значение реестра Windows.
- Значение куста реестра.
- Путь к ключу реестра (без куста и без имени значения).
- Параметр реестра.
- Система (окружение).
- Имя ОС с версией.
- Сетевое имя защищаемого устройства.
- Домен или группа, к которой принадлежит защищаемое устройство.
- Имя браузера.
- Версия браузера.
- Время последнего обращения к веб-ресурсу.
- URL из HTTP-запроса.
- Имя учетной записи, под которой выполнен HTTP-запрос.
- Имя файла процесса, выполнившего HTTP-запрос.
- Полный путь к файлу процесса, выполнившего HTTP-запрос.
- Windows идентификатор (PID) процесса, выполнившего HTTP-запрос.
- HTTP referer (URL источника HTTP-запроса).

- URI ресурса, запрошенного по протоколу HTTP.
- Информация о HTTP агенте пользователя (приложении, выполнившем HTTP-запрос).
- Время выполнения HTTP-запроса.
- Уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные в результатах сканирования YARA

Kaspersky Endpoint Agent автоматически передает данные результатов сканирования YARA в Kaspersky Anti Targeted Attack Platform для построения цепочки развития угрозы.

Данные временно хранятся локально в очереди отправки результатов выполнения задач на сервер Kaspersky Anti Targeted Attack Platform. После отправки данные удаляются.

Данные в результатах сканирования YARA содержат следующую информацию:

- MD5-хеш файла;
- SHA256-хеш файла;
- полное имя файла;
- путь к файлу;
- размер файла;
- имя процесса;
- аргументы процесса;
- путь к файлу процесса;
- Windows идентификатор процесса (PID);
- Windows идентификатор родительского процесса (PID);
- имя учетной записи пользователя, запустившего процесс;
- дата и время запуска процесса.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы хранятся в папке %ProgramData%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain\detects в открытом незашифрованном виде. По умолчанию данные хранятся 7 дней. Эти данные автоматически передаются в Kaspersky Security Center.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

По умолчанию доступ на чтение к файлам имеют только пользователи с правами System и Administrator. Kaspersky Endpoint Agent не управляет правами доступа к этой папке и ее файлам. Доступ определяет системный администратор.

Данные для построения Цепочки развития угрозы могут содержать следующую информацию:

- Дата и время инцидента.
- Имя обнаружения.
- Режим проверки.
- Статус последнего действия, связанного с обнаружением.
- Причина неудачной обработки обнаружения.
- Тип обнаруженного объекта.
- Имя обнаруженного объекта.
- Статус угрозы после обработки объекта программой EPP.
- Причина неудачного выполнения действий над объектом.
- Действия, выполняемые EPP для отката вредоносных действий (для EPP, поддерживающих Откат вредоносных действий).
- Об обрабатываемом объекте:
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.
  - Уникальный идентификатор файла процесса.
  - Идентификатор процесса Windows.
  - Командная строка процесса.
  - Имя учетной записи пользователя, запустившего процесс.
  - Код сеанса входа в систему, в котором запущен процесс.
  - Тип сеанса (например, "интерактивный", "удаленный интерактивный"), в котором запущен процесс.
  - Уровень целостности обрабатываемого процесса.
  - Принадлежность учетной записи пользователя, запустившего процесс, к привилегированным локальным и доменным группам (например, "Администраторы", "Администраторы домена", "Администраторы предприятия", "Администраторы схемы").
  - Идентификатор обрабатываемого объекта.
  - Полное имя обрабатываемого объекта.
  - Идентификатор защищаемого устройства.
  - Полное имя объекта (имя локального файла или веб-адрес загружаемого файла).
  - MD5-хеш обрабатываемого объекта.
  - SHA256-хеш обрабатываемого объекта.
  - Тип обрабатываемого объекта.
  - Дата создания обрабатываемого объекта.
  - Дата последнего изменения обрабатываемого объекта.
  - Размер обрабатываемого объекта.

- Атрибуты обрабатываемого объекта.
- Организация, подписавшая обрабатываемый объект.
- Результат проверки цифрового сертификата обрабатываемого объекта.
- Идентификатор безопасности (SID) обрабатываемого объекта.
- Идентификатор часового пояса обрабатываемого объекта.
- Веб-адрес загрузки обрабатываемого объекта (только для файла на диске).
- Название программы, загрузившей файл.
- MD5-хеш программы, загрузившей файл.
- SHA256-хеш программы, загрузившей файл.
- Название программы, последний раз модифицировавшей файл.
- MD5-хеш программы, последний раз модифицировавшей файл.
- SHA256-хеш программы, последний раз модифицировавшей файл.
- Количество запусков обрабатываемого объекта.
- Дата и время первого запуска обрабатываемого объекта.
- Уникальный идентификатор файла.
- Полное имя файла (имя локального файла или веб-адрес загружаемого файла).
- Путь к обрабатываемой переменной реестра Windows.
- Имя обрабатываемой переменной реестра Windows.
- Значение обрабатываемой переменной реестра Windows.
- Тип обрабатываемой переменной реестра Windows.
- Показатель принадлежности обрабатываемого ключа реестра к точке автозапуска.
- Веб-адрес обрабатываемого веб-запроса.
- Источник ссылок обрабатываемого веб-запроса.
- Агент пользователя обрабатываемого веб-запроса.
- Тип обрабатываемого веб-запроса ("GET" или "POST").
- Локальный IP-порт для обрабатываемого веб-запроса.
- Удаленный IP-порт для обрабатываемого веб-запроса.
- Направление соединения ("входящее" или "исходящее") обрабатываемого веб-запроса.
- Идентификатор процесса, в который произошло внедрение вредоносного кода.

kaspersky

Предоставление расширенной диагностической информации Kaspersky Endpoint Agent специалистам Службы технической поддержки

Для оказания поддержки при неполадках в работе программы Kaspersky Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия:

- Активировать функциональность получения расширенной диагностической информации.
- Дополнительно настроить отдельные компоненты программы, недоступные для изменения стандартными средствами пользовательского интерфейса.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся информация, необходимая для выполнения перечисленных действий (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т.д.), а также состав данных, анализируемых в отладочных целях, будут озвучены вам специалистами Службы технической поддержки. Расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка сохраненных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в документации программы или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Данные в файлах трассировки и дампов

Kaspersky Endpoint Agent может выполнять запись отладочной информации в файлы трассировки в соответствии с заданными параметрами. Файлы трассировки используются для получения поддержки при работе с Kaspersky Endpoint Agent.

Файлы дампов Kaspersky Endpoint Agent формируются операционной системой при сбоях программы и перезаписываются при каждом сбое.

В файлы трассировки и дампов могут попасть персональные данные пользователей или конфиденциальные данные организации.

Не используйте Kaspersky Endpoint Agent на устройствах, передача данных с которых запрещена политикой вашей организации.

По умолчанию Kaspersky Endpoint Agent не записывает отладочную информацию.

Автоматическая отправка файлов трассировки и дампов за пределы устройства, на котором они были сформированы, не производится. Содержимое файлов трассировки можно просмотреть с помощью стандартных средств просмотра текстовых файлов.

Файлы трассировки и дампов хранятся бессрочно и не удаляются при удалении Kaspersky Endpoint Agent.

Отладочная информация может понадобиться при обращении в Службу технической поддержки.

Специальных механизмов ограничения доступа к файлам трассировки и дампов не предусмотрено. Администратор может самостоятельно настроить запись этой информации в защищенную папку.

Путь к папке для записи файлов трассировки и дампов по умолчанию не задан. Администратору нужно указать папку для записи файлов трассировки и дампов самостоятельно.

Данные в файлах трассировки и дампов могут содержать следующую информацию:

- Действия, выполненные Kaspersky Endpoint Agent на устройстве.
- Информация об объектах, обрабатываемых Kaspersky Endpoint Agent.
- Ошибки, возникшие в процессе работы Kaspersky Endpoint Agent.

kaspersky

Данные, предоставляемые SIEM-серверам

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов (см. раздел "Данные в файлах трассировки и дампов" на стр. 89), удаляются с устройства при удалении программы.

При интеграции с SIEM Kaspersky Endpoint Agent может хранить локально и отправлять в адрес SIEM-серверов следующие данные:

1. Общие данные:
    - Хеш md5 объекта.
    - Хеш sha256 объекта.
    - Версия приложения.
    - Версия файла.
    - Время изменения файла.
    - Время создания файла.
    - Значение IntegrityLevel.
    - Идентификатор Logon-сессии.
    - Идентификатор Zone id.
    - Идентификатор терминальной сессии.
    - Имя пользователя.
    - Имя приложения.
    - Имя файла.
    - Командная строка процесса.
    - Маска атрибутов файловой системы.
    - Метод из HTTP-запроса.
    - Окончательный статус обработки угрозы.
    - Описание файла.
    - Полный путь к образу файла.
    - Предыдущее значение IntegrityLevel.
    - Предыдущее значение идентификатора Logon-сессии.
    - Предыдущее значение привилегий и атрибутов привилегий.
    - Привилегии и атрибуты привилегий.
    - Производитель приложения.
    - Путь из HTTP-запроса.
    - Размер файла.
    - Системный идентификатор процесса.

- Состояние процесса.
- Тип аккаунта.
- Тип операции.
- Тип сессии.
- Тип файла.
- Уникальный идентификатор образа файла.
- Уникальный идентификатор процесса.
- Уникальный идентификатор родительского процесса.
- Хост из HTTP-запроса.

2. Данные о сертификатах подписей объектов:
   - Серийный номер сертификата.
   - The Chaintype.
   - Имя издателя.
   - Имя субъекта.
   - Алгоритм отпечатка сертификата.
   - Отпечаток сертификата.
   - Период действия: не ранее.
   - Период действия: не позднее.
   - Время создания подписи файла.
3. Данные об объектах реестра:
   - Ключ реестра.
   - Содержимое значения ключа реестра.
   - Имя значения ключа реестра.
   - Тип значения реестра.
   - Имя ключа реестра до проведения операции.
   - Данные в ключе реестра до проведения операции.
   - Тип значения в реестре до проведения операции.
4. Данные об объектах и результатах их проверки:
   - Email-адрес отправителя, приславшего объект.
   - Email-адрес получателя.
   - URI объекта (HTTP, HTTPS).
   - Значение номера протокола по IANA.
   - Имя объекта.
   - Командная строка.
   - Локальный сетевой адрес.

- Оригинальный идентификатор процесса.
- Сетевой адрес хоста, вызвавшего подозрительные действия.
- Содержимое скрипта, проверяемого через механизм AMSI.
- Ссылка на процесс, скачавший объект.
- Тип объекта.
- Тип содержимого скрипта, проверяемого через механизм AMSI.
- Уникальный идентификатор процесса.

kaspersky

Сетевая изоляция

Использование компонента возможно только при наличии соответствующей лицензии.

Этот раздел содержит информацию о сетевой изоляции и настройке ее параметров.

В этом разделе

О сетевой изоляции в Kaspersky Endpoint Agent

Kaspersky Endpoint Agent предоставляет возможность изолировать устройства от сети по требованию (вручную) или автоматически, в результате ответных действий на обнаружения.

После включения сетевой изоляции программа разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройствах, кроме следующих соединений:

- соединения, указанные в исключениях из сетевой изоляции;
- соединения, инициированные службами совместимого EPP;
- соединения, инициированные службами Kaspersky Endpoint Agent;
- соединения, инициированные Агентом администрирования Kaspersky Security Center.

Включение и отключение сетевой изоляции

Сетевая изоляция устройства может быть включена вручную или автоматически, в результате ответных действий на обнаружения (см. раздел «Настройка параметров стандартной задачи поиска IOC» на стр. 162).

Сетевая изоляция может быть отключена автоматически по истечении заданного периода времени или вручную.

Если в параметрах сетевой изоляции не установлен флажок **Автоматически прекращать изоляцию устройства по истечении** и не указан период времени, сетевая изоляция будет отключена автоматически через пять часов с момента включения.

После отключения сетевой изоляции устройство может работать в сети без ограничений, наложенных Kaspersky Endpoint Agent при сетевой изоляции.

Исключения из сетевой изоляции

Вы можете задать исключения из сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на устройствах после включения сетевой изоляции.

Для упрощения настройки исключений из сетевой изоляции в программе доступен список сетевых профилей (наборы стандартных правил исключения). Редактирование списка и содержания сетевых профилей не предусмотрено.

Исключения можно задать как в составе сетевых профилей, так и отдельно. Исключения, заданные отдельно от сетевых профилей, называются *пользовательскими*.

По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент.

При изменении параметров исключения, заданного при помощи сетевого профиля, это исключение становится пользовательским.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применяются, только если сетевая изоляция включена вручную.
Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства, так как сценарии применения этих параметров разные.

Об управлении сетевой изоляцией в Kaspersky Endpoint Agent

Вы можете управлять сетевой изоляцией с помощью Сервера администрирования Kaspersky Security Center, через интерфейс компонента Central Node или через интерфейс командной строки на защищаемом устройстве. Информация о возможностях управления сетевой изоляцией каждым из перечисленных способов приведена в следующей таблице.

Таблица 4. Управление сетевой изоляцией

Интерфейс управления	Возможности	Примечания
Консоль администрирования Kaspersky Security Center	• Включение и отключение сетевой изоляции (на стр. 133). • Настройка автоматического отключения сетевой изоляции (на стр. 134). • Настройка уведомления пользователя устройства о сетевой изоляции (см. раздел "Включение и отключение уведомления пользователя о сетевой изоляции" на стр. 133). • Настройка исключений из сетевой изоляции (на стр. 135).	В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную). Включение и отключение сетевой изоляции вручную для группы устройств через политику недоступно.
Командная строка	• Получение информации о текущем состоянии и параметрах сетевой изоляции устройства (см. раздел "Управление сетевой изоляцией" на стр. 253). • Отключение сетевой изоляции на устройстве (см. раздел "Управление сетевой изоляцией" на стр. 253).	Включение сетевой изоляции, а также настройка параметров сетевой изоляции недоступны через интерфейс командной строки.
Компонент Central Node	Управление сетевой изоляцией через компонент Central Node описано отдельно.	Kaspersky Endpoint Agent сохраняет параметры сетевой изоляции, полученные от компонента Central Node, в свойствах устройства в Kaspersky Security Center.

kaspersky

Запрет запуска

Этот раздел содержит информацию о функции Запрет запуска и настройке ее параметров.

В этом разделе

О Запрете запуска

Вы можете управлять правилами запрета запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата (см. раздел "Поддерживаемые расширения файлов для Запрета запуска" на стр. 98) на выбранных устройствах. Например, вы можете запретить запуск программ, использование которых считается небезопасным, на выбранном устройстве с Kaspersky Endpoint Agent. Программа идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Правило запрета запуска – это набор критериев, которые учитываются при выполнении блокировки. Объект должен соответствовать всем критериям правила защиты, чтобы программа заблокировала его исполнение.

Параметрами правил запрета запуска можно управлять с помощью Kaspersky Security Center или из командной строки локально на устройстве.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.

Режим применения правил запрета запуска

Можно выбрать один из двух режимов применения правил запрета запуска:

- **Только статистика**.

  В этом режиме Kaspersky Endpoint Agent публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.

- **Активный**.

  В этом режиме Kaspersky Endpoint Agent блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета.

При включении Запрета запуска в Kaspersky Security Center по умолчанию выбран режим **Только статистика**.

Уведомление пользователя о сработавшем правиле запрета запуска

Вы можете выбрать опцию **Уведомлять пользователя устройства при запрете**. Если Запрет запуска включен в режиме (см. раздел "Включение Запрета запуска" на стр. 196) **Активный** и выбрана опция **Уведомлять пользователя устройства при запрете** (см. раздел "**Включение и отключение уведомления пользователей о Запрете запуска**" на стр. 197), на защищаемых устройствах будут отображаться всплывающие уведомления с информацией о сработавших правилах Запрета запуска. Если пользователь устройства не закроет всплывающее уведомление, то оно закроется автоматически через 60 секунд после появления. По умолчанию опция **Уведомлять пользователя устройства при запрете** выключена.

Управление Запретом запуска

Параметрами Запрета запуска можно управлять с помощью Kaspersky Security Center или из командной строки.

С помощью Kaspersky Security Center вы можете:

- включить (см. раздел "Включение Запрета запуска" на стр. 196) или отключить (см. раздел "Отключение Запрета запуска" на стр. 197) использование Запрета запуска;
- выбрать режим применения правил запрета запуска (см. раздел "Включение Запрета запуска" на стр. 196);
- настроить уведомление пользователей о сработавшем правиле запрета запуска (см. раздел "Включение и отключение уведомления пользователей о Запрете запуска" на стр. 197);
- настроить список правил запрета запуска (см. раздел "Управление списком правил Запрета запуска" на стр. 198);
- включить Запрет запуска из карточки инцидента (см. раздел "Выбор действия с файлом из карточки инцидента" на стр. 116).

С помощью командной строки вы можете отключить Запрет запуска (см. раздел "Управление Запретом запуска" на стр. 277) или просмотреть текущие параметры Запрета запуска (см. раздел "Управление Запретом запуска" на стр. 277).

Поддерживаемые расширения файлов для Запрета запуска

Kaspersky Endpoint Agent поддерживает запрет открытия файлов офисного формата через определенные программы. Информация о поддерживаемых расширениях имен файлов и программ приведена в следующей таблице.

Таблица 5. Поддерживаемые расширения имен файлов для запрета открытия

Имя программы	Исполняемый файл	Расширение имени файла
Microsoft Word	winword.exe	• rtf • doc • dot • docm • docx • dotx • dotm • docb
WordPad	wordpad.exe	• docx • rtf
Microsoft Excel	excel.exe	• xls • xlt • xlm • xlsx • xlsm • xltx • xltm • xlsb • xla • xlam • xll • xlw
Microsoft PowerPoint	powerpnt.exe	• ppt • pot • pps • pptx • pptm • potx • potm • ppam • ppsx • ppsm • sldx • sldm
Adobe Acrobat Microsoft Edge Google Chrome	acrord32.exe MicrosoftEdge.exe chrome.exe	• pdf

Поддерживаемые интерпретаторы запуска скриптов

Запрет запуска скрипта обрабатывается Kaspersky Endpoint Agent, если скрипт запущен с помощью одного из следующих интерпретаторов:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Kaspersky Endpoint Agent поддерживает запрет запуска Java-приложений, работающих в среде выполнения Java (процессы java.exe и javaw.exe).

kaspersky

Поиск IOC

Этот раздел содержит информацию о задачах поиска IOC и настройке их параметров.

В этом разделе

О задачах поиска IOC в Kaspersky Endpoint Agent

Задачи поиска IOC – это задачи, в ходе выполнения которых Kaspersky Endpoint Agent использует IOC-файлы (файлы индикаторов компрометации открытого стандарта описания OpenIOC) для поиска этих индикаторов на устройствах.

Kaspersky Endpoint Agent поддерживает три типа задач поиска IOC:

- *Стандартные задачи поиска IOC* – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.
- *Автономные задачи поиска IOC* – групповые задачи, которые создаются автоматически при реагировании на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Подробнее об автономных задачах поиска IOC см. в *Справке Kaspersky Sandbox*.
- *Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform* – пользователи программы могут использовать IOC-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки компьютеров с установленным компонентом Kaspersky Endpoint Agent.

Задачи отличаются возможностями управления, доступными для настройки параметрами, а также областью действия. Описание каждого типа задач поиска IOC приведено в следующей таблице.

Таблица 6. Типы задач поиска IOC

Тип задач	Описание задач	Область действия задач
Стандартные задачи поиска IOC	Задачи создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки, без интеграции со сторонними системами. Для запуска задач используются IOC-файлы, подготовленные пользователем. Параметры задач не зависят от настроек в параметрах политик. Для задач доступен режим **Ретроспективный поиск IOC**. *Ретроспективный поиск IOC* - это режим работы задачи Поиск IOC, при котором Kaspersky Endpoint Agent выполняет поиск индикаторов компрометации по данным, полученным за указанный пользователем интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности защищаемых устройств. Kaspersky Endpoint Agent анализирует данные в журналах операционной системы и браузеров на устройствах. Режим **Ретроспективный поиск IOC** доступен только для Стандартных задач поиска IOC. Вы можете задать следующие действия по реагированию на найденные IOC (недоступно при запуске задач из командной строки): • Запуск на устройстве задач проверки по требованию при помощи EPP. • Включение сетевой изоляции устройства. Просмотр отчетов доступен как в результатах выполнения задач в виде сводной таблицы, так и в карточке обнаруженных IOC.	*Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла. Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации. Локальные или групповые

Тип задач	Описание задач	Область действия задач
Автономные задачи поиска IOC	Задачи создаются автоматически, если в политике Kaspersky Endpoint Agent задано действие **Запустить Поиск IOC на управляемой группе устройств** по реагированию на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Пользователю доступно ограниченное управление задачами в Kaspersky Security Center. В политике можно задать расписание запуска задач и области поиска. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Вы можете задать следующие действия по реагированию на найденные IOC: • Запуск на устройстве задач проверки по требованию при помощи EPP. • Помещение объекта на карантин и удаление с устройства. Просмотр отчетов доступен как в результатах выполнения задач в виде сводной таблицы, так и в карточке обнаруженных IOC.	Групповые
Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform	IOC-файлы загружаются вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Также есть возможность настроить расписание IOC-проверки компьютеров с программой Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Управление задачами с помощью Kaspersky Security Center или через командную строку не предусмотрено. Автоматических действий при обнаружении IOC не предусмотрено. Параметры задач не зависят от политик Kaspersky Endpoint Agent.	Не применимо

Результаты выполнения групповых задач поиска IOC доступны для просмотра в Kaspersky Security Center в течение семи дней с момента выполнения задачи или до момента удаления задачи.

kaspersky

Требования к IOC-файлам

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.
- Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
- Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.
- Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

В таблице ниже приведены особенности и ограничения поддержки стандарта OpenIOC программой.

Таблица 7. Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0:
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	Программа поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`
	Программа поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

Поддерживаемые IOC-термины	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent:

https://support.kaspersky.com/KEA/3.9/ru-RU/IOC_TERMS.zip

Управление задачами поиска IOC в Kaspersky Endpoint Agent

Вы можете управлять задачами поиска IOC через Kaspersky Security Center или через интерфейс командной строки Kaspersky Endpoint Agent, а также загружать IOC-файлы и настраивать расписание IOC-проверки через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Описание каждого типа задач поиска IOC и информация о доступных возможностях управления задачами поиска IOC приведены в таблице ниже.

Таблица 8. Управление задачами поиска IOC

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки
Стандартная задача поиска IOC	• Создание (см. раздел "Создание и настройка стандартной задачи поиска IOC" на стр. 161), удаление (см. раздел "Удаление задач из списка" на стр. 153) и запуск (см. раздел "Запуск задач вручную" на стр. 154) задачи вручную. • Просмотр детальных отчетов в результатах выполнения задачи (см. раздел "Просмотр результатов выполнения задачи поиска IOC" на стр. 164) в виде сводной таблицы и в карточке обнаруженных IOC. *Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла. Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации. • Экспорт IOC-коллекции (на стр. 163).	Управление не предусмотрено.	• Создание и запуск задачи с требуемыми параметрами (см. раздел "Управление стандартными задачами поиска IOC" на стр. 254). • Просмотр данных о выполнении задачи (см. раздел "Управление стандартными задачами поиска IOC" на стр. 254).

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки

	• Настройка следующих параметров в мастере создания задачи (см. раздел "Создание и настройка стандартной задачи поиска IOC" на стр. 161) или в свойствах задачи (см. раздел "Настройка параметров стандартной задачи поиска IOC" на стр. 162) после ее создания:
	  • Параметры IOC-коллекции.
	  • Параметры поиска IOC.
	  • Действия программы при обнаружении IOC (сетевая изоляция устройства и запуск проверки на устройстве с помощью EPP).
	  • Параметры расписания запуска задачи.
	• Срок хранения результатов выполнения задачи на Сервере администрирования (недоступно в мастере создания задачи).		

Автономная задача поиска IOC	• Настройка запуска задач. • Запуск (см. раздел "Запуск задач вручную" на стр. 154) и удаление (см. раздел "Удаление задач из списка" на стр. 153) задачи вручную. • Включение выполнения действий по реагированию на угрозы, обнаруженные Kaspersky Sandbox. • Добавление действия автоматического создания Автономной задачи поиска IOC. • Просмотр детальных отчетов в результатах выполнения задачи (см. раздел "Просмотр результатов выполнения задачи поиска IOC" на стр. 164) в виде сводной таблицы и в карточке обнаруженных IOC. *Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.	Управление не предусмотрено.	Управление не предусмотрено.

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки

	Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.
	
	• Экспорт IOC-коллекции. (см. раздел "Экспорт IOC-коллекции" на стр. 163)
	• Настройка следующих параметров в свойствах задачи (см. раздел "Настройка параметров автономной задачи поиска IOC" на стр. 166):
	  • Действия программы при обнаружении IOC (помещение объекта на карантин и удаление с устройства; запуск проверки на устройстве с помощью EPP).
	  • Параметры расписания запуска задачи.
	Срок хранения результатов выполнения задачи на Сервере администрирования		

Задача поиска IOC, созданная в Central Node	Управление не предусмотрено.	Загрузка IOC-файлов, настройка расписания IOC-проверки.	Управление не предусмотрено.

kaspersky

Сканирование YARA

Этот раздел содержит информацию о сканировании YARA и о настройке параметров сканирования.

В этом разделе

О сканировании YARA в Kaspersky Endpoint Agent

Сканирование YARA – это процесс, в ходе выполнения которого Kaspersky Endpoint Agent использует YARA-файлы (файлы описания сигнатур открытого стандарта YARA) для поиска сигнатур вредоносной активности на устройствах. Сканирование выполняется рекурсивно на локальных дисках. Сканирование сетевых, подключаемых и облачных ресурсов не поддерживается.

Kaspersky Endpoint Agent поддерживает следующие типы сканирования YARA:

- *Сканирование по YARA-файлам с помощью командной строки* – групповые или локальные задачи, которые создаются и настраиваются через интерфейс командной строки. Для запуска задач используются YARA-файлы, подготовленные пользователем.
- *Сканирование по YARA-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform* – пользователи программы могут использовать YARA-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки компьютеров с установленным компонентом Kaspersky Endpoint Agent.

Типы сканирования отличаются возможностями управления и доступными для настройки параметрами. Описание каждого типа сканирования YARA представлено в следующей таблице.

Таблица 9. Типы сканирования YARA

Тип сканирования	Описание
Сканирование по YARA-файлам с помощью командной строки	Сканирование запускается вручную через интерфейс командной строки, без интеграции со сторонними системами. Для запуска сканирования используются YARA-файлы, подготовленные пользователем. Параметры сканирования не зависят от настроек в параметрах политик. Результаты сканирования доступны немедленно после завершения сканирования в командной строке.
Сканирование YARA по YARA-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform	YARA-файлы загружаются вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Также есть возможность настроить расписание YARA-сканирования компьютеров с программой Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Управление сканированием через командную строку не предусмотрено. Автоматических действий при срабатывании YARA-правил не предусмотрено. Параметры сканирования не зависят от политик Kaspersky Endpoint Agent. Подробную информацию об этом типе сканирования см. в *Справке Kaspersky Anti Targeted Attack Platform*.

Требования к YARA-файлам

При сканировании YARA учитывайте следующие требования и ограничения, связанные с YARA-файлами:

- Kaspersky Endpoint Agent поддерживает YARA-файлы с расширением `yara` и `yar` открытого стандарта описания индикаторов компрометации YARA версии 4.0.2.
- В задаче сканирования YARA можно указать только файл с YARA-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи сканирования YARA.
- Если при сканировании вы загрузите YARA-файлы, которые не поддерживаются Kaspersky Endpoint Agent или содержат синтаксические ошибки, запуск сканирования будет прерван с соответствующим уведомлением об ошибке.
- Идентификаторы всех YARA-файлов, которые используются в одной задаче сканирования YARA, должны быть уникальными. Наличие YARA-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

Мы рекомендуем создавать по одному правилу в одном YARA-файле. Такой подход облегчает чтение результатов сканирования.

kaspersky

Управление сканированием YARA в Kaspersky Endpoint Agent

Вы можете управлять сканированием YARA через интерфейс командной строки Kaspersky Endpoint Agent.

В интерфейсе командной строки доступны следующие действия:

- Сканирование файлов и процессов по YARA-правилам и просмотр данных о выполнении сканирования (см. раздел "Управление сканированием файлов и процессов по YARA-правилам" на стр. 265).
- Сканирование объектов точек автозапуска по YARA-правилам и просмотр данных о выполнении сканирования (see section "Управление сканированием объектов точек автозапуска по YARA-правилам" on page 272).

Аудит безопасности

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Задачи аудита безопасности – это групповые и локальные задачи поиска уязвимостей на устройствах и оценки соответствия устройств стандартам операционных систем. Для выполнения задачи аудита безопасности Kaspersky Endpoint Agent использует поставляемые с продуктом или пользовательские базы правил, помещенные в XML-файлы:

- Для поиска уязвимостей на устройствах программа использует правила, написанные на языке OVAL.
- Для оценки безопасности устройств и соответствия стандартам для операционных систем программа использует конфигурации правил, написанные на языках OVAL и XCCDF.

Доступны следующие возможности управления:

- Управление задачами аудита безопасности через Kaspersky Security Center (см. раздел "Управление задачами аудита безопасности" на стр. 220).
- Управление задачами аудита безопасности через интерфейс командной строки (см. раздел "Настройка и запуск задачи аудита безопасности" на стр. 258).

В этом разделе

kaspersky

Ограничения для параметров задачи аудита безопасности

При создании и настройке задачи аудита безопасности учитывайте следующие ограничения:

- Совокупное ограничение в 2 МБ на совокупный размер файлов, использующихся при выборе источника **Пользовательская база правил из файла**.
- Ограничение на размер отчета о результатах выполнения задачи аудита безопасности – 7,5 МБ.

Поддерживаемые типы проверки OVAL

Для выполнения задачи аудита безопасности поддерживаются следующие типы OVAL-проверок:

- accesstoken;
- auditeventpolicy;
- auditeventpolicysubcategories;
- cmdlet - доступно для Windows XP / Server 2003 и выше;
- environmentvariable58;
- environmentvariable;
- family;
- file;
- filehash58;
- filehash;
- group_sid;
- interface;
- lockoutpolicy;
- passwordpolicy;
- port;
- process58;
- process;
- registry;
- rpmverifyfile;
- service;
- sid;
- textfilecontent54;
- user;
- user_sid;
- variable;
- wmi57;

- wmi;
- xmlfilecontent.

Для неподдерживаемых типов OVAL-проверок результат выполнения задачи аудита безопасности – *Неизвестен*.

Работа с карточкой инцидента

Карточка инцидента автоматически удаляется через один месяц после того, как была сформирована.

В карточке инцидента вы можете ознакомиться с информацией, необходимой для анализа инцидента, а также выполнить действия в качестве реакции на инцидент.

В карточке инцидента (см. раздел «Просмотр карточки инцидента» на стр. 116) приведена следующая информация:

- Общая информация об инциденте.
- Информация о защищаемом устройстве, на котором произошел инцидент.
- Сведения об объекте, обнаруженном в ходе инцидента.

Из карточки инцидента вы можете выполнить следующие действия:

- Изолировать устройство, на котором произошел инцидент (см. раздел "Изоляция устройства из карточки инцидента" на стр. 117).
- Поместить файл на карантин (см. раздел "Выбор действия с файлом из карточки инцидента" на стр. 116).
- Запретить запуск файла, обнаруженного в ходе инцидента (см. раздел "Выбор действия с файлом из карточки инцидента" на стр. 116).
- Создать задачу Поиск IOC (см. раздел "Создание задачи Поиск IOC из карточки инцидента" на стр. 117).

Вы также можете воспользоваться функционалом для работы с недоверенными объектами, который доступен в программах Endpoint Protection Platform. Например, вы можете использовать стандартные средства Kaspersky Security Center Web Console, чтобы добавить файл в список разрешенных объектов Контроля запуска программ Kaspersky Endpoint Security для Windows или отправить файл на анализ специалистам "Лаборатории Касперского". Подробнее см. в *справке Kaspersky Endpoint Security для Windows*.

Настройка отчета об угрозах для просмотра карточек инцидентов

► *Чтобы настроить отчет об угрозах для просмотра карточек инцидентов:*

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на имя отчета **Отчет об угрозах**.
3. В открывшемся окне изменения отчета перейдите на закладку **Графы**.
4. Убедитесь, что в блоке параметров **Детальные данные** в списке полей отчета присутствует поле с именем **Открыть инцидент**.
5. Если поле **Открыть инцидент** отсутствует в списке, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.
   b. В правой части окна в раскрывающемся списке выберите поле с именем **Открыть инцидент**.
   c. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

Просмотр карточки инцидента настроен в параметрах отчета об угрозах.

Предусловия построения цепочки развития угрозы

Необходимо выполнение следующих предусловий для построения цепочки развития угрозы:

- На управляемом устройстве с установленным Kaspersky Endpoint Agent установлена совместимая версия Endpoint Protection Platform (Kaspersky Security for Windows Server версии 11 или выше или Kaspersky Security для виртуальных сред Легкий агент).
- Kaspersky Endpoint Agent активирован ключом Kaspersky EDR Optimum.
- Kaspersky Endpoint Agent и Endpoint Protection Platform находятся под управлением веб-консоли Kaspersky Security Center.
- На устройстве с установленной веб-консолью Kaspersky Security Center установлен веб-плагин Kaspersky Endpoint Agent.
- К устройству применена активная политика, в свойствах которой включено построение цепочки развития угрозы (см. раздел "Настройка построения цепочки развития угрозы" на стр. 203) и принудительное применение этих параметров.

  Если к управляемому устройству не применяется политика, необходимо включить построение цепочки развития угрозы в свойствах программы (см. раздел "Настройка построения цепочки развития угрозы" на стр. 203).

  По умолчанию построение цепочки развития угрозы выключено в свойствах программы для управляемого устройства.

kaspersky

Просмотр карточки инцидента

Карточка инцидента доступна в окне со списком инцидентов. Список инцидентов доступен в отчете **Отчет об угрозах** или в подразделе **Оповещения** в разделе **Мониторинг и отчеты** веб-консоли Kaspersky Security Center или Kaspersky Security Center Cloud Console.

Чтобы программа строила цепочку развития угрозы, необходимо выполнить предусловия построения цепочки развития угрозы (на стр. 115).

Если вы добавите лицензионный ключ для EDR Optimum, подраздел **Оповещения** автоматически отобразится в главном меню в разделе **Мониторинг и отчеты**. Вы также можете настроить отображение подраздела **Оповещения** в свойствах интерфейса в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console. Подробную информацию см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть карточку инцидента в подразделе Оповещения:*

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Оповещения**.
2. Выберите инцидент и нажмите на ссылку **больше информации**.

Отобразится карточка инцидента.

► *Чтобы просмотреть карточку инцидента в отчете об угрозах:*

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Выберите отчет типа **Отчет об угрозах** и нажмите на кнопку **Показать отчет**.
3. В окне отчета на вкладке **Подробнее** выберите инцидент и нажмите на ссылку **Представить**.

Отобразится карточка инцидента.

Выбор действия с файлом из карточки инцидента

Для выполнения правил Запрета запуска на устройстве, на котором произошел инцидент, к этому устройству должна быть применена активная политика Kaspersky Endpoint Agent. Если устройство, на котором произошел инцидент, не находится под управлением активной политики, то правило запрета запуска не будет создано.

► *Чтобы выбрать действие с файлом из карточки инцидента:*

1. Откройте карточку инцидента (см. раздел "Просмотр карточки инцидента" на стр. 116).
2. Если вы хотите поместить на карантин (см. раздел "О карантине Kaspersky Endpoint Agent" на стр. 147) файл, обнаруженный в ходе инцидента, в блоке **Файл** нажмите на кнопку **Поместить на карантин**.
3. Если вы хотите запретить запуск файла (см. раздел "О Запрете запуска" на стр. 97), обнаруженного в ходе инцидента, в блоке **Файл** нажмите на кнопку **Запретить запуск**.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.

Изоляция устройства из карточки инцидента

► *Чтобы изолировать устройство из карточки инцидента:*

1. Откройте карточку инцидента (см. раздел "Просмотр карточки инцидента" на стр. 116).
2. Если вы хотите изолировать устройство (см. раздел "О сетевой изоляции в Kaspersky Endpoint Agent" на стр. 94), на котором произошел инцидент, в блоке **Устройство** нажмите на кнопку **Изолировать устройство от сети**.

Создание задачи Поиск IOC из карточки инцидента

► *Чтобы создать задачу Поиск IOC (см. раздел "О задачах поиска IOC в Kaspersky Endpoint Agent" на стр. 101) из карточки инцидента:*

1. Откройте карточку инцидента (см. раздел "Просмотр карточки инцидента" на стр. 116).
2. На закладке **Все события инцидента** выберите элементы списка, на основе которых вы хотите создать задачу поиска IOC.
3. Нажмите на кнопку **Создание задачи поиска IOC**.
4. Выполните одно из следующих действий:
   - Если вы хотите, чтобы индикатор компрометации срабатывал при обнаружении любого из выбранных объектов, в правой части экрана выберите **ИЛИ (любой IOC обнаружен)**.
   - Если вы хотите, чтобы индикатор компрометации срабатывал только при обнаружении всех выбранных объектов, в правой части экрана выберите **И (все IOC обнаружены)**.

5. В группе параметров **Действия при обнаружении IOC** выберите одно из следующих действий:
   - **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.
   - **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.
   - **Дать команду Endpoint Protection Platform на проверку важных областей**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружен индикатор компрометации.
6. Нажмите на кнопку **Создать задачу**.

По умолчанию для задач поиска IOC, созданных из карточки инцидента, используются параметры, описанные в таблице ниже. Вы можете изменять эти значения в параметрах созданной задачи.

Таблица 10. Параметры по умолчанию для задачи Поиск IOC, созданной из карточки инцидента

Параметр	Значение по умолчанию	Описание
Параметры на закладке Расписание		
Запускать по расписанию	Опция выбрана.	Задача запускается по расписанию, с заданными параметрами.
Периодичность	**В указанное время**	Задача запускается один раз в указанные дату и время.
Время запуска	Через 15 минут после создания задачи.	Задача запускается в указанное время.
Дата запуска	Дата создания задачи.	Задача запускается в указанную дату.
Завершать задачу, выполняющуюся более	Опция выбрана. Задано значение в 1 час.	Программа завершает задачу через указанное время после запуска вне зависимости от прогресса выполнения задачи.
Отменить расписание с	Опция *не* выбрана.	Автоматическая отмена расписания запуска задачи не применяется.
Запускать пропущенные задачи	Опция выбрана.	Программа перезапускает задачу, которая не была запущена по расписанию по какой-то причине. Например, если служба Kaspersky Endpoint Agent не выполнялась в запланированный момент запуска задачи.

Параметр	Значение по умолчанию	Описание
Параметры в разделе Дополнительно		
Выберите типы данных (IOC-документы) для анализа во время поиска IOC	При анализе данных файлов (FileItem) выбрана опция **Анализировать данные файлов (FileItem)**. В дополнительных настройках IOC-документа в блоке параметров **Искать индикаторы компрометации в следующих областях** выбрана опция **Важные области на устройстве**.	Программа проверяет критические области на устройстве, а также папку, в которой изначально был обнаружен опасный объект. К критическим областям относятся следующие: • Временные файлы в папках системных и пользовательских учетных записей. • Временные файлы в папке операционной системы и в папке %TEMP% для учетной записи Local System, если эти пути отличаются.
	При анализе данных реестра Windows (RegistryItem) выбрана опция **Анализировать реестр Windows (RegistryItem)**.	Программа проверяет пути пользовательских разделов реестра.

Kaspersky Endpoint Agent версии 3.9 по умолчанию для задач поиска IOC, созданных из карточки инцидента, использует параметры, заданные в разделе **Интеграция с Kaspersky Sandbox** в блоке параметров **Реагирование на угрозы**. Подробную информацию см. в *Справке Kaspersky Sandbox*.

О виджете EDR-оповещений

В виджете EDR-оповещений отображается информация о количестве инцидентов, обнаруженных на устройствах за последний месяц. Виджет EDR-оповещений доступен для отображения на закладке **Панель мониторинга** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console. Из виджета EDR-оповещений вы можете открыть раздел **Оповещения** со списком инцидентов, обнаруженных на устройствах.

► *Чтобы добавить виджет EDR-оповещений на информационную панель:*

1. Перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.

3. В списке доступных веб-виджетов выберите веб-виджет **Оповещения** в категории **Статистика угроз**.
4. Нажмите на кнопку **Добавить**.

Веб-виджет будет добавлен в конец информационной панели.

Об интеграции с Kaspersky Industrial CyberSecurity for Networks

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

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

Программа Kaspersky Endpoint Agent позволяет настроить интеграцию между Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes. Программа Kaspersky Endpoint Agent устанавливается на отдельные устройства с установленной программой Kaspersky Industrial CyberSecurity for Nodes. Данные о событиях на устройстве, полученные программой Kaspersky Industrial CyberSecurity for Nodes, отправляются на сервер Kaspersky Industrial CyberSecurity for Networks посредством Kaspersky Endpoint Agent. Интеграция между программами расширяет возможности Kaspersky Industrial CyberSecurity for Networks по расследованию и реагированию на угрозы в сетях промышленных предприятий.

Вы можете настроить интеграцию Kaspersky Endpoint Agent с программой Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования Kaspersky Security Center, в Kaspersky Security Center Web Console или через интерфейс командной строки локально на устройстве.

Полную информацию о программе Kaspersky Industrial CyberSecurity for Networks, а также информацию о настройке интеграции с Kaspersky Endpoint Agent со стороны программы Kaspersky Industrial CyberSecurity for Networks см. в *Справке Kaspersky Industrial CyberSecurity for Networks*.

Об интеграции с SIEM

Для настройки интеграции Kaspersky Endpoint Agent с SIEM и отправки телеметрии в адрес SIEM-серверов требуется активный лицензионный ключ Kaspersky Endpoint Agent с лицензионным объектом XDR Telemetry.

SIEM – система управления информацией о безопасности и событиями безопасности в ИТ-инфраструктуре организации. SIEM-система позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Интеграция с SIEM подразумевает, что программа Kaspersky Endpoint Agent, установленная на компьютерах под управлением операционных систем Windows, входящих в IT-инфраструктуру организации, осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет на SIEM-сервер данные о событиях на компьютерах (см. раздел "Данные, предоставляемые SIEM-серверам" на стр. 91). В том числе данные, которые Kaspersky Endpoint Agent получает от Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Об интеграции с Kaspersky Industrial CyberSecurity for Networks" на стр. 120).

Вы можете настроить интеграцию Kaspersky Endpoint Agent с SIEM в Консоли администрирования Kaspersky Security Center (см. раздел "Настройка интеграции Kaspersky Endpoint Agent с SIEM" на стр. 139), в Kaspersky Security Center Web Console (см. раздел "Настройка интеграции Kaspersky Endpoint Agent с SIEM" на стр. 188) или через интерфейс командной строки (см. раздел "Управление параметрами интеграции с SIEM" на стр. 283) локально на устройстве.

kaspersky

Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы. В Kaspersky Security Center предусмотрено разграничение прав доступа к Kaspersky Endpoint Agent, реализованное на основе технологии управления доступом на основе ролей (Role Based Access Control, RBAC).

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Консоль администрирования Kaspersky Security Center (далее также *Консоль администрирования*) предоставляет пользовательский интерфейс для работы с Kaspersky Security Center. Консоль администрирования реализована в виде компонента расширения к Консоли управления (Microsoft Management Console, MMC).

Вы можете управлять Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center с помощью плагина управления Kaspersky Endpoint Agent (см. раздел "Установка и обновление плагина управления Kaspersky Endpoint Agent" на стр. 63).

Далее в разделе приведена основная информация об управлении Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center.

В этом разделе

Управление политиками Kaspersky Endpoint Agent

В этом разделе приведены инструкции по созданию политик Kaspersky Endpoint Agent и включению параметров в политиках.

В этом разделе

Создание политики Kaspersky Endpoint Agent

► *Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Нажмите на кнопку **Создать политику**.

   Запустится мастер создания политики.
4. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Endpoint Agent.
5. Нажмите на кнопку **Далее**.
6. В окне **Ввод названия групповой политики** выполните следующие действия:
   a. Введите имя, под которым создаваемая политика будет отображаться в списке политик.
   b. Если вы хотите импортировать параметры существующей политики Kaspersky Endpoint Agent в новую политику:
      1. Установите флажок **Использовать параметры политики для предыдущей версии программы**.
      2. Нажмите на кнопку **Выбрать** и в открывшемся окне выберите политику, параметры которой требуется импортировать.
      3. Нажмите на кнопку **ОК**.
   c. Нажмите на кнопку **Далее**.
7. В окне **Создать политику** выберите один из следующих вариантов:
   - **Создать новую политику и настроить параметры**.
   - **Создать новую политику с параметрами по умолчанию**.

   > Если на предыдущем шаге вы включили параметр **Использовать параметры политики для предыдущей версии программы**, то по умолчанию выбирается вариант **Создать новую политику и настроить параметры**, а в процессе создания политики отображаются параметры, заданные в импортируемой политике. В этом случае положение переключателя применения политики в правом верхнем углу каждого из разделов с параметрами зависит от положения переключателей в блоках параметров импортируемой политики.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбрать тип политики** выберите необходимый способ развертывания Kaspersky Endpoint Agent:
   - **Интеграция с Kaspersky Sandbox**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks**
10. Нажмите на кнопку **Далее**.

11. Если вы выбрали вариант **Создать новую политику и настроить параметры**, выполните одно из следующих действий во всех последовательно отображающихся окнах с параметрами:
    - Чтобы настроить параметры программы из отображаемых разделов во время создания политики:
        a. Нажмите на кнопку **Настроить** рядом с названием необходимого раздела.
        b. В открывшемся окне настройте необходимые параметры и нажмите на кнопку **ОК.**
        c. Нажмите на кнопку **Далее**.
    - Чтобы настроить параметры программы из отображаемых разделов позднее, нажмите на кнопку **Далее**.

    Настройка параметров программы состоит из следующих этапов:

    > Состав этапов зависит от выбранного на предыдущем шаге типа политики и может отличаться от приведенного ниже.

    - Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.
    - Настройка интеграции Kaspersky Endpoint Agent с компонентами Endpoint Detection and Response Expert (KATA EDR) и Kaspersky Industrial CyberSecurity for Networks (KICKS for Networks).
    - Настройка параметров реагирования на угрозы.
    - Настройка репозиториев программы.
    - Настройка параметров безопасности программы.
    - Настройка общих параметров программы.
12. В окне **Целевая группа** выберите группу администрирования Kaspersky Security Center, на которую должна распространяться создаваемая политика, выполнив следующие действия:
    a. Нажмите на кнопку **Обзор**.

       Откроется окно выбора группы администрирования.
    b. Выберите группу администрирования в списке.

       Например, вы можете выбрать группу **Управляемые устройства**.
    c. Если вы хотите создать подгруппу устройств в группе **Управляемые устройства**:
        1. Нажмите на кнопку **Новая группа**.
        2. В открывшемся окне введите имя подгруппы устройств.
        3. Нажмите на кнопку **ОК**.
    d. Нажмите на кнопку **Далее**.
13. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:
    - **Активная политика**, чтобы политика начала действовать сразу после создания.
    - **Неактивная политика**, чтобы активировать политику позже.

- **Политика для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организаций.

14. Установите флажок **Открыть свойства политики сразу после создания**, если требуется выполнить дополнительную настройку политики сразу после ее создания.
15. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик.

Если в политике включено использование KSN и версия Положения о KSN в политике отличается от версии Положения о KSN в Kaspersky Endpoint Agent, установленном на хосте, то после применения политики использование KSN выключается на хосте и в параметрах политики. Такая ситуация может возникнуть, если на хосте установлен Kaspersky Endpoint Agent 3.16, а версия плагина управления Kaspersky Endpoint Agent, с помощью которого политика была последний раз изменена, ниже.

Включение параметров в политике Kaspersky Endpoint Agent

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите. Параметры в разделах политики разделены на блоки. В рамках одной политики вы можете включить как часть блоков, так и все блоки.

► *Чтобы включить блок параметров в политике Kaspersky Endpoint Agent:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. Выберите политику, для которой вы хотите включить параметры.
5. В открывшемся окне выберите раздел и блок параметров, к которым относятся нужные параметры.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

Все параметры блока будут применяться в политике после сохранения изменений.

Если в политике включено использование KSN и версия Положения о KSN в политике отличается от версии Положения о KSN в Kaspersky Endpoint Agent, установленном на хосте, то после применения политики использование KSN выключается на хосте и в параметрах политики. Такая ситуация может возникнуть, если на хосте установлен Kaspersky Endpoint Agent 3.16, а версия плагина управления Kaspersky Endpoint Agent, с помощью которого политика была последний раз изменена, ниже.

kaspersky

Настройка параметров Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров Kaspersky Endpoint Agent.

В этом разделе

Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера

Если программа работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения для отдельного компьютера.

► *Чтобы перейти к параметрам локальной задачи для отдельного компьютера:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - в контекстном меню на имени защищаемого устройства выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. Перейдите в раздел **Задачи**.

6. В списке задач выберите локальную задачу, параметры которой требуется настроить, одним из следующих способов:

   - двойным щелчком мыши на названии задачи;
   - выберите задачу в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи>**.

► *Чтобы перейти к общим параметрам программы для отдельного компьютера:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемое устройство.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:

   - двойным щелчком мыши на имени защищаемого устройства;
   - в контекстном меню на имени защищаемого устройства выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
4. Перейдите в раздел **Программы**.
5. В списке установленных программ выберите Kaspersky Endpoint Agent одним из следующих способов:

   - двойным щелчком мыши на имени Kaspersky Endpoint Agent;
   - выберите Kaspersky Endpoint Agent в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени Kaspersky Endpoint Agent выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Endpoint Agent**.

kaspersky

Настройка параметров безопасности Kaspersky Endpoint Agent

Для обеспечения максимального уровня безопасности IT-инфраструктуры организации вы можете настроить доступ пользователей и сторонних процессов к Kaspersky Endpoint Agent.

В этом разделе

Настройка прав пользователей

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

► *Чтобы настроить права пользователей:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Права пользователей** нажмите на кнопку **Настроить** рядом с названием нужного параметра.

   Откроется окно разрешений для группы Kaspersky Endpoint Agent.
6. В верхнем блоке параметров групп или пользователей выберите группу или пользователя, которому вы хотите предоставить права.
7. В нижнем блоке параметров разрешений для групп или пользователей установите флажки в строках с требуемыми правами.
8. Нажмите на кнопку **OK**.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
10. В окне свойств политики нажмите на кнопку **OK**.

Права пользователей на управление параметрами и службами программы настроены и применены.

Включение защиты паролем

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности устройства. Защита паролем позволяет ограничить доступ пользователей к программе.

► *Чтобы включить защиту паролем:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.
6. Задайте пароль и подтвердите его.

   Мы рекомендуем задать пароль, который удовлетворяет следующим условиям:
   - Длина пароля составляет не менее 8 символов.
   - Пароль не содержит имя учетной записи пользователя.
   - Пароль не совпадает с именем устройства, на котором установлена программа Kaspersky Endpoint Agent.
   - Пароль содержит символы как минимум трех групп из следующего списка:
     - верхний регистр (A-Z);
     - нижний регистр (a-z);
     - цифры (0-9);
     - специальные символы (!$#%).

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопку **OK**.

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Программа не проверяет надежность заданного пароля. Мы рекомендуем использовать сторонние средства для проверки надежности пароля. Пароль считается надежным, если по результатам проверки подтверждена невозможность подбора пароля минимум за 6 месяцев.
Программа не блокирует возможность ввода пароля после множества попыток ввода некорректного пароля.

Включение и отключение механизма самозащиты

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован механизм самозащиты. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

► *Чтобы включить или отключить механизм самозащиты:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Самозащита** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.

   По умолчанию параметр включен.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Механизм самозащиты будет включен или отключен.

kaspersky

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

Программа использует параметры соединения с прокси-сервером для обновления баз, активации программы и работы внешних служб.

Если вы хотите использовать заданный прокси-сервер при соединении с сервером KATA, Kaspersky Sandbox и Kaspersky Industrial CyberSecurity for Networks, убедитесь, что выбрана опция **Подключаться через прокси-сервер, если это задано в общих параметрах** при настройке интеграции с KATA, Kaspersky Industrial CyberSecurity for Networks или Kaspersky Sandbox. По умолчанию опция не выбрана.

► *Чтобы настроить параметры соединения с прокси-сервером:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** выберите подраздел **Общие параметры**.
5. Выберите один из следующих вариантов использования прокси-сервера:
   - **Не использовать прокси-сервер**.
   - **Автоматически определять адрес прокси-сервера.**
   - **Использовать прокси-сервер с указанными параметрами**.
6. Если вы выбрали вариант **Автоматически определять адрес прокси-сервера**, прокси-сервер определяется автоматически для дальнейшей передачи телеметрии.
7. Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

   По умолчанию используется порт 8080.
8. Если вы хотите использовать NTLM-аутентификацию (протокол сетевой аутентификации NT LAN Manager) при подключении к прокси-серверу:
   a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.
   b. В поле **Имя пользователя** введите имя пользователя из учетной записи, которая будет использоваться для авторизации на прокси-сервере.

c. В поле **Пароль** введите пароль подключения к прокси-серверу.

Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

9. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.
10. Нажмите на кнопку **Применить**.

При этом вы вернетесь в окно свойств политики.

11. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
12. Нажмите на кнопку **ОК**.

Параметры соединения с прокси-сервером настроены.

Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent

► *Чтобы включить использование Kaspersky Security Center в качестве прокси-сервера для активации программы:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** выберите подраздел **Общие параметры**.
5. В блоке параметров **Лицензирование** установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **ОК**.

Включено использование Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent.

kaspersky

Настройка параметров сетевой изоляции

В этом разделе приведены инструкции по настройке параметров сетевой изоляции (см. раздел "Сетевая изоляция" на стр. 94) с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Включение и отключение сетевой изоляции

► *Чтобы включить или отключить сетевую изоляцию устройства:*

1. Откройте окно свойств программы для отдельного устройства.
2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Изолировать устройство** включите или выключите параметр **Изолировать данное устройство от сети**.
4. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Включение и отключение сетевой изоляции вручную для группы устройств через политику недоступно.

Включение и отключение уведомления пользователя о сетевой изоляции

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы включить или отключить уведомление пользователя о сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
7. В разделе **Сетевая изоляция** выберите **Общие параметры**.
8. В блоке параметров **Уведомление** включите или выключите параметр **Уведомить пользователя, когда его устройство будет изолировано**.
9. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Настройка автоматического отключения сетевой изоляции

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы настроить параметры автоматического отключения сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Условия изоляции устройства** включите или выключите параметр **Автоматически прекращать изоляцию устройства по истечении**, чтобы включить или выключить функцию автоматического отключения сетевой изоляции по истечении заданного периода времени.
   - По умолчанию функция включена.
4. Задайте период, по истечении которого сетевая изоляция должна быть отключена.

   По умолчанию задан период в 30 минут.
5. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Если в параметрах сетевой изоляции не установлен флажок **Автоматически прекращать изоляцию устройства по истечении** и не указан период времени, сетевая изоляция будет отключена автоматически через пять часов с момента включения.

См. также

Настройка исключений из сетевой изоляции

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применяются, только если сетевая изоляция включена вручную.
Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства, так как сценарии применения этих параметров разные.

► *Чтобы настроить параметры исключения из сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. Если вы открыли окно свойств программы для отдельного устройства, то в разделе **Сетевая изоляция** выберите **Исключения**.
3. Если вы открыли окно свойств политики программы, то в разделе **Сетевая изоляция** выберите **Изоляция при обнаружении**.
4. Вы можете выполнить следующие действия:
   - Добавить пользовательское исключение
   - Добавить исключения из списка стандартных сетевых профилей
   - Изменить параметры добавленного исключения
   - Включить или отключить использование исключения
   - Удалить исключение из списка
5. Чтобы сохранить изменения, нажмите на кнопку **Применить**.

kaspersky

Настройка общих параметров интеграции с серверами сбора телеметрии

В этом разделе содержится информация о том, как настроить общие параметры интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks с помощью Консоли администрирования Kaspersky Security Center.

В этом разделе

Настройка параметров передачи данных

► *Чтобы настроить параметры передачи данных:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
5. В блоке параметров **Параметры передачи данных** выполните следующие действия:
   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.

     По умолчанию задано 30 секунд.
   - Укажите значения в поле **Максимальное количество событий в одном пакете**.

     По умолчанию задано 1024 событий в одном пакете.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

kaspersky

Настройка параметров регулирования количества запросов

Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node. Степень важности событий программа оценивает самостоятельно.

► *Чтобы настроить параметры регулирования количества запросов:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
5. В блоке параметров **Регулирование количества запросов** вы можете выполнить следующие действия:
   - Включить или выключить параметр **Включить регулирование количества запросов**.

     По умолчанию параметр включен.
   - Указать количество событий в поле **Максимальное количество событий в час**.

     Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить указанную в этом поле величину. По умолчанию задано 3000 событий в час.
   - Указать порог потока однотипных событий низкой важности в поле **Процент превышения лимита событий**.

     Если поток однотипных событий низкой важности превысит указанный в этом поле порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5% до 100%. По умолчанию задано 15%.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

   По умолчанию переключатель находится в положении **Политика применяется**.
7. Нажмите на кнопку **OK**.

Выбор источника параметров Сетевой изоляции

► *Чтобы выбрать источник параметров Сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В разделе **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
3. В блоке **Источник параметров Сетевой изоляции** в раскрывающемся списке **Приоритетный сервер** выберите сервер, который будет источником параметров Сетевой изоляции. Kaspersky Endpoint Agent применяет параметры Сетевой изоляции по следующим правилам:
   - Если настроена интеграция только с сервером KATA, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции, определенные на сервере с установленным KATA Central Node.
   - Если настроена интеграция только с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции, определенные на сервере с установленным KICS for Networks.
   - Если настроена интеграция и с сервером KATA, и с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции, определенные на сервере, выбранном в раскрывающемся списке **Приоритетный сервер**.
   - Если интеграция с сервером KATA и сервером KICS for Networks не настроена, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции, определенные локально на узле с установленным Kaspersky Endpoint Agent с помощью командной строки (см. раздел "Управление сетевой изоляцией" на стр. 253) или в свойствах узла в Kaspersky Security Center Web Console.
4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

kaspersky

Настройка интеграции Kaspersky Endpoint Agent с SIEM

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с SIEM-сервером при помощи Консоли администрирования Kaspersky Security Center.

В этом разделе

См. также

Включение интеграции с SIEM

► *Чтобы включить интеграцию с SIEM:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с SIEM**.
5. В блоке **Параметры подключения** с помощью одноименного флажка включите интеграцию с SIEM.
6. В блоке параметров **Список SIEM-серверов** добавьте параметры подключения к одному или нескольким SIEM-серверам:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Свойства сервера**.
   b. В одноименном поле укажите доменное имя или IP-адрес SIEM-сервера.
   c. В поле **Порт** введите порт для подключения к SIEM-серверу.

d. В раскрывающемся списке **Протокол** выберите протокол, с помощью которого осуществляется передача данных между Kaspersky Endpoint Agent и SIEM-сервером.

e. Нажмите на кнопку **Добавить**.

Параметры подключения к SIEM-серверу отобразятся в блоке параметров **Список SIEM-серверов**.

f. Если необходимо, повторите пункты a–e для добавления параметров подключения к другим SIEM-серверам.

Kaspersky Endpoint Agent подключается к первому SIEM-серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму SIEM-серверу и так далее по списку.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопку **OK**.

Интеграция с SIEM будет включена сразу после применения политики.

Настройка защищенного соединения с SIEM-сервером

► *Чтобы настроить доверенное соединение с SIEM-сервером:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с SIEM**.
5. В блоке **Параметры подключения** установите флажок **Использовать TLS-шифрование**, чтобы шифровать передачу данных между Kaspersky Endpoint Agent и SIEM-сервером.
6. Если вы хотите настроить дополнительную защиту подключения с использованием закрепленного TLS-сертификата:
   a. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.
   b. Добавьте TLS-сертификат:
      i. Нажмите на кнопку **Добавить TLS-сертификат**.

      Откроется окно **Добавление TLS-сертификата**.

ii. Выполните одно из следующих действий:

- Нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
- Скопируйте содержимое файла сертификата в поле **Данные TLS-сертификата**.

iii. Нажмите на кнопку **Добавить**.

Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

7. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата:
   a. Нажмите на кнопку **Добавить сертификат клиента**.

      Откроется окно **Защита с помощью сертификата клиента**.

   b. Установите флажок **Защита подключения с помощью сертификата клиента**.
   c. Нажмите на кнопку **Загрузить**.
   d. В открывшемся окне выберите файл формата PFX, в котором в зашифрованном виде хранится сертификат клиента.
   e. Нажмите на кнопку **Открыть**.
   f. В поле **Пароль криптоконтейнера** введите пароль для доступа к PFX-файлу.
   g. Нажмите на кнопку **ОК**.
8. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
9. Нажмите на кнопку **ОК**.

Защищенное соединение с SIEM-сервером настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с SIEM-сервером

► *Чтобы настроить время ожидания ответа от SIEM-сервера:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с SIEM**.

5. В блоке **Параметры подключения** в поле **Время ожидания (сек.)** укажите продолжительность ожидания ответа от SIEM-сервера.

   По истечении указанного времени Kaspersky Endpoint Agent повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию указано значение 10 секунд.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

7. Нажмите на кнопку **OK**.

kaspersky

Настройка параметров EDR-телеметрии

В этом разделе содержится информация о том, как настроить:

- Исключения EDR-телеметрии о процессах программ, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.
- Оптимизацию объема EDR-телеметрии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.
- Исключения EDR-телеметрии о сетевых коммуникациях, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.

См. также

Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ

Вы можете настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ с помощью Консоли администрирования Kaspersky Security Center в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о процессах программ доступны при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные об исключенных процессах программ.

Управление (включение / выключение) оптимизацией объема отправляемой EDR-телеметрии о процессах программ доступно при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Если включена оптимизация объема отправляемой EDR-телеметрии, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe о процессах программ на сервер с установленным Kaspersky Industrial CyberSecurity for Networks.

► *Чтобы включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. Перейдите в раздел **EDR-телеметрия** → **Исключенные процессы**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Настройте оптимизацию объема отправляемой EDR-телеметрии:

   При интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node оптимизация объема отправляемой EDR-телеметрии должна быть всегда включена.

   - Выключите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов.
   - Включите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent не отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов.

   Если параметр **Использовать исключения** выключен, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов вне зависимости от значения параметра **Оптимизировать объем отправляемой телеметрии**.

5. Создайте список исключений:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Свойства правила** настройте параметры исключения.
   c. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Свойства правила**.

      Новое исключение создано и отображается в списке.
   d. Если необходимо экспортировать список исключений в файл формата XML, нажмите на кнопку **Экспорт**.
   e. Если необходимо импортировать список исключений из файла формата XML, нажмите на кнопку **Импорт**.

f. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

g. Если необходимо удалить исключение из списка, выберите исключение и нажмите на кнопку **Удалить**.

6. Если вы настраиваете параметры политики, убедитесь, что переключатель в правом верхнем углу блока параметров находится в активном положении.
7. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях

Вы можете настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях с помощью Консоли администрирования Kaspersky Security Center в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о сетевых коммуникациях применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным Kaspersky Industrial CyberSecurity for Networks данные, подпадающие под параметры исключений.

► *Чтобы включить и настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. Перейдите в раздел **EDR-телеметрия** → **Исключенные сетевые коммуникации**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Создайте список исключений:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Свойства правила** настройте параметры исключения.
   c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.
   d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.
5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.
6. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Включение и настройка исключений отправляемой EDR-телеметрии об операциях с файлами

Вы можете настроить исключения отправляемой EDR-телеметрии об операциях с файлами с помощью Консоли администрирования Kaspersky Security Center в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии об операциях с файлами применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Managed Detection and Response данные, подпадающие под параметры исключений.

► *Чтобы включить и настроить исключения отправляемой EDR-телеметрии об операциях с файлами:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В разделе **EDR-телеметрия** выберите **Исключенные операции с файлами**.

   Откроется окно **Исключенные операции с файлами**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Создайте список исключений:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Свойства правила** настройте параметры исключения.
   c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.
   d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.
5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении.
6. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Настройка параметров хранилищ в Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров карантина и параметров синхронизации данных с Сервером администрирования с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

О карантине Kaspersky Endpoint Agent

Карантин – это специальное локальное хранилище на устройстве. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

По умолчанию локальное хранилище карантина расположено в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Quarantine`. По умолчанию объекты, восстановленные из карантина, хранятся в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Restored`.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на устройствах с программой Kaspersky Endpoint Agent. Агенты администрирования устройств передают информацию о файлах на карантине на Сервер администрирования.

Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования. Все объекты находятся на защищаемых устройствах с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Об управлении карантином в Kaspersky Endpoint Agent

Через Kaspersky Security Center можно настраивать параметры карантина (см. раздел "Настройка параметров хранилищ в Kaspersky Endpoint Agent" на стр. 147), просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина. Подробную информацию об управлении объектами, находящимися на карантине, через Kaspersky Security Center см. в документации Kaspersky Security Center.

kaspersky

Для того чтобы Kaspersky Endpoint Agent отправлял данные об объектах, помещенных на карантин, на Сервер администрирования Kaspersky Security Center, необходимо включить эту опцию (см. раздел "Настройка синхронизации данных с Сервером администрирования" на стр. 149) в параметрах карантина в политике Kaspersky Endpoint Agent. По умолчанию опция включена.

Через интерфейс командной строки на устройстве можно просматривать информацию о параметрах карантина и свойствах объектов, находящихся на карантине (см. раздел "Просмотр информации о параметрах карантина и объектах на карантине" на стр. 242).

Kaspersky Endpoint Agent помещает объект на карантин под системной учетной записью (SYSTEM).

Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя защищаемого устройства.

Настройка параметров карантина и восстановления объектов из карантина

► *Чтобы настроить параметры карантина:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Репозитории** выберите подраздел **Карантин**.
5. В разделе **Параметры Карантина** настройте параметры карантина:
   a. В поле **Папка Карантина** укажите путь, по которому будет создана папка карантина на устройствах, или нажмите на кнопку **Обзор** и выберите путь.

      По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`. **//Что такое %SOYUZAPPDATA%?**

      Почему Endpoint Agent\4.0 - вроде бы версия 3.8? может, лучше написать <версия>?

      Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent. Например, если программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим: C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine.

b. Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер Карантина (МБ)** и укажите или выберите в списке максимальный размер карантина в МБ.

Например, вы можете задать максимальный размер карантина 200 МБ.

При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

c. Чтобы задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

Например, вы можете задать пороговое значение карантина 50 МБ.

При достижении порогового значения карантина, Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

6. В разделе **Восстановление объектов из Карантина** в поле **Папка для восстановленных объектов** укажите путь, по которому будет создана папка для объектов, восстановленных из карантина.

По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent. Например, если программа Kaspersky Endpoint Agent установлена на диске C, путь к папке восстановленных из карантина объектов будет следующим: C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопку **Применить** и затем на кнопку **OK**.

Параметры карантина и папка для восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center. Синхронизация данных нужна для управления карантином через Kaspersky Security Center (см. раздел "Об управлении карантином в Kaspersky Endpoint Agent" на стр. 147).

► *Чтобы настроить синхронизацию данных с Сервером администрирования:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
5. В разделе **Параметры**, в подразделе **Отправлять следующие данные на Сервер администрирования** установите флажок **Данные об объектах в Карантине на управляемых устройствах**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **Применить** и затем на кнопку **OK**.

Синхронизация данных с Сервером администрирования будет настроена.

kaspersky

Настройка диагностики сбоев

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

► *Чтобы настроить диагностику сбоев:*

1. Откройте окно свойств программы для отдельного устройства.
2. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.
3. Если вы хотите включить запись отладочной информации в файлы трассировки:
   a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.
   b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

      Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

   c. В поле **Максимальный размер файла трассировки (МБ)** укажите размер файла в мегабайтах.

      По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.
4. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:
   a. Включите параметр **Перезаписывать старые файлы трассировки**.
   b. В поле **Максимальное количество файлов для одного журнала трассировки** укажите желаемое значение.

      По умолчанию задан 1 файл. Когда достигается указанное количество файлов, программа перезаписывает старые файлы, начиная с самого старого. Указанное ограничение применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение.
5. Если вы хотите включить запись файлов дампа:
   a. Включите параметр **Создавать файлы дампа**.
   b. В поле **Папка файлов дампа** укажите папку для сохранения файлов дампа.

      Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.
6. Нажмите на кнопку **OK**.

Диагностика сбоев настроена и включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы для диагностики сбоев будут создаваться в папках, которые вы указали.

kaspersky

Управление задачами Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами Kaspersky Endpoint Agent.

В этом разделе

Создание локальной задачи

Локальные задачи – это задачи, которые выполняются на конкретном устройстве. Подробнее о задачах см. в документации Kaspersky Security Center.

► *Чтобы создать локальную задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Управляемые устройства**.
3. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит требуемое устройство.
4. В рабочей области выберите закладку **Устройства**.
5. Выберите устройство, для которого вы хотите создать локальную задачу.
6. Выполните одно из следующих действий:
   - В контекстном меню устройства выберите пункт **Все задачи** → **Создать задачу**.
   - В контекстном меню устройства выберите пункт **Свойства** и в открывшемся окне **Свойства: <Название устройства>** на закладке **Задачи** нажмите на кнопку **Добавить**.
   - В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.

   Запустится мастер создания задачи.
7. Выберите нужную задачу и нажмите **Далее**.
8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

Групповые задачи - это задачи, которые выполняются на устройствах выбранной группы администрирования. Подробнее о задачах см. в документации Kaspersky Security Center.

► *Чтобы создать групповую задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех устройств, управляемых с помощью программы Kaspersky Security Center.
   - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят требуемые устройства.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
5. Выберите нужную задачу и нажмите **Далее**.
6. Следуйте указаниям мастера создания задачи.

Просмотр списка задач

► *Чтобы просмотреть список задач на сервере Kaspersky Security Center:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

Отобразится список задач.

Удаление задач из списка

► *Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. В списке задач выберите задачи, которые вы хотите удалить, и правой клавишей мыши откройте контекстное меню.

   Отобразится список действий, которые можно выполнить над задачами.
4. Выберите действие **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Запуск задач вручную

Вы можете запускать созданные задачи вручную. Например, вручную можно запускать задачи, в которых не настроен запуск по расписанию (см. раздел "Запуск задач по расписанию" на стр. 154).

► *Чтобы вручную запустить одну задачу:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В контекстном меню нужной задачи выберите действие **Запустить**.

Задача запустится.

Запуск задач по расписанию

► *Чтобы настроить запуск задачи по расписанию:*

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.
3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:
   c. В списке **Каждый** выберите периодичность запуска задачи. Например, один раз в день или два раза в неделю, по вторникам и четвергам.
   d. В списках **Время** и **Дата** выберите время и дату начала действия расписания.
5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и настройте следующие параметры в окне **Дополнительно**:
   - **Завершать задачи, выполняющиеся более**
   - **Отменить расписание с**
   - **Запускать пропущенные задачи**
   - **Запускать задачу каждые**
6. Нажмите на кнопку **ОК**.

Запуск задач по расписанию настроен и применяется на устройствах.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Вы также можете изменить срок хранения результатов выполнения задач (см. раздел "Изменение срока хранения результатов выполнения задач на Сервере администрирования" на стр. 155).

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

► *Чтобы просмотреть результат выполнения задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. В меню выберите пункт **Результаты**.

Откроется окно **Результат выполнения задачи**.

Изменение срока хранения результатов выполнения задач на Сервере администрирования

По умолчанию результаты выполнения задач хранятся на Сервере администрирования в течение семи дней.

► *Чтобы изменить срок хранения результатов выполнения задач на Сервере администрирования:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел **Уведомление**.
6. Убедитесь, что в разделе **Сохранять информацию о результатах** установлен флажок **На Сервере администрирования в течение (сут)** и укажите, в течение какого времени (в сутках) требуется хранить результат выполнения задачи.
7. Нажмите на кнопку **Применить**, а затем на кнопку **OK**.

Не рекомендуем сокращать срок хранения результатов выполнения задач поиска IOC.

Создание задачи активации Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 75) с помощью файла ключа

► *Чтобы создать задачу активации Kaspersky Endpoint Agent:*

1. Запустите мастер создания задачи **Активация программы** для нужной области действия одним из следующих способов:
   - Запустите мастер создания локальной задачи (см. раздел "Создание задач" на стр. 206).
   - Запустите мастер создания групповой задачи.
2. В окне **Параметры активации** выполните следующие действия:
   a. Выберите **Активировать при помощи файла ключа или ключа** и нажмите на кнопку **Выбрать**.
   b. В раскрывающемся списке выберите нужный способ распространения ключа.
   c. Если вы выбрали **Файл ключа из папки**, в открывшемся окне укажите расположение файла ключа и нажмите на кнопку **Открыть**.
   d. Если вы выбрали **Файл ключа из хранилища Kaspersky Security Center**, в открывшемся окне выберите нужный ключ и нажмите **ОК**.

      Подробная информация о хранилище ключей Kaspersky Security Center приведена в документации Kaspersky Security Center.
3. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.
4. Нажмите на кнопку **Далее**.
5. В окне **Расписание** настройте параметры расписания запуска задачи и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в документации Kaspersky Security Center.
6. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой будет выполняться задача, и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в документации Kaspersky Security Center.
7. В окне **Определение названия задачи** задайте имя задачи и нажмите на кнопку **Далее**.
8. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.
9. Нажмите на кнопку **Завершить**.

Будет создана новая задача активации программы для выбранного устройства или группы устройств.

Управление задачами обновления баз и модулей Kaspersky Endpoint Agent

В этом разделе приведены инструкции, как создать и настроить задачу обновления баз и модулей программы.

kaspersky

В этом разделе

Создание задачи обновления баз и модулей программы

► *Чтобы создать задачу обновления баз и модулей программы Kaspersky Endpoint Agent в Kaspersky Security Center:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите программу, для которой будет создана задача – **Kaspersky Endpoint Agent**, и тип задачи **Обновление баз и модулей программы**.
5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи обновления баз.

Мастер создания задачи обновления баз состоит из следующих шагов:

1. Выбор источника обновления баз
2. Настройка параметров обновления модулей программы
3. Настройка расписания обновления баз
4. Выбор устройств, на которых будет выполняться задача
5. Выбор учетной записи пользователя Kaspersky Security Center, с правами которой будет выполняться задача
6. Указание названия задачи
7. Запуск задачи сразу после создания

Настройка параметров задачи обновления баз и модулей программы

Для поддержания сертифицированного состояния программы запрещается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу программы из сертифицированного состояния.

После создания задачи обновления баз и модулей программы вы можете настроить параметры этой задачи.

► *Чтобы изменить параметры задачи:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Обновление баз и модулей программы** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите настроить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

- Название задачи
- Устройства, на которых будет выполняться задача
- Источник обновления баз
- Настройка дополнительных параметров обновления баз
- Расписание обновления баз
- Учетную запись пользователя Kaspersky Security Center, с правами которой будет выполняться задача
- Срок хранения результатов выполнения задачи на Сервере администрирования

kaspersky

Управление задачами поиска IOC в Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами поиска IOC (см. раздел "О задачах поиска IOC в Kaspersky Endpoint Agent" на стр. 101) в Kaspersky Endpoint Agent с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Управление стандартными задачами поиска IOC

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

В этом разделе приведены инструкции по управлению стандартными задачами поиска IOC.

В этом разделе

Требования к IOC-файлам

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

- Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
- Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.
- Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

В таблице ниже приведены особенности и ограничения поддержки стандарта OpenIOC программой.

Таблица 11. Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0:
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`)

	"string": строка (применимые условия: is, contains, matches, starts-with, ends-with) "duration": продолжительность в секундах (применимые условия: is, greater-than, less-than)
Особенности интерпретации типов данных	Типы данных "boolean string", "restricted string", "md5", "IP", "sha256", "base64Binary" интерпретируются как строка (string). Программа поддерживает интерпретацию параметра Content для типов данных int и date, заданного в виде промежутков: OpenIOC 1.0: С использованием оператора TO в поле Content: <Content type="int">49600 TO 50700</Content> <Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content> <Content type="int">[154192 TO 154192]</Content> OpenIOC 1.1: С помощью условий greater-than и less-than С использованием оператора TO в поле Content Программа поддерживает интерпретацию типов данных date и duration, если индикаторы заданы в формате ISO 8601, Zulu time zone, UTC.
Поддерживаемые IOC-термины	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent:

https://support.kaspersky.com/KEA/3.9/ru-RU/IOC_TERMS.zip

Создание и настройка стандартной задачи поиска IOC

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

► *Чтобы создать и настроить стандартную задачу поиска IOC,*

в зависимости от требуемой области действия задачи выполните одно из следующих действий:

- Запустите мастер создания локальной задачи (см. раздел "Создание задач" на стр. 206).
- Запустите мастер создания групповой задачи.

Мастер создания задачи позволяет настроить следующие параметры:

- IOC-коллекция
- Типы данных (IOC-документы) для анализа во время поиска IOC
- Ретроспективный поиск IOC
- Действия программы при обнаружении IOC
- Расписание запуска задачи
- Учетную запись пользователя Kaspersky Security Center для запуска задачи
- Название задачи

Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.

Настройка параметров стандартной задачи поиска IOC

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

► *Чтобы настроить параметры стандартной задачи поиска IOC:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.

3. Откройте параметры требуемой задачи одним из следующих способов:
   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Название задачи>**.
4. В левой части окна выберите раздел параметров, которые вы хотите настроить.
5. В правой части окна внесите необходимые изменения и нажмите на кнопку **Применить**, а затем на кнопку **OK**.

   Настройка параметров стандартной задачи поиска IOC завершена.

Вы можете настроить следующие параметры задачи:

- Название задачи
- Срок хранения результатов выполнения задачи на Сервере администрирования
- IOC-коллекция
- Ретроспективный поиск IOC
- Действия программы при обнаружении IOC
- Типы данных (IOC-документы) для анализа во время поиска IOC
- Расписание запуска задачи поиска IOC
- Учетная запись пользователя Kaspersky Security Center для запуска задачи
- Исключение групп устройств из области действия задачи

Экспорт IOC-коллекции

► *Чтобы экспортировать IOC-коллекцию:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. Выберите раздел **Параметры поиска IOC**.
6. В разделе **IOC-коллекция** нажмите на кнопку **Экспортировать**.
7. В открывшемся окне задайте имя файла, а также выберите папку, в которую вы хотите его сохранить.
8. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной вами папке.

Просмотр результатов выполнения задачи поиска IOC

► *Чтобы просмотреть результаты выполнения задачи Поиск IOC:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры нужной задачи одним из следующих способов:
   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Имя задачи>**.
4. Выберите раздел **Результаты**.
5. В списке **Показать результаты по устройству** выберите, по каким устройствам вы хотите просмотреть результаты выполнения задач поиска IOC.
6. Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.
7. Чтобы просмотреть подробную информацию об обнаруженном индикаторе компрометации, нажмите на кнопку **Показать карточку**.

   Карточка обнаруженных IOC содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

   Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.

kaspersky

Управление автономными задачами поиска IOC

Автономные задачи поиска IOC – групповые задачи, которые создаются автоматически при реагировании на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Подробнее об автономных задачах поиска IOC см. в *Справке Kaspersky Sandbox*.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

В этом разделе приведены инструкции по настройке параметров автономных задач поиска IOC с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Настройка прав пользователей для управления задачами поиска IOC

Необходимо настроить права пользователя Kaspersky Security Center, учетная запись которого используется для управления задачами поиска IOC.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

► *Чтобы настроить права пользователя Kaspersky Security Center для управления задачами поиска IOC:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите **Сервер администрирования**.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.
4. В левой части окна выберите раздел **Безопасность**.
5. Выберите пользователя Kaspersky Security Center, учетную запись которого вы хотите использовать для управления задачами поиска IOC.

   В нижней части окна отобразится список прав выбранного пользователя, сгруппированных по программам, которыми пользователь может управлять в Kaspersky Security Center.
6. В группе прав **Kaspersky Endpoint Agent** раскройте блок **Предотвращение вторжений**.

7. Для типов прав **Изменение**, **Выполнение** и **Выполнение действий над выборками устройств** установите флажки в столбце **Разрешить**.
8. Нажмите на кнопки **Применить** и **OK**.

   Настройка прав пользователей для управления задачами поиска IOC завершена.

Настройка параметров автономной задачи поиска IOC

► *Чтобы настроить параметры автономной задачи поиска IOC:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите изменить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **OK**.

Вы можете настроить следующие параметры задачи:

- Название задачи
- Срок хранения результатов выполнения задачи на Сервере администрирования
- Действия программы, при обнаружении IOC
- Расписание запуска задач поиска IOC
- Учетная запись пользователя Kaspersky Security Center для запуска задачи
- Исключение групп устройств из области действия задачи

Экспорт IOC-коллекции

► *Чтобы экспортировать IOC-коллекцию:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. Выберите раздел **Параметры поиска IOC**.
6. В разделе **IOC-коллекция** нажмите на кнопку **Экспортировать**.

7. В открывшемся окне задайте имя файла, а также выберите папку, в которую вы хотите его сохранить.
8. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной вами папке.

Просмотр результатов выполнения задачи поиска IOC

► *Чтобы просмотреть результаты выполнения задачи Поиск IOC:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры нужной задачи одним из следующих способов:
   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Имя задачи>**.
4. Выберите раздел **Результаты**.
5. В списке **Показать результаты по устройству** выберите, по каким устройствам вы хотите просмотреть результаты выполнения задач поиска IOC.
6. Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.
7. Чтобы просмотреть подробную информацию об обнаруженном индикаторе компрометации, нажмите на кнопку **Показать карточку**.

   Карточка обнаруженных IOC содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

   Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.

Управление программой с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы. В Kaspersky Security Center предусмотрено разграничение прав доступа к Kaspersky Endpoint Agent, реализованное на основе технологии управления доступом на основе ролей (Role Based Access Control, RBAC).

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Вы управляете Kaspersky Security Center с помощью *Kaspersky Security Center Web Console* (далее также *Web Console*). Web Console представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.

Kaspersky Security Center Cloud Console

В сертифицированной версии программы использование Kaspersky Security Center Cloud Console приводит к выходу программы из безопасного состояния.

Kaspersky *Security Center Cloud Console* – это программа, которая размещается и поддерживается "Лабораторией Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер. Kaspersky Security Center Cloud Console позволяет администратору устанавливать программы безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых программ. Администратор может использовать подробную панель мониторинга, где можно просмотреть моментальные снимки состояния корпоративных устройств, подробные отчеты и детальные параметры политик защиты.

Kaspersky Security Center Cloud Console как и Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы.

Вы управляете Kaspersky Security Center Cloud Console с помощью *облачной Консоли администрирования*, которая представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Security Center Cloud Console.

Подробную информацию о Kaspersky Security Center Cloud Console см. в *Справке Kaspersky Security Center Cloud Console* https://help.kaspersky.com/KSC/CloudConsole/ru-RU/5022.htm.

kaspersky

Управление программой Kaspersky Endpoint Agent

Далее в этом разделе приведены универсальные инструкции по управлению Kaspersky Endpoint Agent, которые пригодны как для управления программой с помощью Kaspersky Security Center Web Console, так и с помощью облачной Консоли администрирования.

Для управления Kaspersky Endpoint Agent через Web Console необходимо установить веб-плагин управления Kaspersky Endpoint Agent (см. раздел "Установка и обновление веб-плагина управления Kaspersky Endpoint Agent" на стр. 64).

В этом разделе

Управление политиками Kaspersky Endpoint Agent

В этом разделе приведены инструкции по созданию политик Kaspersky Endpoint Agent и включению параметров в политиках.

В этом разделе

Создание политики Kaspersky Endpoint Agent

► *Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center Web Console:*

1. В главном окне перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите программу Kaspersky Endpoint Agent и нажмите **Далее**.
4. Выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:
   - **Интеграция с Kaspersky Sandbox;**
   - **Endpoint Detection and Response Optimum;**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks.**

Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.

5. Нажмите **Далее**.
6. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен переключатель **Обеспечить принудительное наследование параметров для дочерних политик**.
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**.
7. На закладке **Параметры программы** вы можете настроить параметры политики Kaspersky Endpoint Agent.
8. Нажмите на кнопку **Сохранить**.

Если в политике включено использование KSN и версия Положения о KSN в политике отличается от версии Положения о KSN в Kaspersky Endpoint Agent, установленном на хосте, то после применения политики использование KSN выключается на хосте и в параметрах политики. Такая ситуация может возникнуть, если на хосте установлен Kaspersky Endpoint Agent 3.16, а версия плагина управления Kaspersky Endpoint Agent, с помощью которого политика была последний раз изменена, ниже.

См. также

Настройка использования KSN в Kaspersky Endpoint Agent.....183

kaspersky

Включение параметров в политике Kaspersky Endpoint Agent

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите.

Включение параметров доступно для блоков, в которых находятся эти параметры. В рамках одной политики вы можете включить как часть блоков параметров, так и все блоки параметров.

► *Чтобы включить блок параметров в политике Kaspersky Endpoint Agent:*

1. Откройте окно свойств политики программы.
2. Выберите раздел и блок параметров, к которым относятся нужные параметры.
3. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

Все параметры блока будут применяться в политике после сохранения изменений.

Если в политике включено использование KSN и версия Положения о KSN в политике отличается от версии Положения о KSN в Kaspersky Endpoint Agent, установленном на хосте, то после применения политики использование KSN выключается на хосте и в параметрах политики. Такая ситуация может возникнуть, если на хосте установлен Kaspersky Endpoint Agent 3.16, а версия плагина управления Kaspersky Endpoint Agent, с помощью которого политика была последний раз изменена, ниже.

kaspersky

Настройка параметров Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров Kaspersky Endpoint Agent.

В этом разделе

Открытие окна параметров Kaspersky Endpoint Agent

► *Чтобы открыть окно параметров политики Kaspersky Endpoint Agent, выполните следующие действия:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел Устройства → Политики и профили политик.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры программы**.

► *Чтобы открыть окно параметров Kaspersky Endpoint Agent для отдельного устройства:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство.
3. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
4. Выберите **Kaspersky Endpoint Agent**.
5. В открывшемся окне выберите вкладку **Параметры программы**.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**, кроме параметров сетевой изоляции.
В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

Настройка параметров безопасности Kaspersky Endpoint Agent

Для обеспечения максимального уровня безопасности IT-инфраструктуры организации вы можете настроить доступ пользователей и сторонних процессов к Kaspersky Endpoint Agent. Для этого предусмотрены следующие возможности:

- Ограничение прав пользователей (см. раздел "Настройка прав пользователей" на стр. 173) на управление параметрами и службами программы.
- Защита действий в программе паролем (см. раздел "Включение защиты паролем" на стр. 174).
- Механизм самозащиты программы (см. раздел "Включение и отключение механизма самозащиты" на стр. 175).

В этом разделе

Настройка прав пользователей

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

► *Чтобы настроить права пользователей:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.

5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
8. В блоке параметров **Права пользователей на управление службами программы** нажмите на кнопку **Настроить** рядом с названием нужного параметра (**Права пользователей на управление программой** или **Настройка прав пользователей на управление программой**).

   Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**.

Включение защиты паролем

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности устройства. Защита паролем позволяет ограничить доступ пользователей к программе.

► *Чтобы включить защиту паролем:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
8. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.
9. Задайте пароль и подтвердите его.

   Рекомендуется задать пароль, который удовлетворяет следующим условиям:
   - Длина пароля должна быть не менее 8 символов.
   - Пароль не должен содержать имени учетной записи пользователя.
   - Пароль не должен совпадать с именем устройства, на котором установлена программа Kaspersky Endpoint Agent.

- Пароль должен содержать символы как минимум трех групп из следующего списка:
  - верхний регистр (A-Z);
  - нижний регистр (a-z);
  - цифры (0-9);
  - специальные символы (!$#%).

10. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
11. Нажмите на кнопку **OK**.
12. Нажмите на кнопку **Сохранить**.

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Программа не проверяет надежность заданного пароля. Рекомендуется использовать сторонние средства для проверки надежности пароля. Пароль считается надежным, если по результатам проверки подтверждена невозможность подбора пароля минимум за 6 месяцев.
Программа не блокирует возможность ввода пароля после множества попыток ввода некорректного пароля.

Включение и отключение механизма самозащиты

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован *механизм самозащиты*. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

► *Чтобы включить или отключить механизм самозащиты:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
8. В блоке параметров **Самозащита** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.

9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

Программа использует параметры соединения с прокси-сервером для обновления баз, активации программы и работы внешних служб.

Если вы хотите **Использовать прокси-сервер с указанными параметрами** при соединении с сервером KATA, Kaspersky Industrial CyberSecurity for Networks или Kaspersky Sandbox, убедитесь, что выбрана опция **Подключаться через прокси-сервер, если это задано в общих параметрах** при настройке интеграции с KATA, Kaspersky Industrial CyberSecurity for Networks или Kaspersky Sandbox. По умолчанию опция не выбрана.

► *Чтобы настроить параметры соединения с прокси-сервером:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
8. Выберите один из следующих вариантов использования прокси-сервера:
   - **Не использовать прокси-сервер**.
   - **Автоматически определять адрес прокси-сервера**.
   - **Использовать прокси-сервер с указанными параметрами**.
9. Если вы выбрали вариант **Автоматически определять адрес прокси-сервера**, прокси-сервер определяется автоматически для дальнейшей передачи телеметрии.

10. Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

    По умолчанию используется порт 8080.

11. Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:

    a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.

    b. В поле **Имя пользователя** введите имя пользователя, учетная запись которого будет использоваться для авторизации на прокси-сервере.

    c. В поле **Пароль** введите пароль подключения к прокси-серверу.

    Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

12. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.
13. Если вы настраиваете свойства политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
14. Нажмите на кнопку **OK**.
15. В окне свойств политики нажмите на кнопку **Сохранить**.

Параметры соединения с прокси-сервером настроены.

Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent

► *Чтобы включить использование Kaspersky Security Center в качестве прокси-сервера для активации программы:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
8. В блоке параметров **Лицензирование** установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопку **OK**.
11. В окне свойств политики нажмите на кнопку **Сохранить**.

Включено использование Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent.

kaspersky

Настройка параметров сетевой изоляции

В этом разделе приведены инструкции по настройке параметров сетевой изоляции (см. раздел "Сетевая изоляция" на стр. 94) с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Включение и отключение сетевой изоляции

► *Чтобы включить или отключить сетевую изоляцию устройства:*

1. Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
7. В разделе **Сетевая изоляция** выберите **Общие параметры**.
8. В блоке параметров **Изолировать устройство** установите или снимите флажок **Изолировать данное устройство от сети**.
9. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Включение и отключение сетевой изоляции вручную для группы устройств через политику недоступно.

Включение и отключение уведомления пользователя о сетевой изоляции

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы включить или отключить уведомление пользователя о сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Сетевая изоляция** выберите **Общие параметры**.
8. В блоке параметров **Уведомление** установите или снимите флажок **Уведомить пользователя, когда его устройство будет изолировано**.
9. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Настройка автоматического отключения сетевой изоляции

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы настроить параметры автоматического отключения сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.

6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Сетевая изоляция** выберите **Общие параметры**.
8. В блоке параметров **Условия изоляции устройства** включите или выключите параметр **Автоматически прекращать изоляцию устройства по истечении**.
9. Задайте период, по истечении которого сетевая изоляция должна быть отключена.

   По умолчанию задан период в 30 минут.
10. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Если в параметрах сетевой изоляции не установлен флажок **Автоматически прекращать изоляцию устройства по истечении** и не указан период времени, сетевая изоляция будет отключена автоматически через пять часов с момента включения.

Настройка исключений из сетевой изоляции

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применяются, только если сетевая изоляция включена вручную.
Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства, так как сценарии применения этих параметров разные.

► *Чтобы настроить параметры исключения из сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. Если вы открыли окно свойств программы для отдельного устройства, то в разделе **Сетевая изоляция** выберите **Исключения**.
8. Если вы открыли окно свойств политики программы, то в разделе **Сетевая изоляция** выберите **Изоляция при обнаружении**.

   Вы можете выполнить следующие действия:
   - Добавить пользовательское исключение
   - Добавить исключения из списка стандартных сетевых профилей

- Изменить параметры добавленного исключения
- Удалить исключение из списка

9. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка типа политики Kaspersky Endpoint Agent

Выбор типа политики Kaspersky Endpoint Agent необходим для того, чтобы состав отображаемых в политике параметров соответствовал выбранному способу развертывания Kaspersky Endpoint Agent.

► *Чтобы настроить тип политики:*

1. Откройте окно свойств политики программы.
2. В разделе **Параметры программы** выберите подраздел **Интерфейс и управление**.
3. В открывшемся окне выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:
   - **Managed Detection and Response**.

     Функциональность включена по умолчанию и ее нельзя исключить.

   - **Интеграция с Kaspersky Sandbox**.
   - **Endpoint Detection and Response Optimum**.
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks**.

   Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.

4. Нажмите на кнопку **ОК**.

Тип политики изменен. В политике доступны параметры для выбранного способа развертывания Kaspersky Endpoint Agent.

kaspersky

Настройка использования KSN в Kaspersky Endpoint Agent

В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Agent использует данные, полученные от пользователей во всем мире. Сеть Kaspersky Security Network предназначена для получения этих данных.

Kaspersky Security Network (далее также KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программы EPP на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Endpoint Agent, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Agent передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. По умолчанию использование KSN отключено. После включения использования KSN, вы можете отключить эту опцию в любой момент времени.

Начиная с версии 3.10 в Kaspersky Endpoint Agent нет возможности настроить использование службы Kaspersky Managed Protection (далее KMP). Если в предыдущей установленной версии Kaspersky Endpoint Agent было включено использование службы KMP, то после обновления программы до версии 3.10 и выше служба KMP продолжает работать. После обновления вы можете отключить службу KMP только при помощи Плагина управления Kaspersky Endpoint Agent или Веб-плагина Kaspersky Endpoint Agent версий ниже 3.10.

► *Чтобы включить или выключить использование KSN:*

1. Выполните одно из следующих действий:

- Откройте окно свойств программы для отдельного устройства.

2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. Ознакомьтесь с условиями Положения о KSN:

   Условия Положения о KSN требуется принять, если вы впервые включаете использование KSN или версия Положения о KSN в политике не совпадает с версией Положения о KSN в плагине управления Kaspersky Endpoint Agent. Такая ситуация возникает, если плагин обновлен до версии 3.16, а политика создана в более ранней версии плагина.

   a. В разделе **Kaspersky Security Network** перейдите по ссылке **Ознакомиться с условиями Положения о KSN**.
   b. В открывшемся окне прочтите условия Положения о KSN.
   c. Если вы согласны с условиями Положения о KSN, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KSN**.
   d. Нажмите на кнопку **OK**.
8. Выполните одно из следующих действий:
   - Установите флажок **Включить использование Kaspersky Security Network (KSN)**, если вы хотите включить использование KSN.
   - Снимите флажок **Включить использование Kaspersky Security Network (KSN)**, если вы хотите выключить использование KSN.
9. Если вы хотите использовать Kaspersky Security Center в качестве посредника для передачи телеметрии, установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

   Флажок позволяет управлять передачей данных от защищаемых устройств в KSN.

   Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center.

   Если флажок снят, данные с Сервера администрирования и защищаемых устройств отправляются в KSN напрямую, минуя Kaspersky Security Center. Активная политика определяет, какой тип данных отправляется в KSN напрямую.
   По умолчанию флажок установлен.
10. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
11. Нажмите на кнопку **OK**.
12. В окне свойств политики нажмите на кнопку **Сохранить**.

kaspersky

Настройка общих параметров интеграции с серверами сбора телеметрии

В этом разделе содержится информация о том, как настроить общие параметры интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks с помощью Kaspersky Security Center Web Console.

В этом разделе

Настройка параметров передачи данных

► *Чтобы настроить параметры передачи данных, выполните следующие действия:*

1. Откройте окно свойств политики программы.
2. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.

   Откроется окно **Общие параметры**.
3. В блоке параметров **Параметры передачи данных** выполните следующие действия:
   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.
   - Укажите значения в поле **Максимальное количество событий в одном пакете**.
4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.
5. Нажмите на кнопку **OK**.

Настройка параметров регулирования количества запросов

Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node.

► *Чтобы настроить параметры регулирования количества запросов:*

1. Откройте окно свойств политики программы.
2. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.

   Откроется окно **Общие параметры**.

3. В блоке параметров **Регулирование количества запросов** вы можете выполнить следующие действия:
   - Установить или снять флажок **Включить регулирование количества запросов**, чтобы включить или отключить функцию.

     По умолчанию функция включена.
   - Указать значения в поле **Максимальное количество событий в час**.

     Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить указанную в этом поле величину. По умолчанию задано 3000 событий в час.
   - Указать значения в поле **Процент превышения лимита событий**.

     Если поток однотипных событий низкой важности превысит указанный в этом поле порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5% до 100%. По умолчанию задано 15%.
4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.
5. Нажмите на кнопку **ОК**.

Выбор источника параметров Сетевой изоляции и Запрета запуска

► *Чтобы выбрать источник параметров Сетевой изоляции и Запрета запуска:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.
8. В блоке **Источник параметров Сетевой изоляции и Запрета запуска** в раскрывающемся списке **Приоритетный сервер** выберите сервер, который будет источником параметров Сетевой изоляции и Запрета запуска. Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска по следующим правилам:
   - Если настроена интеграция только с сервером KATA, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере с установленным KATA Central Node.

- Если настроена интеграция только с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере с установленным KICS for Networks.
- Если настроена интеграция и с сервером KATA, и с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере, выбранном в раскрывающемся списке **Приоритетный сервер**.
- Если интеграция с сервером KATA и сервером KICS for Networks не настроена, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные локально на узле с установленным Kaspersky Endpoint Agent с помощью командной строки или в свойствах узла в Консоли администрирования Kaspersky Security Center.

9. Нажмите на кнопку **OK**, чтобы сохранить изменения.

kaspersky

Настройка интеграции Kaspersky Endpoint Agent с SIEM

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с SIEM-сервером при помощи Kaspersky Security Center Web Console.

В этом разделе

См. также

Включение интеграции с SIEM

► *Чтобы включить интеграцию с программой Kaspersky Industrial CyberSecurity for Networks:*

1. Выполните одно из следующих действий:
   - Чтобы настроить параметры интеграции с SIEM для группы защищаемых устройств, откройте окно свойств политики программы.
   - Чтобы настроить параметры интеграции с SIEM для отдельного защищаемого устройства, откройте параметры программы для устройства.
2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с SIEM**.

   Откроется окно **Интеграция с SIEM**.
3. В блоке **Параметры подключения** с помощью одноименного флажка включите интеграцию с SIEM.
4. В блоке параметров **Список SIEM-серверов** добавьте параметры подключения к одному или нескольким SIEM-серверам:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Параметры SIEM-сервера**.
   b. В одноименном поле укажите доменное имя или IP-адрес SIEM-сервера.
   c. В поле **Порт** введите порт для подключения к SIEM-серверу.
   d. В раскрывающемся списке **Протокол** выберите протокол, с помощью которого осуществляется передача данных между Kaspersky Endpoint Agent и SIEM-сервером.
   e. Нажмите на кнопку **Добавить**.

      Параметры подключения к SIEM-серверу отобразятся в блоке параметров **Список SIEM-серверов**.

5. Если необходимо, повторите пункты a–e для добавления параметров подключения к другим SIEM-серверам.

   Kaspersky Endpoint Agent подключается к первому SIEM-серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму SIEM-серверу и так далее по списку.

6. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

7. Нажмите на кнопку **ОК**.

Интеграция с SIEM будет включена сразу после применения политики.

Настройка защищенного соединения с SIEM-сервером

► *Чтобы настроить защищенное соединение Kaspersky Endpoint Agent с SIEM-сервером:*

1. Выполните одно из следующих действий:
   - Чтобы настроить параметры интеграции с SIEM для группы защищаемых устройств, откройте окно свойств политики программы.
   - Чтобы настроить параметры интеграции с SIEM для отдельного защищаемого устройства, откройте параметры программы для устройства.
2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с SIEM**.

   Откроется окно **Интеграция с SIEM**.
3. В блоке **Параметры подключения** установите флажок **Использовать TLS-шифрование**, чтобы шифровать передачу данных между Kaspersky Endpoint Agent и SIEM-сервером.
4. Если вы хотите настроить дополнительную защиту подключения с использованием закрепленного TLS-сертификата:
   a. Установите флажок **Использовать закреплённый сертификат для защиты соединения**.
   b. Добавьте TLS-сертификат:
      i. Нажмите на кнопку **Добавить новый TLS-сертификат**.
      ii. В открывшемся окне выполните одно из следующих действий:
         - Нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
         - Скопируйте содержимое файла сертификата в поле **Данные TLS-сертификата**.
      iii. Нажмите на кнопку **ОК**.

      Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.
5. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата:
   a. В блоке **Дополнительная защита подключения** установите флажок **Защита подключения с помощью сертификата клиента**.
   b. Нажмите на кнопку **Загрузить криптоконтейнер**.

c. В открывшемся окне выберите файл формата PFX, в котором в зашифрованном виде хранится сертификат клиента.

d. Нажмите на кнопку **Открыть**.

6. В поле **Пароль криптоконтейнера** введите пароль для доступа к PFX-файлу.
7. Нажмите на кнопку **ОК**.
8. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.
9. Нажмите на кнопку **ОК**.

Защищенное соединение с SIEM-сервером настроено.

Настройка времени ожидания ответа от SIEM-сервера

► *Чтобы настроить время ожидания ответа от SIEM-сервера:*

1. Выполните одно из следующих действий:
   - Чтобы настроить параметры интеграции с SIEM для группы защищаемых устройств, откройте окно свойств политики программы.
   - Чтобы настроить параметры интеграции с SIEM для отдельного защищаемого устройства, откройте параметры программы для устройства.
2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с SIEM**.

   Откроется окно **Интеграция с SIEM**.
3. В блоке **Дополнительные параметры** в поле **Время ожидания (сек.)** укажите продолжительность ожидания ответа от SIEM-сервера.

   По истечении указанного времени Kaspersky Endpoint Agent повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию указано значение 10 секунд.
4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.
5. Нажмите на кнопку **ОК**.

kaspersky

Настройка параметров EDR-телеметрии

В этом разделе содержится информация о том, как настроить:

- Исключения EDR-телеметрии о процессах программ, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.
- Оптимизацию объема EDR-телеметрии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.
- Исключения EDR-телеметрии о сетевых коммуникациях, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ

Вы можете включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ с помощью Kaspersky Security Center Web Console в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о процессах программ доступны при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные об исключенных процессах программ.

Управление (включение / выключение) оптимизацией объема отправляемой EDR-телеметрии о процессах программ доступно при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Если включена оптимизация объема отправляемой EDR-телеметрии, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe о процессах программ на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

► *Чтобы включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     b. Выберите устройство.
     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
     d. Выберите **Kaspersky Endpoint Agent**.
     e. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
2. В разделе **EDR-телеметрия** выберите **Исключенные процессы**.

   Откроется окно **Исключенные процессы**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Настройте оптимизацию объема отправляемой EDR-телеметрии:

   При интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node оптимизация объема отправляемой EDR-телеметрии должна быть всегда включена.

   - Выключите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов.
   - Включите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent не отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов.

   Если параметр **Использовать исключения** выключен, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов вне зависимости от значения параметра **Оптимизировать объем отправляемой телеметрии**.
5. Создайте список исключений:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Свойства правила** настройте параметры исключения.
   c. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Свойства правила**.

   Новое исключение создано и отображается в списке.

d. Если необходимо экспортировать список исключений в файл формата XML, нажмите на кнопку **Экспорт**.

e. Если необходимо импортировать список исключений из файла формата XML, нажмите на кнопку **Импорт**.

f. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

g. Если необходимо удалить исключение из списка, выберите исключение и нажмите на кнопку **Удалить**.

6. Если вы настраиваете параметры политики, убедитесь, что переключатель в правом верхнем углу блока параметров находится в активном положении.

7. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях

Вы можете настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях с помощью Kaspersky Security Center Web Console в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о сетевых коммуникациях применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным или Kaspersky Industrial CyberSecurity for Networks данные, подпадающие под параметры исключений.

► *Чтобы включить и настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях:*

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.

     b. Выберите устройство.

     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.

     d. Выберите **Kaspersky Endpoint Agent**.

     e. В открывшемся окне выберите вкладку **Параметры программы**.

   - Откройте окно свойств политики программы.

2. В разделе **EDR-телеметрия** выберите **Исключенные сетевые коммуникации**.

   Откроется окно **Исключенные сетевые коммуникации**.

3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.

4. Создайте список исключений:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Свойства правила** настройте параметры исключения.
   c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.
   d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.
5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.
6. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Включение и настройка исключений отправляемой EDR-телеметрии об операциях с файлами

Вы можете настроить исключения отправляемой EDR-телеметрии об операциях с файлами с помощью Kaspersky Security Center Web Console в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии об операциях с файлами применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Managed Detection and Response данные, подпадающие под параметры исключений.

► *Чтобы включить и настроить исключения отправляемой EDR-телеметрии об операциях с файлами:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     b. Выберите устройство.
     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
     d. Выберите **Kaspersky Endpoint Agent**.
     e. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
2. В разделе **EDR-телеметрия** выберите **Исключенные операции с файлами**.

   Откроется окно **Исключенные операции с файлами**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.

4. Создайте список исключений:
    a. Нажмите на кнопку **Добавить**.
    b. В открывшемся окне **Свойства правила** настройте параметры исключения.
    c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.
    d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.
5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении.
6. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Настройка параметров Запрета запуска

В этом разделе приведены инструкции по настройке параметров Запрета запуска.

В этом разделе

Включение Запрета запуска

► *Чтобы включить Запрет запуска:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. Выберите раздел **Запрет запуска**.
8. В блоке параметров **Режим запрета** установите флажок **Включить запрет запуска недоверенных объектов**.
9. В раскрывающемся списке **Применять правила запрета в режиме** выберите требуемый режим применения правил запрета:
   - **Только статистика**.

     В этом режиме Kaspersky Endpoint Agent публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.
   - **Активный**.

     В этом режиме Kaspersky Endpoint Agent блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета.

   При включении Запрета запуска в Kaspersky Security Center по умолчанию выбран режим **Только статистика**.

10. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
11. Нажмите на кнопку **OK**.
12. Нажмите на кнопку **Сохранить**.

Отключение Запрета запуска

► *Чтобы отключить Запрет запуска:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. Выберите раздел **Запрет запуска**.
8. В блоке параметров **Режим запрета** снимите флажок **Включить запрет запуска недоверенных объектов**.
9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**.

Включение и отключение уведомления пользователей о Запрете запуска

Вы можете выбрать опцию **Уведомлять пользователя устройства при запрете**.

Если Запрет запуска включен в режиме (см. раздел "Включение Запрета запуска" на стр. 196) **Активный** и выбрана опция **Уведомлять пользователя устройства при запрете** (см. раздел "**Включение и отключение уведомления пользователей о Запрете запуска**" на стр. 197), на защищаемых устройствах будут отображаться всплывающие уведомления с информацией о сработавших правилах Запрета запуска. Если пользователь устройства не закроет всплывающее уведомление, то оно закроется автоматически через 60 секунд после появления. По умолчанию опция **Уведомлять пользователя устройства при запрете** выключена.

Предварительно необходимо включить Запрет запуска (см. раздел "Включение Запрета запуска" на стр. 196).

► *Чтобы включить или отключить уведомление пользователя о Запрете запуска:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     b. Выберите устройство.
     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
     d. Выберите **Kaspersky Endpoint Agent**.
     e. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Режим запрета** установите или снимите флажок **Уведомлять пользователя устройства при запрете**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

Управление списком правил Запрета запуска

► *Чтобы настроить список правил Запрета запуска:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     b. Выберите устройство.
     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
     d. Выберите **Kaspersky Endpoint Agent**.
     e. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Правила запрета** можно выполнить следующие действия:
   - Добавить правило запрета в список.
   - Изменить параметры правила запрета.
   - Удалить правило запрета из списка.

4. В блоке параметров **Правила запрета** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения правил запрета.
5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
6. Нажмите на кнопку **OK**.
7. В окне свойств политики нажмите на кнопку **Сохранить**.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.
При использовании Kaspersky Endpoint Agent версии 3.10 и выше, чтобы создать правило запрета по критерию пути к файлу, расположенному на компакт-диске или в ISO-образе, необходимо указать путь в формате `\?\GLOBALROOT\Device\<имя устройства>\<путь к файлу>`, где `<имя устройства>` - это имя устройства чтения компакт-дисков или смонтированного ISO-образа в вашей системе. Например, путь может выглядеть следующим образом: `\?\GLOBALROOT\Device\CdRom1\some_file.exe`.

При указании объектов по критерию пути к файлу можно использовать маски файлов (с помощью символов ? и *).

kaspersky

Настройка параметров хранилищ в Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров карантина и параметров синхронизации данных с Сервером администрирования с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

О карантине Kaspersky Endpoint Agent

Карантин – это специальное локальное хранилище на устройстве. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

По умолчанию локальное хранилище карантина расположено в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Quarantine`. По умолчанию объекты, восстановленные из карантина, хранятся в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Restored`.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на устройствах с программой Kaspersky Endpoint Agent. Агенты администрирования устройств передают информацию о файлах на карантине на Сервер администрирования.

Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования. Все объекты находятся на защищаемых устройствах с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Об управлении карантином в Kaspersky Endpoint Agent

Через Kaspersky Security Center можно настраивать параметры карантина (см. раздел "Настройка параметров хранилищ в Kaspersky Endpoint Agent" на стр. 147), просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина. Подробную информацию об управлении объектами, находящимися на карантине, через Kaspersky Security Center см. в документации Kaspersky Security Center.

Для того чтобы Kaspersky Endpoint Agent отправлял данные об объектах, помещенных на карантин, на Сервер администрирования Kaspersky Security Center, необходимо включить эту опцию (см. раздел "Настройка синхронизации данных с Сервером администрирования" на стр. 149) в параметрах карантина в политике Kaspersky Endpoint Agent. По умолчанию опция включена.

Через интерфейс командной строки на устройстве можно просматривать информацию о параметрах карантина и свойствах объектов, находящихся на карантине (см. раздел "Просмотр информации о параметрах карантина и объектах на карантине" на стр. 242).

Kaspersky Endpoint Agent помещает объект на карантин под системной учетной записью (SYSTEM).

Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя защищаемого устройства.

Настройка параметров карантина и восстановления объектов из карантина

► *Чтобы настроить параметры карантина:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры программы**.
4. В разделе **Репозитории** выберите подраздел **Карантин**.
5. В разделе **Параметры Карантина** настройте параметры карантина:
   e. В поле **Папка Карантина** укажите путь, по которому будет создана папка карантина на устройствах, или нажмите на кнопку **Обзор** и выберите путь.

   По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

   Пример:

   Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим:

   ```
   C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
   ```

6. Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер Карантина (МБ)** и укажите или выберите в списке максимальный размер карантина в мегабайтах.

   Например, вы можете задать максимальный размер карантина 200 МБ.

   При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

7. Чтобы задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

   Например, вы можете задать пороговое значение карантина 50 МБ.

   При достижении порогового значения карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

8. В разделе **Восстановление объектов из Карантина** в поле **Папка для восстановленных объектов** укажите путь, по которому будет создана папка для объектов, восстановленных из карантина.

   По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

   Пример:

   Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке восстановленных из карантина объектов будет следующим:

   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопки **Применить** и **ОК**.

Параметры карантина и папка для восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center.

► *Чтобы настроить синхронизацию данных с Сервером администрирования:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     a. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     b. Выберите устройство.
     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
     d. Выберите **Kaspersky Endpoint Agent**.
     e. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
2. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
3. Установите флажок **Данные об объектах в Карантине на управляемых устройствах**.

4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **Сохранить**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка построения цепочки развития угрозы

Для построения цепочки развития угрозы необходимо выполнение определенных предусловий (см. раздел "Предусловия построения цепочки развития угрозы" на стр. 115).

Вы можете включить построение цепочки развития угрозы для объектов, обнаруженных на управляемых устройствах. Цепочка развития угрозы отображается в карточке инцидента (см. раздел "Работа с карточкой инцидента" на стр. 114).

► *Чтобы включить построение цепочки развития угрозы:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
   - Откройте окно свойств политики программы.
7. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
8. Установите флажок **Отправлять данные для построения цепочки развития угрозы** в блоке параметров **Синхронизация с Сервером администрирования**.
9. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров **Синхронизация с Сервером администрирования** измените положение переключателя с **Не определено** на **Принудительно**.
10. Нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**.

Построение цепочки развития угрозы настроено.

Настройка диагностики сбоев

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

► *Чтобы настроить диагностику сбоев:*

1. Откройте окно свойств программы для отдельного устройства.
2. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
3. Выберите устройство.
4. В открывшемся окне **<Имя устройства>** выберите вкладку **Программы**.
5. Выберите **Kaspersky Endpoint Agent**.
6. В открывшемся окне выберите вкладку **Параметры программы**.
7. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.
8. Если вы хотите включить запись отладочной информации в файлы трассировки:
   a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.
   b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

      Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

   c. В поле **Максимальный размер файла трассировки (МБ)** укажите размер файла в мегабайтах.

      По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.
9. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:
   a. Включите параметр **Перезаписывать старые файлы трассировки**.
   b. В поле **Максимальное количество файлов для одного журнала трассировки** укажите желаемое значение.

      По умолчанию задан 1 файл. Когда достигается указанное количество файлов, программа перезаписывает старые файлы, начиная с самого старого. Указанное ограничение применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение.

10. Если вы хотите включить запись файлов дампа:
    a. Включите параметр **Создавать файлы дампа**.
    b. В поле **Папка** файлов **дампа** укажите папку для сохранения файлов дампа.

    > Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

11. Нажмите на кнопку **OK**.

Диагностика сбоев настроена и включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы для диагностики сбоев будут создаваться в папках, которые вы указали.

kaspersky

Управление задачами Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами Kaspersky Endpoint Agent.

В этом разделе

Создание задач

► *Чтобы создать задачу:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.
4. В раскрывающемся списке **Тип задачи** выберите нужный тип задачи и следуйте дальнейшим шагам мастера.
5. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.

Если вы не установите этот флажок, задача будет создана с заданными по умолчанию значениями параметров, которые вы можете изменить позже в любое время для каждого из следующих типов задач:

- **Активация программы** (см. раздел "**Создание задач активации Kaspersky Endpoint Agent**" на стр. 210)
- **Поиск IOC** (см. раздел "**Настройка параметров стандартной задачи поиска IOC**" на стр. 216)
- Аудит безопасности (см. раздел "Создание задачи аудита безопасности с параметрами по умолчанию" на стр. 221)
- **Удалить файл** (см. раздел "**Настройка параметров задачи Удалить файл**" на стр. 232)
- **Поместить файл на карантин** (см. раздел "**Настройка параметров задачи Поместить файл на карантин**" на стр. 230)
- **Завершить процесс** (см. раздел "**Настройка параметров задачи Завершить процесс**" на стр. 234)
- **Запустить процесс** (см. раздел "**Настройка параметров задачи Запустить процесс**" на стр. 233)
- **Обновление баз и модулей программы** (см. раздел "**Настройка параметров задачи обновления баз и модулей программы**" на стр. 212)

6. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Просмотр списка задач

► *Чтобы просмотреть список задач,*

в главном окне веб-консоли перейдите в раздел **Устройства** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которым они относятся.

Удаление задач из списка

► *Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.
2. В отобразившемся списке задач установите флажки напротив задач, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Настройка расписания запуска задач

► *Чтобы настроить запуск задачи по расписанию:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. На закладке **Расписание** в разделе **Общие** переведите переключатель из положения **Расписание выключено** в положение **Запускать по расписанию**.
4. В раскрывающемся списке **Периодичность** выберите один из следующих вариантов: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
5. Если вы выбрали запуск задачи **В указанное время**, укажите время и дату запуска задачи.
6. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, настройте параметры запуска задачи:
   a. В поле **Каждый** задайте периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.
   b. В полях **Время запуска** и **Дата запуска** задайте время и дату начала действия расписания.
7. Чтобы выполнить расширенную настройку расписания, выберите раздел **Дополнительно** и выполните следующие действия:
   a. Если вы хотите задать максимальное время ожидания выполнения задачи, установите флажок **Завершать задачу, выполняющуюся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

c. Если вы хотите, чтобы программа при первой возможности запускала задачи, не выполненные вовремя, установите флажок Запускать пропущенные задачи.

d. Если вы хотите избежать одновременного обращения большого количества устройств к Серверу администрирования и запускать задачу на устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок Распределять время запуска задач в интервале и задайте интервал запуска в минутах.

8. Нажмите на кнопку **Сохранить**.

Запуск задач вручную

Программа запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время.

► *Чтобы запустить задачу вручную:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в графе **Статус** или нажав на кнопку **Результат выполнения**.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Вы также можете изменить срок хранения результатов выполнения задач (см. раздел "Изменение срока хранения результатов выполнения задач на Сервере администрирования" на стр. 210).

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

► *Чтобы просмотреть результат выполнения задачи:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.
2. В отобразившемся списке задач нажмите на имя задачи.

   Откроется окно настройки параметров задачи.
3. Перейдите на закладку **Результаты**.

Информация отображается в списке **Результаты выполнения задачи**.

Вы также можете просмотреть **Результаты последнего выполнения** задачи на закладке **Общие**.

Изменение срока хранения результатов выполнения задач на Сервере администрирования

По умолчанию результаты выполнения задач хранятся на Сервере администрирования в течение семи дней.

► *Чтобы изменить срок хранения результатов выполнения задач на Сервере администрирования:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.
2. В отобразившемся списке задач нажмите на имя задачи.

   Откроется окно настройки параметров задачи.
3. Перейдите на закладку **Параметры**.
4. В разделе **Уведомления** нажмите на кнопку **Параметры.**
5. Убедитесь, что в списке **Выберите поведение программы после завершения задачи** выбран параметр **Хранить в базе данных Сервера администрирования в течение (сут)** и укажите, в течение какого времени (в сутках) требуется хранить результат выполнения задачи.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить.**

Изменения будут сохранены.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Создание задач активации Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent с помощью лицензионного ключа из хранилища ключей Kaspersky Security Center. Подробную информацию об управлении лицензионными ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

► *Чтобы создать задачу активации Kaspersky Endpoint Agent:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.
4. В раскрывающемся списке **Тип задачи** выберите **Активация программы**.
5. В поле **Название задачи** задайте отображаемое имя задачи.

6. Если вы хотите создать задачу для устройств определенной группы Сервера администрирования, выполните следующие действия:
   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Группа устройств** и нажмите **Далее**.
   b. Выберите нужную группу Сервера администрирования и нажмите **Далее**.
7. Если вы хотите создать задачу для определенных устройств по диапазону IP-адресов, NetBIOS-именам, DNS-именам или выбрать из списка устройств, обнаруженных в сети Сервером администрирования, выполните следующие действия:
   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выбранные устройства или импортируемые устройства из списка** и нажмите **Далее**.
   b. Добавьте в список устройства по нужным критериям и нажмите **Далее**.
8. Если вы хотите создать задачу для устройств из определенной выборки, выполните следующие действия:
   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выборка** и нажмите **Далее**.
   b. Укажите нужную выборку из списка и нажмите **Далее**.
9. В окне **Выберите лицензионный ключ** выберите нужный лицензионный ключ из списка доступных в хранилище ключей Kaspersky Security Center.
10. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.
11. Нажмите **Далее**.
12. В окне **Выбор учетной записи для запуска задачи** выберите нужную учетную запись и нажмите **Далее**.
13. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.
14. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

kaspersky

Настройка параметров задачи обновления баз и модулей программы

Для поддержания сертифицированного состояния программы запрещается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу программы из сертифицированного состояния.

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

► *Чтобы настроить параметры задачи обновления баз и модулей программы:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры подключения**.
5. Если вы используете Kaspersky Security Center, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Сервер администрирования Kaspersky Security Center**.
   - **Серверы обновлений «Лаборатории Касперского»**.
   - **Другие HTTP-, FTP-серверы или сетевые папки**.
6. Если вы используете Kaspersky Security Center Cloud Console, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Точки распространения**. Использование в качестве источника обновлений устройства с установленным Агентом администрирования.

     Подробная информация об использовании точек распространения доступна в справке Kaspersky Security Center Cloud Console https://help.kaspersky.com/KSC/CloudConsole/ru-RU/98876.htm.
   - **Серверы обновлений «Лаборатории Касперского»**. Использование в качестве источника обновлений серверов обновлений "Лаборатории Касперского".
7. Если вы хотите включить параметр **Использовать серверы обновлений «Лаборатории Касперского», если указанные пользователем серверы недоступны**, установите флажок рядом с названием параметра.

   Недоступно в Kaspersky Security Center Cloud Console.

8. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

   Недоступно в Kaspersky Security Center Cloud Console.

   a. Нажмите на ссылку **Параметры**, чтобы открыть окно **Пользовательские источники обновлений**.

   b. Добавьте источники обновлений в список, выполнив следующие действия:

      1. Нажмите на кнопку **Добавить**.
      2. В открывшемся диалоговом окне в поле **Веб-адрес** введите адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений, и нажмите на кнопку **OK**.
      3. Если вы хотите использовать этот источник для обновления баз, установите переключатель рядом с его адресом в положение **Включить**.

         Выполняйте аналогичные действия для добавления каждого нового источника.

      4. Нажмите на кнопку **OK**.

         Окно **Пользовательские источники обновлений** закроется.

9. Выберите раздел **Параметры обновления**.
10. В блоке параметров **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:
    - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.
    - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
    - **Загружать и устанавливать важные обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.
11. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.
12. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

kaspersky

Управление стандартными задачами поиска IOC

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

В этом разделе приведены инструкции по управлению стандартными задачами поиска IOC.

В этом разделе

Требования к IOC-файлам

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.
- Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
- Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.
- Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

В таблице ниже приведены особенности и ограничения поддержки стандарта OpenIOC программой.

Таблица 12. Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0:
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	Программа поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`

	Программа поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.
Поддерживаемые IOC-термины	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent:

https://help.kaspersky.com/KEA/3.9/ru-RU/IOC_TERMS.zip

Настройка параметров стандартной задачи поиска IOC

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

► *Чтобы настроить параметры стандартной задачи поиска IOC:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Параметры поиска IOC** настройте IOC-коллекцию, выполнив следующие действия:
   a. В блоке параметров **IOC-коллекция** нажмите на кнопку **Переопределить IOC-файлы**.
   b. В открывшемся диалоговом окне нажмите на кнопку **Добавить IOC-файлы** и укажите IOC-файлы, которые вы хотите использовать для задачи.

      Для одной задачи поиска IOC можно выбрать несколько IOC-файлов.

c. Нажмите на кнопку **ОК**, чтобы закрыть диалоговое окно.

> Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.

d. Если вы хотите посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, выполните следующие действия:

1. Нажмите на ссылку с именами всех загруженных IOC-файлов в блоке параметров **IOC-файлы**.

   Откроется окно **Содержимое IOC ()**.

2. Чтобы просмотреть детальную информацию об отдельном IOC-файле, на закладке **IOC-коллекция** в списке файлов нажмите на имя нужного IOC-файла.

   В открывшемся окне отображена информация о выбранном IOC-файле.

3. Чтобы закрыть окно с информацией о выбранном IOC-файле, нажмите на кнопку **ОК** или **Отмена**.

4. Чтобы просмотреть информацию сразу обо всех загруженных IOC-файлах, перейдите на закладку **Данные IOC**.

   В рабочей области окна отображена информация о каждом загруженном IOC-файле.

5. Если вы хотите, чтобы определенный IOC-файл не использовался при запуске задачи поиска IOC, на закладке **IOC-коллекция** переведите переключатель рядом с его именем из положения **Включить** в положение **Исключить**.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Содержимое IOC ()**.

e. Если вы хотите экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать IOC-коллекцию**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.

f. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

g. В блоке параметров **Ретроспективный поиск IOC** настройте параметры ретроспективного режима поиска IOC:

   Ретроспективный поиск IOC - это режим работы задачи Поиск IOC, при котором Kaspersky Endpoint Agent выполняет поиск индикаторов компрометации по данным, полученным за указанный пользователем интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности защищаемых устройств. Kaspersky Endpoint Agent анализирует данные в журналах операционной системы и браузеров на устройствах.

   Режим **Ретроспективный поиск IOC** доступен только для Стандартных задач поиска IOC.

1. В блоке параметров **Ретроспективный поиск IOC** включите параметр **Выполнять Ретроспективный поиск IOC в интервале**.

2. Укажите временной интервал.

   Во время выполнения задачи программа анализирует данные, собранные за указанный вами интервал времени, включая границы указанного интервала (с 00:00 даты начала до

23:59 даты окончания). По умолчанию задан интервал, начинающийся в 00:00 дня, предшествующего дню создания задачи, и заканчивающийся в 23:59 дня создания задачи.

Если во время выполнения задачи Поиск IOC со включенным параметром **Выполнять Ретроспективный поиск IOC в интервале** программа не обнаруживает данных для анализа за указанный временной интервал, программа не информирует об этом. В этом случае программа сообщает об отсутствии индикаторов компрометации в отчете о выполнении задачи.

h. В блоке параметров **Действия** настройте ответные действия при обнаружении индикатора компрометации:

1. Установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.
2. Установите флажок **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.
3. Установите флажок **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.
4. Установите флажок **EPP запустить проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружены индикаторы компрометации.

Если включен параметр **Поместить на карантин и удалить** или **Запустить проверку важных областей**, в качестве ответных действий Kaspersky Endpoint Agent может признать обнаруженные файлы зараженными и удалить их с устройства.

i. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите защитить критические системные файлы от помещения на карантин и удаления при обнаружении индикатора компрометации.

Опция доступна, только если в блоке параметров **Действия** выбрано **Поместить на карантин и удалить**.

При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

5. В разделе **Дополнительно** выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи, и настройте дополнительные параметры поиска:

a. В блоке параметров **Выберите типы данных (IOC-документы) для анализа во время поиска IOC** установите флажки рядом с нужными IOC-документами.

В зависимости от загруженных IOC-файлов, некоторые флажки могут быть неактивными.

Kaspersky Endpoint Agent автоматически выбирает типы данных (IOC-документы) для задачи Поиск IOC в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

b. Если установлен флажок **Анализировать данные файлов (FileItem)**, нажмите на ссылку **Дополнительно (FileItem)** и в открывшемся окне **Параметры проверки документа FileItem** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

Вы можете выбрать одну из предзаданных областей, а также указать пути до нужных областей самостоятельно.

c. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

d. Если установлен флажок **Анализировать данные WEL (EventLogItem)**, нажмите на ссылку **Дополнительно (EventLogItem)** и в открывшемся окне **Параметры проверки документа EventLogItem** настройте дополнительные параметры анализа событий:

- **Проверять только события, зафиксированные в течение указанного периода**.

  Если флажок установлен, во время выполнения задачи учитываются только те события, которые были зафиксированы в указанный период.

- **Проверять события, относящиеся к следующим каналам**.

  Список каналов, которые анализируются во время выполнения задачи.

e. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Просмотр результатов выполнения задачи поиска IOC

► *Чтобы просмотреть результаты выполнения задачи Поиск IOC:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Результаты поиска IOC**.
5. В раскрывающемся списке **Устройство** выберите, для каких устройств вы хотите просмотреть результаты выполнения задачи поиска IOC.

   Отобразится сводная таблица результатов выполнения задачи на выбранных устройствах.

   Если на устройствах обнаружены индикаторы компрометации, в столбце **Результаты** отображается *обнаружены индикаторы компрометации*.

6. Если вы хотите просмотреть подробную информацию об обнаруженных индикаторах компрометации на определенном устройстве, выполните следующие действия:

   a. Нажмите на ссылку **обнаружены индикаторы компрометации** в строке с именем нужного устройства.

   Откроется окно **Результаты поиска IOC** со списком всех IOC-файлов, использованных в рамках задачи. Если на выбранном устройстве присутствует объект, который совпадает с определенным индикатором компрометации, в столбце **Статус** отображается *совпадает*.

b. Нажмите на ссылку **совпадает** в строке с именем нужного IOC-файла.

Откроется окно **Карточка инцидента IOC**.

Карточка инцидента IOC содержит информацию об объектах на устройстве, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

> Просмотр Карточки инцидента IOC недоступен для IOC-файлов, при проверке которых не было обнаружено совпадений на устройстве.

Управление задачами аудита безопасности

> Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Задачи аудита безопасности – это локальные или групповые задачи, которые создаются и настраиваются через Kaspersky Security Center Web Console или через интерфейс командной строки. Эти задачи используются для поиска уязвимостей и оценки соответствия производственных систем стандартам безопасности.

В этом разделе приведены инструкции по управлению задачами аудита безопасности.

В этом разделе

Создание задачи аудита безопасности с параметрами по умолчанию

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

► *Чтобы создать и настроить стандартную задачу аудита безопасности:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.
3. Запустится мастер создания задачи.
4. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Agent.
5. В раскрывающемся списке **Тип задачи** выберите **Аудит безопасности**.
6. Введите название задачи или оставьте название по умолчанию.
7. Выберите устройства, для которых будет назначена задача.
8. Нажмите на кнопку **Далее**.
9. На закладке **Источник правил** по умолчанию выбрано **Пользовательская база правил из файла**.
10. Нажмите на кнопку **Импортировать базу правил из файла**.
11. В открывшемся окне укажите архив с базой правил.

    Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и XCCDF-правилами.

    Совокупный размер архива не должен превышать 2 МБ.

12. Нажмите на кнопку **ОК**.

    В разделе **Источник правил** отобразятся данные по загруженным правилам. По ссылкам **Подробнее** в полях **Платформы** и **Продукты** вы можете открыть окна со списками операционных систем и продуктов, которые упомянуты в правилах выбранного источника.

13. Если необходимо, загрузите файл с внешними переменными:

    Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.
    b. Нажмите на кнопку **Импортировать внешние переменные из файла**.
    c. В открывшемся окне укажите путь к файлу с внешними переменными.
    d. Нажмите на кнопку **ОК**.
    e. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

f. Выберите один из режимов:

- **Проверять все уязвимости**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.

- **Проверять все уязвимости, кроме добавленных в список**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.

- **Проверять уязвимости, добавленные в список**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

g. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

14. В разделе **Дополнительно**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

    Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Применять директивы**.

    b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

    Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

    По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

15. В разделе **Расширенные параметры**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

16. Нажмите на кнопку **Далее**.

17. В открывшемся окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

    - Выберите учетную запись по умолчанию.
    - Введите имя и пароль пользователя, с правами учетной записи которого вы хотите выполнять задачу.

18. Нажмите на кнопку **Далее**.

19. В окне **Завершить создание задачи** нажмите на кнопку **Готово**.

    Задача будет создана с параметрами по умолчанию и отобразится в списке задач. Далее вы можете изменять параметры задачи.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

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

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

База данных уязвимостей Kaspersky ICS CERT для АСУ ТП поставляется и обновляется вместе с обновлениями баз и модулей Kaspersky Endpoint Agent. Поэтому, прежде чем приступить к настройке параметров задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП в качестве источника правил, обновите базы и модули программы (см. раздел "Настройка параметров задачи обновления баз и модулей программы" на стр. 212).

► *Чтобы настроить параметры задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП в качестве источника правил:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи аудита безопасности.
3. Выберите закладку **Параметры программы**.
4. В разделе **Источник правил** выберите **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**.

   Отобразится информация о базе уязвимостей. По ссылкам **Подробнее** в полях **Платформы** и **Продукты** вы можете открыть окна со списками операционных систем и продуктов, которые упомянуты в правилах выбранного источника.
5. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:
   a. Выберите один из режимов:
      - **Проверять все уязвимости**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.
      - **Проверять все уязвимости, кроме добавленных в список**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.
      - **Проверять уязвимости, добавленные в список**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

6. В разделе **Дополнительно**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:
   a. Установите флажок **Применять директивы**.
   b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

      Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

      По умолчанию переключатели включены для статусов **True** и **False** для всех директив.
7. В разделе **Расширенные параметры**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:
   a. Установите флажок **Включить запись в журнал**.
   b. Выберите необходимый **Уровень записи в журнал** из списка.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

   Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

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

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Конфигурации безопасности и соответствий стандартам поставляются и обновляются вместе с обновлениями баз и модулей Kaspersky Endpoint Agent. Поэтому, прежде чем приступить к настройке параметров задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам, обновите базы и модули программы (см. раздел "Настройка параметров задачи обновления баз и модулей программы" на стр. 212).

► *Чтобы настроить параметры задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам в качестве источника правил:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи аудита безопасности.
3. Выберите закладку **Параметры программы**.
4. В разделе **Источник правил** выберите **Конфигурации безопасности и соответствий стандартам для операционных систем**.
5. Нажмите на кнопку **Выбрать конфигурацию правил**.
6. В открывшемся окне выберите одну из конфигураций безопасности и соответствий стандартам.

7. Нажмите на кнопку **OK**.

   В разделе **Источник правил** отобразится информация о выбранной конфигурации безопасности и соответствий стандартам. А в разделе **Правила** отобразится список правил, входящих в выбранную в качестве источника конфигурацию безопасности и соответствий стандартам.

8. В разделе **Расширенные параметры**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

   a. Установите флажок **Включить запись в журнал**.

   b. Выберите необходимый **Уровень записи в журнал** из списка.

9. В разделе **Правила** изучите список правил, входящих в выбранную конфигурацию безопасности и соответствий стандартам:

   - Нажатием на название правила откройте описание правила.
   - Нажатием на кнопку **Фильтр** откройте окно для фильтрации правил.

10. Если необходимо, по результатам изучения правил, входящих в выбранную конфигурацию безопасности и соответствий стандартам, повторите пункты 6, 7, 9 инструкции, чтобы выбрать другую конфигурацию.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

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

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Прежде чем приступить к настройке параметров задачи аудита безопасности с использованием пользовательской базы из хранилища Kaspersky Security Center:

1. Создайте отпечаток сертификата подписи пользовательской базы через интерфейс командной строки (см. раздел "Создание отпечатка сертификата подписи для файлов с OVAL- или XCCDF-правилами" на стр. 262).

   Вы можете использовать уже существующий отпечаток сертификата подписи пользовательской базы.

2. Создайте инсталляционный пакет Kaspersky Security Center с именем package.zip через интерфейс командной строки (см. раздел "Создание инсталляционного пакета Kaspersky Security Center с пользовательскими OVAL- или XCCDF-правилами" на стр. 262).

3. Создайте и запустите задачу установки инсталляционного пакета, указав для установки только Сервер администрирования (см. раздел "Создание задачи удаленной установки Kaspersky Endpoint Agent" на стр. 58), чтобы добавить архив package.zip с OVAL- и XCCDF-правилами, созданный на предыдущем шаге, в репозиторий Kaspersky Security Center.

В Kaspersky Endpoint Agent можно только обновить установленный и развернутый пакет с пользовательской базой правил. Удалить пакет правил невозможно.

► *Чтобы настроить параметры задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Источник правил** выберите **Пользовательская база правил из хранилища Kaspersky Security Center**.
5. Нажмите на кнопку **Выбрать файл из пользовательской коллекции**.
6. В открывшемся окне выберите архив с базой правил.

   Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и / или XCCDF-правилами.

   Совокупный размер архива не должен превышать 2 МБ.

7. Нажмите на кнопку **ОК**.

   В разделе **Источник правил** отобразятся данные о загруженных правилах. По ссылкам **Подробнее** в полях **Платформы** и **Продукты** вы можете открыть окна со списками операционных систем и продуктов, которые упомянуты в правилах выбранного источника.
8. Если необходимо, укажите отпечаток сертификата подписи пользовательской базы правил:
   a. Установите флажок **Использовать отпечаток**.
   b. В поле **Отпечаток** введите отпечаток, полученный через интерфейс командной строки.
9. Если необходимо, загрузите файл с внешними переменными:

   Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

   a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.
   b. Нажмите на кнопку **Импортировать внешние переменные из файла**.
   c. В открывшемся окне укажите путь к файлу с внешними переменными.
   d. Нажмите на кнопку **ОК**.
10. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

    Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

a. Выберите один из режимов:

- **Проверять все уязвимости**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.

- **Проверять все уязвимости, кроме добавленных в список**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.

- **Проверять уязвимости, добавленные в список**.

  Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

11. В разделе **Расширенные параметры**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

    Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Применять директивы**.

    b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

       Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

       По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

12. В разделе **Расширенные параметры**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

13. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

kaspersky

Настройка параметров задачи аудита безопасности с использованием пользовательской базы из файла

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

► *Чтобы настроить параметры задачи аудита безопасности с использованием пользовательской базы из файла:*

1. В главном окне Kaspersky Security Center Web Console откройте раздел **Устройства** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Источник правил** выберите **Пользовательская база правил из файла**.
5. Нажмите на кнопку **Импортировать базу правил из файла**.
6. В открывшемся окне укажите архив с базой правил.

   Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и XCCDF-правилами.

   Совокупный размер архива не должен превышать 2 МБ.

7. Нажмите на кнопку **ОК**.

   В разделе **Источник правил** отобразятся данные по загруженным правилам. По ссылкам **Подробнее** в полях **Платформы** и **Продукты** вы можете открыть окна со списками операционных систем и продуктов, которые упомянуты в правилах выбранного источника.

8. Если необходимо, загрузите файл с внешними переменными:

   Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

   a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.
   b. Нажмите на кнопку **Импортировать внешние переменные из файла**.
   c. В открывшемся окне укажите путь к файлу с внешними переменными.
   d. Нажмите на кнопку **ОК**.

9. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

   Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

   a. Выберите один из режимов:

      - **Проверять все уязвимости**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.

      - **Проверять все уязвимости, кроме добавленных в список**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.

      - **Проверять уязвимости, добавленные в список**.

        Kaspersky Endpoint Agent проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

   b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

10. В разделе **Дополнительно**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

    Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Применять директивы**.

    b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

       Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

       По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

11. В разделе **Расширенные параметры**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

12. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Просмотр результатов выполнения задачи аудита безопасности

► *Чтобы просмотреть результаты выполнения задачи аудита безопасности:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Отчет**.

Список отчетов содержит результаты выполнения задачи в отсортированном по дате порядке. Каждая строка списка содержит статус выполнения задачи на указанном в параметрах задачи узле, а также дату и время завершения выполнения задачи и детальная информация.

Вы можете фильтровать данные в отчете с помощью фильтра.

Отчет о выполнении задачи аудита безопасности доступен для просмотра в Kaspersky Security Center в течение семи дней с момента выполнения задачи или до момента удаления задачи.

Экспорт результатов выполнения задачи аудита безопасности в отдельный файл

► *Чтобы экспортировать результаты выполнения задачи аудита безопасности в отдельный файл:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Отчет** выберите необходимый отчет и нажмите на кнопку **Подробнее**.
5. В открывшемся окне **Результаты выполнения задачи аудита безопасности** выполните одно из следующих действий:
   - Если вы хотите получить архив с отчетом по всем результатам выполнения задачи в формате XML, нажмите на кнопку **Экспортировать**.

     В **Загрузки** добавится ZIP-архив с отчетом в формате XML. Если в параметрах задачи была включена запись событий о выполнении аудита безопасности в журнал, то дополнительно добавится ZIP-архив с журналом в TXT- файле.
   - Если вы хотите получить архив с отчетом выполнения задачи в формате HTML:
     a. При необходимости, отфильтруйте данные отчета с помощью кнопки **Фильтр**.
     b. Нажмите на кнопку **Создать отчет**.

     В **Загрузки** добавится ZIP-архив с отчетом в формате HTML. В отчет будут включены только отфильтрованные строки.

   Название архива с отчетом содержит имя узла, для которого выполнялась задача, а также дату и время создания архива отчета.

Настройка параметров задачи Поместить файл на карантин

Если вы считаете, что на компьютере находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин.

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

► *Чтобы настроить параметры задачи Поместить файл на карантин:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В раскрывающемся списке **Укажите файл, который требуется поместить на карантин** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.
5. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.
6. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:
   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.
   - Укажите значение в поле **Путь к папке файла**.
7. В блоке параметров **Действия после помещения файла на карантин** выберите, необходимо ли удалять файл с защищаемого устройства после помещения на карантин.

   Если файл заблокирован другим процессом, то файл будет удален только после перезагрузки устройства.

8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.
9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки устройства. Рекомендуется проверить успешность выполнения задачи после перезагрузки устройства.

Задача помещения файла на карантин может завершиться с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин исполняемый файл, и он запущен в настоящий момент. Чтобы решить проблему, создайте задачу завершения процесса (см. раздел "Настройка параметров задачи Завершить процесс" на стр. 234) для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Настройка параметров задачи Удалить файл

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

► *Чтобы настроить параметры задачи Удалить файл:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В списке **Файл, который нужно удалить** нажмите на кнопку **Добавить**.
5. Откроется диалоговое окно **Файл, который нужно удалить**.
6. В раскрывающемся списке **Укажите файл, который нужно удалить** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.
7. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.
8. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:
   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.
   - Укажите значение в поле **Путь к папке файла**.
   - Установите флажок **Включить подпапки**, чтобы программа удаляла все вхождения объекта не только в указанной папке, но и во всех ее подпапках.
9. Нажмите на кнопку **ОК**, чтобы добавить заданный объект в список **Файл, который нужно удалить**.

   Вы можете указать несколько объектов для удаления в рамках одной задачи Удалить файл.
10. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

11. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. Рекомендуется проверить успешность удаления файла после перезагрузки устройства.

Удаление файла с подключенного сетевого диска не поддерживается.

Настройка параметров задачи Запустить процесс

Задача Запустить процесс позволяет запустить необходимую программу или команду на устройстве.

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

► *Чтобы настроить параметры задачи Запустить процесс:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Если вы хотите запустить программу с помощью командной строки (cmd.exe) или выполнить команду, введите необходимую команду в поле **Исполняемая команда**.
5. Если вы хотите запустить программу напрямую, выполните следующие действия:
   a. Укажите путь к исполняемому файлу программы в поле **Рабочая папка**.
   b. Укажите ключи запуска программы в поле **Аргументы**.
6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

kaspersky

Настройка параметров задачи Завершить процесс

Если вы считаете, что запущенный на устройстве процесс может угрожать безопасности устройства или локальной сети организации, вы можете завершить его.

Создание задачи (см. раздел "Создание задач" на стр. 206) выполняется предварительно отдельным этапом.
Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

► *Чтобы настроить параметры задачи Завершить процесс:*

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В поле **Полный путь к файлу** укажите путь к файлу процесса, который вы хотите завершить.
5. В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **Не задан**, **MD5** или **SHA256**.
6. Если вы выбрали **MD5** или **SHA256**, укажите значение в поле **Контрольная сумма**.
7. Если вы хотите, чтобы программа учитывала регистр символов в пути к файлу процесса, установите флажок **Путь с учетом регистра символов**.
8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.
9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную (см. раздел "Запуск задач вручную" на стр. 209) или настроить автоматический запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 208).

Управление Kaspersky Endpoint Agent через интерфейс командной строки

Программой Kaspersky Endpoint Agent можно управлять через интерфейс командной строки. Функциональность интерфейса командной строки обеспечивает утилита agent.exe. Утилита agent.exe входит в комплект поставки программы Kaspersky Endpoint Agent и устанавливается на каждое устройство вместе с Kaspersky Endpoint Agent в папку `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 32-разрядная операционная система) или `%ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 64-разрядная операционная система).

Пример:

Если на устройстве установлена 64-разрядная операционная система Windows и для установки программы Kaspersky Endpoint Agent вы выбрали установку на диск C, то при установке утилита agent.exe будет размещена в следующую папку:

`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

► *Чтобы управлять программой Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите команду: `agent.exe --<параметр программы, который вы хотите настроить>=<действие над параметром, которое вы хотите выполнить>` и нажмите на клавишу **ENTER**.

   Отобразится результат выполнения команды (код возврата).

► *Для вызова справки по всем доступным к управлению параметрам программы и их возможным значениям,*

выполните команду: `agent.exe --help`

В этом разделе

kaspersky

Управление активацией Kaspersky Endpoint Agent

► *Чтобы управлять активацией программы через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:
   - Чтобы активировать программу с помощью файла ключа:

     `agent.exe --license=add <путь к файлу ключа>`
   - Чтобы указать дополнительный ключ для автоматического продления срока действия лицензии:

     `agent.exe --license=reserve <путь к файлу ключа>`
   - Чтобы удалить добавленный основной или дополнительный ключ:

     `agent.exe --license=delete <серийный номер ключа>`
   - Чтобы просмотреть статус добавленных ключей:

     `agent.exe --license=show`

Коды возврата команды `--license`:

- `-305` – срок действия добавляемого ключа истек.
- `2` – неопределенная программная ошибка.
- `-302` – добавляемый ключ находится в списке запрещенных ключей.
- `-301` – добавляемый ключ не подходит для активации Kaspersky Endpoint Agent.
- `-303` – файл ключа поврежден.
- `4` – синтаксические ошибки.
- `-304` – указан некорректный путь к файлу ключа.

Управление аутентификацией Kaspersky Endpoint Agent

► *Чтобы управлять аутентификацией программы через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **Enter**.
3. Выполните следующую команду и нажмите на клавишу **Enter**:

   ```
   agent.exe --proxy={enable|disable|show} --mode={auto|custom} --server=<адрес_прокси-сервера> --port=<номер_порта> --use-auth={yes|no} --proxy-user=<имя_пользователя> --proxy-password=<пароль_пользователя> --bypass-local={yes|no}
   ```

Описание параметров аутентификации представлено в следующей таблице.

Таблица 13. Параметры команды аутентификации.

Параметры	Описание
`--proxy={enable|disable|show}`	Обязательный параметр. Параметр управляет подключением к прокси-серверу. Доступны следующие значения: `enable` – включает использование прокси-сервера. `disable` – отключает использование прокси-сервера. `show` – отображает текущие настройки использования прокси-сервера. Указанный прокси-сервер будет использоваться для работы с Kaspersky Security Network и для обновления баз. Настройки указанного прокси-сервера можно применять для интеграции с другими системами сбора статистики, при этом в параметрах интеграции потребуется отдельно включить использование указанного прокси-сервера.
► *`--mode={auto|custom}`*	Обязательный параметр. Параметр устанавливает режим настройки прокси-сервера. Доступны следующие значения: `auto` – автоматическое определение прокси-сервера. `custom` – ручная настройка параметров доступа к прокси-серверу.

▶ *--server=<адрес_прокси-сервера>*	Обязательный параметр. Параметр указывает адрес прокси-сервера.
▶ *--port=<номер_порта>*	Обязательный параметр. Параметр указывает порт подключения к прокси-серверу.
▶ *--use-auth={yes|no}*	Необязательный параметр. Параметр указывает необходимость аутентификации на прокси-сервере. Доступны следующие значения: yes – для подключения к прокси-серверу необходимо указать имя пользователя и пароль. no – подключение к прокси-серверу возможно без указания имени пользователя и пароля. Используется по умолчанию.
▶ *--proxy-user=<имя_пользователя>*	Необязательный параметр. Параметр указывает имя пользователя для подключения к прокси-серверу. По умолчанию используется пустое значение.
▶ *--proxy-password=<пароль_пользователя>*	Необязательный параметр. Параметр указывает пароль для подключения к прокси-серверу. По умолчанию используется пустое значение.
▶ *--bypass-local={yes|no}*	Необязательный параметр. Параметр устанавливает режим прямого подключения к локальным адресами без использования прокси-сервера. Доступные значения: yes –подключения к адресам внутри текущей локальной сети будут осуществляться без прокси-сервера. Используется по умолчанию. no – подключения к адресам текущей локальной сети и к внешним адресам будут осуществляться через прокси-сервер.

kaspersky

Настройка трассировки

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

► *Чтобы настроить трассировку в программе Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --trace=enable --folder <путь к папке для сохранения файлов трассировки>`, чтобы включить трассировку.

     Трассировка будет включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы трассировки будут создаваться в папке, которую вы указали.

     Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы трассировки не будут созданы.

   - `agent.exe --trace=enable --folder <путь к папке для сохранения файлов трассировки> --rotation=yes --rotate-file-size=<максимальный размер файла в МБ> --rotate-files-count=<максимальное количество файлов>`, чтобы включить трассировку в режиме перезаписи старых файлов трассировки при достижении указанных значений размера и количества файлов.

     Указанное ограничение по количеству файлов применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение. Если с параметром `--rotation=yes` не указать параметры `--rotate-file-size` или `--rotate-files-count` (один из, или оба), то программа использует значения по умолчанию. По умолчанию задан 1 файл размером в 50 МБ.

   - `agent.exe --trace=disable`, чтобы выключить трассировку.

     Трассировка будет отключена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

- `agent.exe --trace=show`, чтобы просмотреть текущее состояние трассировки и путь к папке для сохранения файлов трассировки.

  Отобразятся значения параметров `trace.enable` (`true`, если трассировка включена или `false`, если трассировка отключена) и `trace.folder` (путь к папке).

Коды возврата команды `--trace`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами журнала трассировки).
- 9 – неверная операция (например, попытка выполнения команды `--trace=disable`, если трассировка уже отключена).

Настройка создания дампа процессов Kaspersky Endpoint Agent

► *Чтобы настроить создание дампа процессов Kaspersky Endpoint Agent через интерфейс командной строки программы:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --dump=enable --folder <путь к папке, в которой вы хотите создавать дамп>`, чтобы включить создание дампа процессов Kaspersky Endpoint Agent.

     Создание дампа будет включено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы дампа будут создаваться в папке, которую вы указали.

     > Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы дампа не будут созданы.

- `agent.exe --dump=disable`, чтобы отключить создание дампа.

  Создание дампа будет отключено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

- `agent.exe --dump=show`, чтобы просмотреть текущее состояние создания дампа и путь к папке с файлами дампа.

  Отобразятся значения параметров `dump.enable` (`true`, если создание дампа включено или `false`, если создание дампа отключено) и `dump.folder` (путь к папке).

Коды возврата команды `--dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами дампа).
- 9 – неверная операция (например, попытка выполнения команды `--dump=disable`, если создание дампа уже отключено).

Просмотр информации о параметрах карантина и объектах на карантине

► *Чтобы просмотреть информацию о параметрах карантина и объектах, находящихся на карантине, через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --quarantine=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть список объектов, помещенных на карантин.

   Отобразится следующая информация обо всех объектах, находящихся в папке карантина, указанной при настройке параметров карантина:

   - Идентификаторы объектов, помещенных на карантин к текущему моменту (параметр `ouid`).
   - Имена объектов, помещенных на карантин (имя + расширение).

- Дата и время помещения объекта на карантин (UTC).
- Исходный путь к файлу, помещенному на карантин, и путь восстановления файла из карантина, заданный по умолчанию (без имени файла).
- Размер файла, помещенного на карантин (в байтах).
- Учетная запись пользователя, с правами которой выполнялась задача помещения файла на карантин.
- Статус объекта:
  - `DETECT`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
  - `CUSTOM`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.
- Способ, которым файл был помещен на карантин:
  - `AUTOMATIC_<название программы, обнаружившей угрозу в файле, помещенном на карантин>`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
  - `BY USER`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.

- `agent.exe --quarantine=limits`, чтобы просмотреть текущие значения параметров **Максимальный размер Карантина (МБ)** и **Пороговое значение места на диске (МБ)**, а также статусы применения этих параметров (статусы флажков), заданные при настройке параметров карантина (см. раздел "Настройка параметров карантина и восстановления объектов из карантина" на стр. 148).

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Действия над объектами на карантине

► *Чтобы выполнить действия над объектами, находящимися на карантине программы Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующие действия и нажмите на клавишу **ENTER**:
   - Если вы хотите безвозвратно удалить объекты, находящиеся на карантине, выполните команду:

     `agent.exe --quarantine=delete --ouid=<`идентификаторы объектов на карантине через запятую. Обязательный параметр`> [--pwd=<`текущий пароль пользователя`>]`.

     Объекты с указанными идентификаторами будут удалены из папки карантина, указанной при настройке параметров карантина.
   - Если вы хотите восстановить объекты из карантина, выполните команду:

     `agent.exe --quarantine=restore --ouid=<`идентификаторы объектов на карантине через запятую. Обязательный параметр`> [--path-type=<`один из вариантов выбора папки назначения при восстановлении объекта из карантина: `original|custom|settings`. Необязательный параметр`> --path=<`путь к папке назначения для восстановленных объектов. Обязательный параметр, если передан параметр `--path-type` и указано значение `original>] [--action=<`одно из действий над объектом: `replace|rename`. Необязательный параметр`>] [--pwd=<`текущий пароль пользователя`>]`.
   - Если вы хотите поместить объект на карантин, выполните одну из следующих команд:
     - `agent.exe --quarantine=add [--file=<`полный путь к объекту, который вы хотите поместить на карантин`>] [--pwd=<`текущий пароль пользователя`>]`.
     - `agent.exe --quarantine=add [--hash=<`хеш объекта, который вы хотите поместить на карантин. Обязательный параметр, если вы не указываете полный путь к объекту и передаете параметр `--hashalg >]--hashalg=<`один из типов хеша: `md5|sha256`. Обязательный параметр, если вы не указываете полный путь к объекту`> [--file=<`путь к папке с объектом, который вы хотите поместить на карантин`>] [--pwd=<`текущий пароль пользователя`>]`.

Таблица 14. Параметры команд при выполнении действий над объектами на карантине

Параметр	Описание
--ouid	Обязательный параметр. В параметре передается уникальный числовой (int64) идентификатор объекта на карантине. Отображается при просмотре информации об объектах на карантине (команда --quarantine=show).
--path-type=<original|custom|settings>	Параметр описывает логику выбора папки назначения при восстановлении объекта из карантина. • Если параметр не передан, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением <original>, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением <settings>, объект будет восстановлен в папку, указанную при настройке параметров карантина. Если папка недоступна, задача завершается с ошибкой. • Если параметр передан со значением <custom>, объект будет восстановлен в папку, путь к которой вы укажете для параметра --path. Если папка недоступна, задача завершается с ошибкой.
--path=<путь к папке назначения для восстановленных объектов>	Обязательный параметр, если передан параметр --path-type со значением <custom>. Параметр определяет путь, по которому вы хотите создать папку для объектов, восстановленных из карантина, если вы не хотите использовать папку, в которой находился объект до помещения его на карантин и папку, указанную при настройке параметров карантина.
--action=<replace|rename>	Параметр определяет действие над объектом, которое вы хотите выполнить, если при восстановлении объекта из карантина папка назначения для восстановленных объектов содержит файл с таким же именем. • Если параметр не передан, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс _restored. • Если параметр передан со значением <rename>, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс _restored. • Если параметр передан со значением <replace>, первоначальный объект будет заменен на восстановленный объект.

`--file=<`полный путь к объекту, который вы хотите поместить на карантин`>`	Обязательный параметр, если не передан параметр `--hashalg`. Параметр задает полный путь к объекту, который вы хотите поместить на карантин.
`--hashalg=<md5|sha256>`	Обязательный параметр, если не передан параметр `--file` и не указан полный путь к объекту, который вы хотите поместить на карантин. Параметр задает алгоритм хеширования, по которому будет рассчитана контрольная сумма объекта, который вы хотите поместить на карантин. Параметр может быть передан с одним из двух значений: `<md5>` или `<sha256>`.
`--hash=<контрольная сумма файла>`	Обязательный параметр, если передан параметр `--hashalg`. Параметр задает контрольную сумму объекта, который вы хотите поместить на карантин.
`--file=<папка с файлом>`	Обязательный параметр, если передан параметр `--hashalg`. Параметр задает путь к папке с объектом, который вы хотите поместить на карантин и хеш которого вы указали в параметре `--hash`.
`--pwd=<`текущий пароль пользователя`>`	Позволяет ввести пароль пользователя, под учетной записью которого выполняется команда.

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Запуск обновления баз или модулей Kaspersky Endpoint Agent

► *Чтобы запустить обновление баз или модулей программы Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

```
agent.exe --update=bases|modules [--source=<адреса пользовательских источников обновлений баз, разделенные точкой с запятой без пробела>|kl|ksc]
```

Таблица 15. Параметры команд при запуске обновления баз Kaspersky Endpoint Agent

Параметр	Описание
`--update=bases|modules`	Обязательный параметр. Позволяет указать тип обновления: • `--update=bases` позволяет запустить обновление баз программы. • `--update=modules` позволяет запустить обновление модулей программы. После обновления модулей программы Kaspersky Endpoint Agent теряет статус сертифицированного продукта.
`--source=<адреса пользовательских источников обновления баз>|kl|ksc]`	Необязательный параметр. Позволяет выбрать источник обновления баз. • `--source=<адреса пользовательских источников обновлений баз>` позволяет указать источник обновлений баз **Другие HTTP-, FTP-серверы или сетевые папки** и задать путь к сетевой папке или IP-адрес, FTP или HTTP-адрес сервера, с которого программа будет загружать обновления баз. Вы можете указать несколько адресов пользовательских источников обновлений баз, разделенных точкой с запятой без пробела (";"). Программа будет загружать обновления с первого доступного источника обновлений баз. Если все адреса будут недоступны, задача завершится с ошибкой. • `--source=kl` позволяет указать источник обновления баз **Серверы обновлений "Лаборатории Касперского"**. Если серверы будут недоступны, задача завершится с ошибкой. • `--source=ksc` позволяет указать источник обновления баз **Сервер администрирования Kaspersky Security Center**. Если Сервер администрирования будет недоступен, задача завершится с ошибкой.

Коды возврата команды `--update=bases`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.
- 200 – все объекты актуальны.
- -206 – файлы обновлений отсутствуют в указанном источнике обновлений баз или имеют неизвестный формат.
- -209 – ошибка подключения к источнику обновлений баз.
- -232 – ошибка подключения к прокси-серверу.
- -234 – ошибка подключения к Kaspersky Security Center.
- -236 – базы программы повреждены.

Запуск, остановка и просмотр текущего состояния программы

► *Чтобы запустить, остановить или просмотреть текущее состояние программы Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --product=<start|stop|state> [--pwd=<текущий пароль пользователя>]
   ```

Таблица 16. Параметры команд при запуске, остановке и просмотре текущего состояния Kaspersky Endpoint Agent

Параметр	Описание
`--product=<start|stop|state>`	Позволяет запустить, остановить или просмотреть текущее состояние программы. • `--product=<start>` запускает программу. • `--product=<stop>` останавливает программу. Если в программе настроена защита паролем, для выполнения команды `--product=<stop>` требуется ввести пароль. • `--product=<state>` отображает текущее состояние программы: запущена или остановлена.
`--pwd=<текущий пароль пользователя>`	Позволяет ввести пароль пользователя, с правами учетной записи которого выполняется команда.

Коды возврата команды `--product=<start|stop|state>`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.
- 9 – неверная операция (например, попытка выполнения команды `--product=start`, если программа уже запущена).

Защита программы паролем

Чтобы ограничить выполнение действий с программой Kaspersky Endpoint Agent, которые могут привести к снижению уровня защиты компьютера пользователя и данных, обрабатываемых на этом компьютере, а также к снижению уровня самозащиты программы, требуется защитить программу паролем.

Ввод пароля требуется для выполнения следующих команд в интерфейсе командной строки Kaspersky Endpoint Agent:

- `--sandbox=disable`
- `--sandbox=show`
- `--sandbox=enable --tls=no`

- `--sandbox=enable --pinned-certificate=<полный путь к файлу TLS-сертификата соединения Kaspersky Endpoint Agent с Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefense`
- `--license=delete`
- `--message-broker --type=kata <параметры>`
- `--event --action=enable`
- `--event --action=disable`

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

Также требуется вводить пароль при выполнении следующих действий над программой:

- удаление программы и удаленная деинсталляция программы с помощью Kaspersky Security Center;
- обновление программы (`upgrade`);
- восстановление программы (`repair`);
- работа в мастере установки программы;
- работа в интерфейсе командной строки.

После включения защиты паролем (см. раздел "Включение защиты паролем" на стр. 174) и применения политики Kaspersky Security Center, на всех устройствах управляемой группы Kaspersky Endpoint Agent применяется единый пароль.

После отключения защиты паролем в политике (см. раздел "Включение параметров в политике Kaspersky Endpoint Agent" на стр. 171) параметры защиты паролем сохраняются для локального устройства с возможностью редактирования.

Пароль хранится в параметрах программы в зашифрованном виде (как контрольная сумма).

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

► *Чтобы настроить защиту паролем программы Kaspersky Endpoint Agent через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --password=state`, чтобы просмотреть текущий статус защиты программы паролем.
   - `agent.exe --password=set --pwd=<текущий пароль пользователя> --new=<новый пароль пользователя>`, чтобы установить новый пароль пользователя.
   - `agent.exe --password=reset --pwd=<текущий пароль пользователя>`, чтобы сбросить пароль пользователя.

Защита служб программы технологией PPL

В Kaspersky Endpoint Agent реализована защита служб программы с помощью технологии *Protected Process Light (PPL)*.

Защита служб программы с помощью технологии Protected Process Light (PPL) может применяться только для следующих операционных систем:

- для рабочих станций – Windows 10 версия 1703 RS2 и выше;
- для серверов – Windows Server 2016 версия 1709 и выше.

Процессы, исполняющиеся с признаком PPL, не могут быть остановлены или изменены другими процессами без признака PPL.

Использование признака PPL для служб программы позволяет защитить службы от вредоносных воздействий извне и попыток компрометации.

► *Чтобы настроить защиту служб программы технологией PPL через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --ppl=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть текущий статус защиты служб программы технологией PPL.
   - `agent.exe --ppl=disable [--pwd=<текущий пароль пользователя>]`, чтобы отключить защиту служб программы технологией PPL.

Коды возврата команды `--ppl`:

- 0 – команда выполнена успешно.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.

Управление параметрами самозащиты

► *Чтобы управлять параметрами самозащиты через интерфейс командной строки Kaspersky Endpoint Agent:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   `agent.exe --selfdefense=<enable|disable>`

Управление фильтрацией событий

► *Чтобы управлять фильтрацией событий через интерфейс командной строки Kaspersky Endpoint Agent:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

```
agent.exe --event
=<createprocess|loadimage|registry|network|eventlog|filechange|accountl
oggon|codeinjection|wmiactivity> --action=<enable|disable|show>
```

Управление сетевой изоляцией

► *Чтобы управлять сетевой изоляцией через интерфейс командной строки:*

Включение сетевой изоляции, а также настройка параметров сетевой изоляции недоступны через интерфейс командной строки.

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд:
   - `agent.exe --isolation=show`

     Команда выводит в консоль текущие параметры сетевой изоляции на устройстве, включая список заданных сетевых профилей исключений, а также список правил, заданных в сетевых профилях.
   - `agent.exe --isolation=disable`

     Команда отключает сетевую изоляцию на устройстве.
4. Нажмите на клавишу **ENTER**.

Коды возврата команды `--isolation`:

- -1 – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.

- 4 – синтаксическая ошибка.
- 9 – неверная операция (например, попытка отключения сетевой изоляции, если сетевая изоляция не включена).

Управление стандартными задачами поиска IOC

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

► *Чтобы создать и настроить стандартную задачу поиска IOC через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **Enter**:

   ```
   agent.exe --scan-ioc {[--path=<путь к папке с IOC-файлами>] | [<полный путь к IOC-файлу>]} [--process=no] [--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>] [--registry=no] [--dnsentry=no] [--arpentry=no] [--ports=no] [-services=no] [--system=no] [--users=no] [--volumes=no] [--eventlog=no] [--datetime=<дата публикации события>] [--channels=<список каналов>] [--files=no] [--network=no] [--url=no] [--drives=<all|system|critical|custom>] [--excludes=<список исключений>][--scope=<настраиваемый список папок>] [--retro]
   ```

Если команда `--scan-ioc` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.
Если команда `--scan-ioc` передана с двумя обязательными параметрами одновременно (`--path=<путь к папке с IOC-файлами>` и `<полный путь к IOC-файлу>`), Kaspersky Endpoint Agent выполняет проверку всех переданных IOC-файлов.

Таблица 17. Параметры команд при запуске и настройке стандартных задач поиска IOC

Параметры	Описание
`--scan-ioc`	Обязательный параметр. Запускает стандартную задачу поиска IOC на устройстве.
`--path=<путь к папке с IOC-файлами>`	Путь к папке с IOC-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр `<полный путь к IOC-файлу>`.
`<полный путь к IOC-файлу>`	Полный путь к IOC-файлу с расширением ioc или xml, по которому требуется выполнять поиск. Обязательный параметр, если не задан параметр `--path=<путь к папке с IOC-файлами>`. Передается без аргумента `--path`.
`--process=<no>`	Необязательный параметр. Параметр выключает анализ данных о процессах при проверке. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не учитывает запущенные на устройстве процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>`	Необязательный параметр. Параметр позволяет сузить область анализируемых данных для проверки IOC-документов ProcessItem и FileItem, путем указания конкретного файла. В качестве значения параметра может быть задан: • `<полный путь к исполняемому файлу процесса (ProcessItem)>` – ProcessItem • `<полный путь к файлу>` – FileItem Параметр может быть передан только совместно с аргументами `--process=yes` и `--files=yes`.

Параметры	Описание
`--dnsentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в локальном кеше DNS (IOC-документ DnsEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.
`--arpentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в ARP-таблице (документ ArpEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`--ports=no`	Необязательный параметр. Параметр выключает анализ данных о портах, открытых на прослушивание (документ PortItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.

Параметры	Описание
`--volumes=no`	Необязательный параметр. Параметр выключает анализ данных о томах (документ VolumeItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.
`--eventlog=no`	Необязательный параметр. Параметр выключает анализ данных о записях в журнале событий Windows (документ EventLogItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.

Коды возврата команды `--scan-ioc`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку следующие данные о результатах выполнения задачи:

Таблица 18. Данные, которые программа выводит в командную строку при обнаружении IOC

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные о каждом документе IOC, в котором было найдено совпадение.
`Date`	Дата создания файла, в котором обнаружены маркеры компрометации.
`Created`	Только для FileItem. Время создания объекта, в котором обнаружены маркеры компрометации.
`Pid`	Идентификатор процесса, для которого обнаружены маркеры компрометации.
`Upid`	Уникальный идентификатор процесса, для которого обнаружены маркеры компрометации.
`ParentPid`	Идентификатор родительского объекта, содержащего процесс, для которого обнаружены маркеры компрометации.
`Username`	Имя пользователя, который вносил изменения в объект сканирования.
`StartTime`	Время запуска процесса, для которого обнаружены маркеры компрометации.

Настройка и запуск задачи аудита безопасности

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Вы можете настраивать и запускать задачу аудита безопасности через интерфейс командной строки для следующих источников правил:

- **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**;
- **Конфигурации безопасности и соответствий стандартам для операционных систем**;
- **Пользовательская база правил из файла**.

► *Чтобы настроить и запустить задачу аудита безопасности через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например: `cd C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent`
3. Нажмите на клавишу **Enter**.
4. Введите команду:

   ```
   agent.exe --scan-oval [--source={kl|kl-compl|file}] [--repository=show] [--path={<полный путь и имя архива с OVAL-правилами>|<полный путь к папке, содержащей файлы с OVAL- и XCCDF-правилами>}] [--external-vars=<полный путь и имя ZIP-архива с внешними переменными>] [--mode={all|exclude|include}] [--definitions=<тип уязвимости_01;тип уязвимости_02;тип уязвимости_N>] [--log={none|critical|warning|information|debug}] --result-path=<путь к папке с отчетом>
   ```
5. Нажмите на клавишу **Enter**.

Таблица 19. Параметры команды для настройки и запуска задачи аудита безопасности

Параметр	Описание
`--scan-oval`	Обязательный параметр. Запускает задачу аудита безопасности на устройстве.
`--source`	Определяет источник правил, которые необходимы для аудита безопасности. Доступные значения: • `kl` – база данных уязвимостей Kaspersky ICS CERT для АСУ ТП, входящая в поставку. Доступна для обращения через командную строку после успешного обновления баз и модулей Kaspersky Endpoint Agent. • `kl-compl` – конфигурации безопасности и соответствий стандартам для операционных систем, входящие в поставку. Доступны для обращения через командную строку после успешного обновления баз и модулей Kaspersky Endpoint Agent. • `file` – пользовательская база правил из файла. Если значение параметра не указано, по умолчанию используется источник **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП** (`--source=kl`).

Параметр	Описание
`--repository`	Параметр доступен, если в качестве источника правил выбраны конфигурации безопасности и соответствия стандартам для операционных систем (`--source=kl-compl`). Если параметр указан, то вместо выполнения задачи аудита безопасности Kaspersky Endpoint Agent сохраняет в папку отчета (определяется параметром `--result-path`) XML-файл, в котором перечислены названия имеющихся конфигураций безопасности.
`--path`	Параметр передает путь к файлам с правилами для источника **Пользовательская база правил из файла** (`--source=file`). Доступные значения параметра: • `<полный путь и имя архива с OVAL-правилами>` – указывает полный путь и имя архива с XML-файлом с OVAL-правилами. • `<полный путь к папке, содержащей файлы с OVAL- и XCCDF-правилами>` – указывает полный путь к папке с XML-файлами с OVAL- и / или XCCDF-правилами. OVAL- и XCCDF-правила должны быть сохранены в кодировке UTF-8 без BOM.
`--external-vars`	Параметр указывает полный путь и имя ZIP-архива с XML-файлом с внешними переменными для OVAL-правил. Параметр доступен, если источник содержит только OVAL-правила.
`--mode`	Параметр определяет режим проверки на уязвимости. Параметр доступен, если источник содержит только OVAL-правила. Доступные значения параметра: • `all` – выполняется проверка на все уязвимости, указанные в источнике. • `exclude` – выполняется проверка на уязвимости, указанные в источнике, кроме указанных с помощью параметра `--definitions`. • `include` – выполняется проверка на уязвимости, которые указаны с помощью параметра `--definitions`. Если значение параметра не задано, по умолчанию используется режим `all`.

Параметр	Описание
`--definitions`	Параметр определяет список типов уязвимостей, разделенных точкой с запятой, которые необходимо проверить или исключить из проверки. Параметр доступен, если источник содержит только OVAL-правила. Например: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. Используется совместно с параметром `--mode=include` или `--mode=exclude`.
`--log`	Параметр определяет режим записи в журнал событий о выполнении задачи. Доступные значения: • `none` – запись в журнал отключена; • `critical` – только критические события; • `warning` – критические и предупреждающие события; • `information` – критические, предупреждающие и информационные события; • `debug` – критические, предупреждающие, информационные и отладочные события. Если значение параметра не задано, по умолчанию используется режим `critical`. Файл журнала в формате LOG сохраняется в папку, указанную с помощью параметра `--result-path`.
`--result-path`	Обязательный параметр. Параметр указывает путь к папке, куда будет записан отчет сканирования в формате XML. Имя файла содержит имя узла, дату и время выполнения задачи. В эту же папку сохраняется журнал событий о выполнении задачи в формате LOG. Если параметр не задан, выполнение задачи завершается с ошибкой.

Коды возврата команды `--scan-oval`:

- `0` – команда выполнена успешно;
- `1` – общая ошибка.

Если команда выполнена успешно (код `0`), в папке, указанной с помощью параметра `--result-path`, создается отчет в формате XML и, если был определен параметр `--log`, журнал событий о выполнении задачи в формате LOG.

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

► *Чтобы создать отпечаток сертификата подписи файлов с OVAL-или XCCDF-правилами:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt `cmd.exe`) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл ovaldbmgr.exe.

   Например: `cd C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\Tools`
3. Нажмите на клавишу **Enter**.
4. В зависимости от размещения сертификата выполните одну из следующих команд:
   - Для создания сертификата с последующим размещением в System Storage Local Machine:

     `ovaldbmgr.exe --signer=make-cert --subject=<имя_сертификата>`
   - Для создания сертификата с последующим размещением в контейнере PFX:

     `ovaldbmgr.exe --signer=make-cert --subject=<имя_сертификата> --export --pwd=<пароль_для_доступа_к_PFX-контейнеру> --pfx=<полный_путь_и_имя_файла_PFX-контейнера>`
5. Нажмите на клавишу **Enter**

   В случае успешного формирования сертификата в командной строке возвращается отпечаток сертификата.

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

► *Чтобы создать инсталляционный пакет Kaspersky Security Center в виде подписанного архива с OVAL- или XCCDF-правилами:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt `cmd.exe`) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл ovaldbmgr.exe.

   Например: `cd C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\Tools`
3. Нажмите на клавишу **Enter**.

4. В зависимости от размещения сертификата выполните одну из следующих команд:
   - Если сертификат подписи расположен в System Storage Local Machine:

     ```
     ovaldbmgr.exe --make-package --command={replace|merge} --subject=<имя сертификата> --output=<полный путь> --source=<полный путь> <полный путь к файлу с OVAL-или XCCDF-правилами>
     ```

   - Если сертификат подписи расположен в контейнере PFX:

     ```
     ovaldbmgr.exe --make-package --command={replace|merge} --pfx=<полный путь к контейнеру pfx> --pwd=<пароль доступа к контейнеру pfx> --output=<полный путь> --source=<полный путь> <полный путь к файлу с OVAL- или XCCDF-правилами>
     ```

5. Нажмите на клавишу **Enter**.

Таблица 20. Параметры команды для создания инсталляционного пакета Kaspersky Security Center

Параметры	Описание
`--make-package`	Обязательный параметр. Создает архив с файлами.
`--command={replace|merge}`	Обязательный параметр. Параметр определяет режим развертывания пакета в Kaspersky Security Center. Доступные значения: • `replace` – замена существующего в хранилище Kaspersky Security Center инсталляционного пакета на создаваемый. • `merge` – объединение создаваемого инсталляционного пакета с уже существующим в хранилище Kaspersky Security Center пакетом. Если значение параметра не задано, команда завершается с ошибкой.
`--pfx=<полный путь к контейнеру pfx>`	Обязательный параметр. Параметр указывает полный путь к контейнеру PFX, который содержит сертификат подписи (см. раздел "Создание отпечатка сертификата подписи для файлов с OVAL- или XCCDF-правилами" на стр. 262).
`--pwd=<пароль доступа к контейнеру pfx>`	Обязательный параметр. Параметр передает пароль доступа к контейнеру PFX.

Параметры	Описание
`--subject=<имя сертификата>`	Обязательный параметр. Параметр передает имя сертификат подписи. Если указано имя несуществующего сертификата подписи, команда завершается с ошибкой.
`--output=<полный путь>`	Обязательный параметр. Параметр указывает полный путь к папке, в которой в результате выполнения команды будет создан инсталляционный пакет.
`--source=<полный путь>`	Параметр указывает полный путь к папке, в которой содержится папка с OVAL- и XCCDF-правилам, которые вы желаете включить в пакет Kaspersky Security Center.
`<полный путь к файлу с OVAL- или XCCDF-правилами>`	Параметр указывает полный путь к файлам с OVAL- или XCCDF-правилами в формате XML, которые вы желаете включить в пакет Kaspersky Security Center. OVAL- и XCCDF-правила должны быть сохранены в кодировке UTF-8 без BOM. Файл с OVAL- или XCCDF-правилами должен быть расположен в папке, которая расположена в еще одной папке. Например: C:\Users\UserName\Desktop\folder\subfolder\OvalRules.xml Вы можете указать несколько значений параметра через пробел. Чтобы указать файлы с OVAL- или XCCDF-правилами, можно выбрать один из следующих вариантов: • Задать только значение параметра `--source=<полный путь>`. • Указать одно или несколько значений `<полный путь к файлу с OVAL- или XCCDF-правилами>` через пробел. • Одновременно задать значение параметра `--source=<полный путь>` и указать одно или несколько значений `<полный путь к файлу с OVAL- или XCCDF-правилами>` через пробел. Если не задано ни одного значения `<полный путь к файлу с OVAL- или XCCDF-правилами>` и не задан параметр `--source=<полный путь>`, задача завершится с ошибкой.

В результате выполнения команды Kaspersky Endpoint Agent создает:

- Архив с именем package.zip в папке, указанной в значении параметра `--output=<полный путь>`. Архив содержит следующие файлы:
  - Один или несколько ZIP-файлов для каждого из пользовательских файлов с OVAL- или XCCDF-правилами. Каждый архив содержит один XML-файл с правилами и файл подписи этого XML-файла.
  - Файл ovaldbmgr.kud для развертывания пакета Kaspersky Security Center.
  - Утилиту развертывания ovaldbmgr.exe.
- Отпечаток сертификата, которым подписан архив package.zip.

  Вы можете указать отпечаток в параметрах задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center в качестве источника правил (см. раздел "Настройка параметров задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center" на стр. 225).

См. также

Создание отпечатка сертификата подписи для файлов с OVAL- или XCCDF-правилами.....262

Управление сканированием файлов и процессов по YARA-правилам

Сканирование YARA представляет собой процессы, которые вы можете создавать и настраивать вручную через интерфейс командной строки. Для запуска сканирования используются YARA-файлы.

В задаче сканирования YARA можно указать только файл с YARA-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи сканирования YARA.

► *Чтобы запустить сканирование YARA через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды cd перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду cd "`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`" и нажать на клавишу **Enter**.

3. Выполните следующую команду и нажмите на клавишу **Enter**:

   ```
   agent.exe --scan-yara [<путь к yara-файлу>] [--path=<путь к папке с yara-правилами>] [--fast-scan] [--tag-hint=<тег правила>] [--id-hint=<идентификатор правила>] [--max-rules=<максимальное количество правил сканирования>] [--timeout=<остановка сканирования по истечении указанного времени в секундах>] [--recursive] [--scan_folders [<список папок для сканирования>] [--scan-memory] [--scan-process <имя процесса>][--max-size=<размер файла в байтах>] [--excludes <список объектов для сканирования>] [--includes <список объектов для сканирования>]
   ```

   Если команда `--scan-yara` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

Описание параметров сканирования представлено в следующей таблице.

Таблица 21. Параметры команд при запуске и настройке сканирования YARA

Параметры	Описание
`--scan-yara [<полный путь к yara-файлу>]`	Обязательный параметр. Запускает сканирование YARA на устройстве. Проверка выполняется по правилам из YARA-файлов с расширением yara или yar. Параметру может быть передано несколько значений через пробел. Хотя бы одно значение <полный путь к yara-файлу> должен быть указано, если не задан параметр --path. Если в дополнение к аргументам параметра --scan-yara также задан параметр --path, при сканировании используются как указанные в аргументах файлы с YARA-правилами, так и файлы из папки параметра --path.
`--path=<путь к папке с yara-файлами>`	Путь к папке с YARA-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр <полный путь к yara-файлу>.
`--fast-scan`	Необязательный параметр. Параметр запускает проверку в режиме быстрого сканирования. Для каждого объекта сканирования в журнале фиксируется одно вхождение обнаруженного маркера, при этом дубликаты обнаруженных маркеров не отображаются в журнале. Использование данного параметра позволяет сократить время проверки больших файлов. Если параметр не передан, выполняется стандартная проверка и дубликаты обнаруженных маркеров отображаются в журнале.
`--tag-hint=<тег правила>`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным тегом. Можно указать только одно значение параметра. Правила без тегов или с другими тегами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.

Параметры	Описание
--id-hint=<идентификатор правила>	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным идентификатором. Можно указать только одно значение параметра. Правила без идентификаторов или с другими идентификаторами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
--max-rules=<максимальное количество правил сканирования>	Необязательный параметр. Параметр задаёт лимит уникальных сработавших правил обнаружения, при превышении которого проверка прекращается. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
Параметры	**Описание**
--timeout=<остановка сканирования по истечении указанного времени в секундах>	Необязательный параметр. Параметр указывает продолжительность проверки в секундах. По истечении указанного времени проверка будет остановлена. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
--recursive	Необязательный параметр. Параметр запускает рекурсивную проверку вложенных папок в рамках значения [<список папок для сканирования>].

Параметры	Описание
`--scan_folders [<список папок для сканирования>]`	Дополнительно в параметрах `--scan-folders`, `--excludes`, `--includes` в качестве аргументов можно указывать ссылки на файлы аргументов с префиксом "`@`". Файлы аргументов - это текстовые файлы в кодировке UTF-8, которые содержат списки объектов для обработки с использованием соответствующего параметра в командной строке. Пример: Файл my_rules.txt содержит две строки: • c:\trusted*.* • *.abc Файл rules2.txt содержит одну строку: • img_*.jpg В случае запуска сканирования с параметрами вида "`--scan-folders --exclude *.txt @my_rules.txt *.xml @rules2.txt`" будет проведено сканирование всех файлов на всех дисках, за исключением файлов с расширениями "`txt`", файлов в папке "`c:\trusted`", файлов с расширением "`abc`", файлов с расширением "`xml`" и файлов по маске "`img_*.jpg`". Необязательный параметр. Параметр запускает сканирование файлов по указанному списку папок. Если значение параметра <`список папок для сканирования`> не задано, сканирование производится рекурсивно на всех локальных дисках, кроме сетевых, облачных и подключаемых.
`--scan-memory`	Необязательный параметр. Параметр запускает сканирование памяти всех запущенных процессов.
`--scan-process <имя процесса>`	Необязательный параметр. Параметр запускает сканирование памяти только для указанных процессов. Для значения <`имя процесса`> поддерживаются стандартные маски "`?`" и "`*`".

Параметры	Описание
`--max-size=<размер файла в байтах>`	Необязательный параметр. Сканирование выполняется только для тех файлов, размер которых не превышает заданное значение. Файлы большего размера пропускаются при сканировании.
`--includes <список объектов для сканирования>`	Дополнительно в параметрах `--scan-folders`, `--excludes`, `--includes` в качестве аргументов можно указывать ссылки на файлы аргументов с префиксом "`@`". Файлы аргументов - это текстовые файлы в кодировке UTF-8, которые содержат списки объектов для обработки с использованием соответствующего параметра в командной строке. Пример: Файл my_rules.txt содержит две строки: • c:\trusted*.* • *.abc Файл rules2.txt содержит одну строку: • img_*.jpg В случае запуска сканирования с параметрами вида "`--scan-folders --exclude *.txt @my_rules.txt *.xml @rules2.txt`" будет проведено сканирование всех файлов на всех дисках, за исключением файлов с расширениями "`txt`", файлов в папке "`c:\trusted`", файлов с расширением "`abc`", файлов с расширением "`xml`" и файлов по маске "`img_*.jpg`". Необязательный параметр. Параметр позволяет ограничить область сканирования. Можно задать несколько значений параметра через пробел. Доступные значения: • имя файла; • путь к файлу; • маска имени файла; • маска пути к файлу. Передается с параметром --scan-folders. Пример: --scan-folders c:*.* --recursive --includes *.exe c:\temp*.* *.dll – сканирование будет проведено для всех файлов с расширениями "exe" и "dll" на диске C:, а также будут просканированы рекурсивно все файлы в папке C:\temp

Параметры	Описание
`--excludes <список объектов для сканирования>`	Дополнительно в параметрах `--scan-folders`, `--excludes`, `--includes` в качестве аргументов можно указывать ссылки на файлы аргументов с префиксом "`@`". Файлы аргументов - это текстовые файлы в кодировке UTF-8, которые содержат списки объектов для обработки с использованием соответствующего параметра в командной строке. Пример: Файл my_rules.txt содержит две строки: • c:\trusted*.* • *.abc Файл rules2.txt содержит одну строку: • img_*.jpg В случае запуска сканирования с параметрами вида "`--scan-folders --exclude *.txt @my_rules.txt *.xml @rules2.txt`" будет проведено сканирование всех файлов на всех дисках, за исключением файлов с расширениями "`txt`", файлов в папке "`c:\trusted`", файлов с расширением "`abc`", файлов с расширением "`xml`" и файлов по маске "`img_*.jpg`". Необязательный параметр. Параметр исключает указанные файлы или папки из сканирования. Можно задать несколько значений параметра через пробел. Доступные значения: • имя файла; • путь к файлу; • маска имени файла; • маска пути к файлу. Передается с параметром --scan-folders. Пример: --scan-folders c:*.* --excludes readme.txt c:\trusted*.* *.xml – при сканировании будут пропущены файлы readme.txt, все файлы из папки C:\trusted, а также все файлы с расширением xml в корневой папке на диске C:.

Коды возврата команды `--scan-yara`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `5` – не найден один или несколько файлов с YARA-правилами из указанных в значении параметра.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку результаты сканирования. Описание результатов сканирования представлено в следующей таблице:

Таблица 22. Данные, которые программа выводит в командную строку при обнаружении сигнатур YARA.

`Offset`	Смещение в объекте, для которого Kaspersky Endpoint Agent выполняет сканирование.
`Data`	Сигнатуры, которые Kaspersky Endpoint Agent ищет во время сканирования.
`Object Name`	Имя объекта сканирования.
`Rule Name`	Имя правила, которое используется во время сканирования.

Управление сканированием объектов точек автозапуска по YARA-правилам

Сканирование YARA для точек автозапуска представляет собой процессы, которые вы можете создавать и настраивать вручную через интерфейс командной строки. Для запуска сканирования используются YARA-файлы.

В задаче сканирования YARA для объектов точек автозапуска можно указать только файл с YARA-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи сканирования YARA.

По умолчанию сканирование объектов по правилам YARA осуществляется для следующих типов точек автозапуска:

- Logon
- Run

- Explorer
- Shell
- Office
- Internet Explorer
- Tasks
- Services
- Drivers
- Telephony
- Cryptography
- Debuggers
- COM
- Session Manager
- Network
- LSA
- Applications
- Codecs
- Shellex
- Unspecified

► *Чтобы запустить сканирование YARA для точек автозапуска через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **Enter**.
3. Выполните следующую команду и нажмите на клавишу **Enter**:

   ```
   agent.exe --scan-yara [<путь к yara-файлу>] [--path=<путь к папке с yara-правилами>] --scan-autoruns=yes [--fast-scan] [--tag-hint=<тег правила>] [--id-hint=<идентификатор правила>] [--max-rules=<максимальное количество правил сканирования>] [--timeout=<остановка сканирования по истечении указанного времени в секундах>] [--max-size=<размер файла в байтах>] [--exclude-autoruns=COM]
   ```

   Если команда `--scan-yara --scan-autoruns` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

Описание параметров сканирования представлено в следующей таблице.

Таблица 23. Параметры команд при запуске и настройке сканирования YARA

Параметры	Описание
`--scan-yara [<полный путь к yara-файлу>]`	Обязательный параметр. Запускает сканирование YARA для файлов точек автозапуска на устройстве. Проверка выполняется по правилам из YARA-файлов с расширением yara или yar. Параметру может быть передано несколько значений через пробел. Хотя бы одно значение <полный путь к yara-файлу> должно быть указано, если не задан параметр --path. Если в дополнение к аргументам параметра `--scan-yara --scan-autoruns` также задан параметр `--path`, при сканировании используются как указанные в аргументах файлы с YARA-правилами, так и файлы из папки параметра `--path`.
`--path=<путь к папке с yara-файлами>`	Путь к папке с YARA-файлами, по которым требуется выполнять поиск файлов точек автозапуска. Обязательный параметр, если не задан параметр <полный путь к yara-файлу>.
`--scan-autoruns=yes`	Обязательный параметр. Параметр обращается к точкам автозапуска и сканирует объекты для всех типов точек автозапуска по указанным YARA-правилам. Для запуска сканирования необходимо передать значение `yes`. Если значение параметра не указано, параметр будет проигнорирован.
`--fast-scan`	Необязательный параметр. Параметр запускает проверку в режиме быстрого сканирования. Для каждого объекта сканирования в журнале фиксируется одно вхождение обнаруженного маркера, при этом дубликаты обнаруженных маркеров не отображаются в журнале. Использование этого параметра позволяет сократить время проверки больших файлов. Если параметр не передан, выполняется стандартная проверка и дубликаты обнаруженных маркеров отображаются в журнале.

Параметры	Описание
`--tag-hint=<тег правила>`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным тегом. Можно указать только одно значение параметра. Правила без тегов или с другими тегами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--id-hint=<идентификатор правила>`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным идентификатором. Можно указать только одно значение параметра. Правила без идентификаторов или с другими идентификаторами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--max-rules=<максимальное количество правил сканирования>`	Необязательный параметр. Параметр задает лимит уникальных сработавших правил обнаружения, при превышении которого проверка прекращается. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--timeout=<остановка сканирования по истечении указанного времени в секундах>`	Необязательный параметр. Параметр указывает продолжительность проверки каждого объекта в секундах. По истечении указанного времени проверка будет остановлена. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--max-size=<размер файла в байтах>`	Необязательный параметр. Сканирование выполняется только для тех файлов, размер которых не превышает заданное значение. Файлы большего размера пропускаются при сканировании.

Параметры	Описание
`--exclude-autoruns=<список объектов для сканирования>`	Необязательный параметр. Параметр исключает из сканирования файлы в указанной точке автозапуска. Можно задать несколько значений параметра через пробел. Доступное значение: COM (в настоящее время поддерживается исключение только этого типа точек автозапуска). Пример: `--exclude-autoruns=COM` При сканировании будут пропущены файлы из области точки автозапуска COM. **Ограничения** В полученных списках точек автозапуска для COM-объектов могут отсутствовать сборки компонентов, написанные на .NET ввиду особенностей их регистрации в системе.

Коды возврата команды `--scan-yara`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `5` – не найден один или несколько файлов с YARA-правилами из указанных в значении параметра.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку результаты сканирования. Описание результатов сканирования представлено в следующей таблице.

Таблица 24. Данные, которые программа выводит в командную строку при обнаружении сигнатур YARA.

`Offset`	Смещение в объекте, для которого Kaspersky Endpoint Agent выполняет сканирование.
`Data`	Сигнатуры, которые Kaspersky Endpoint Agent ищет во время сканирования.
`Object Name`	Имя объекта сканирования.
`Rule Name`	Имя правила, которое используется во время сканирования.

Управление Запретом запуска

► *Чтобы управлять Запретом запуска через интерфейс командной строки:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --prevention=disable`, чтобы отключить запрет запуска.
   - `agent.exe --prevention=show`, чтобы вывести в командную строку текущие параметры Запрета запуска.

Коды возврата команды `--prevention`:

- -1 – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 9 – неверная операция (например, попытка отключения Запрет запуска, если Запрет запуска уже отключен).

kaspersky

Создание дампа памяти

Вы можете создать дамп памяти компьютера, на котором установлена программа Kaspersky Endpoint Agent.

Перед созданием дампа памяти рекомендуем завершить процессы критически важных программ. После создания дампа памяти рекомендуем перезагрузить компьютер, для которого создан дамп памяти.

► *Чтобы создать дамп памяти через интерфейс командной строки Kaspersky Endpoint Agent:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите команду:

   `agent.exe --memory-dump --path=<путь к локальной или сетевой папке, в которой вы хотите сохранить дамп памяти> [--user=<имя пользователя> --pwd=<пароль>]`.

   Имя пользователя и пароль необходимы, если доступ к папке для сохранения дампа памяти защищен паролем.

   Убедитесь, что папка для сохранения дампа памяти, доступна для записи. Иначе файл дампа не будет создан.
4. Нажмите на клавишу **ENTER**.

   В указанной папке Kaspersky Endpoint Agent создаст файл дампа памяти с названием MemoryDump_<имя хоста>_<дата и время старта записи файла>.dmp.

Таблица 25. Параметры команды для создания дампа памяти

Параметр	Описание
`--path`	Обязательный параметр. Параметр передает полный путь к локальной или сетевой папке, в которую программа сохраняет дамп памяти. Имя сетевой папки должно быть указано в UNC-формате.
`--user`	Параметр передает логин для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа памяти необходим доступ к папке для учетной записи SYSTEM.
`--pwd`	Параметр передает пароль для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа памяти необходим доступ к папке для учетной записи SYSTEM.

Коды возврата команды `--memory-dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Kaspersky Endpoint Agent не выполняет шифрование и сжатие файла дампа памяти. Если необходимо, вы можете настроить шифрование и сжатие папки для сохранения дампа памяти с помощью сторонних инструментов.

Чтобы Kaspersky Endpoint Agent мог сохранять файл дампа памяти в сетевую папку в зашифрованном виде, требуется настроить использование SMB-протокола версии 3 или выше.

kaspersky

Создание дампа диска

Вы можете создать дамп физического или логического диска компьютера, на котором установлена программа Kaspersky Endpoint Agent.

► *Чтобы создать дамп диска через интерфейс командной строки Kaspersky Endpoint Agent:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

   Введите команду:

   ```
   agent.exe --disk-image --volume=<имя диска> [--format=<формат файла, RAW или EWF>] [--max-size=<размер в байтах>] [--segment-size=<размер в байтах>] --path=<путь к локальной или сетевой папке, в которой вы хотите сохранить дамп диска> [--user=<имя пользователя> --pwd=<пароль>]
   ```

   Имя пользователя и пароль необходимы, если доступ к папке для сохранения дампа диска защищен паролем.

   > Убедитесь, что папка для сохранения дампа диска, доступна для записи. Иначе файл дампа не будет создан.

3. Нажмите на клавишу **ENTER**.

   В указанной папке Kaspersky Endpoint Agent создаст файл дампа диска с названием в формате <имя диска>_<дата и время старта записи файла>.<расширение>.

   Расширение файла дампа диска может быть следующим:

   - Если в команде для создания дампа диска указан формат RAW (`--format=RAW`):
     - если дамп диска не разделен (не задан параметр `--segment-size`), то файл дампа диска имеет расширение raw;
     - если дамп диска разделен (задан параметр `--segment-size`), то части дампа имеют расширение 001, 002, 003 и далее по порядку до 999.
   - Если в команде для создания дампа диска указан формат EWF (`--format=EWF`):
     - если дамп диска не разделен (не задан параметр `--segment-size`), то файл дампа диска имеет расширение E01;
     - если дамп диска разделен (задан параметр `--segment-size`), то части дампа имеют расширение E01, E02, ..., E99; EAA, EAB, ..., EAZ; FAA, FAB, ..., FZZ, <...>; ZAA, ZAB, ..., ZZZ.

Таблица 26. Параметры команды для создания дампа диска

Параметр	Описание
`--volume`	Обязательный параметр. Параметр передает номер физического диска или имя логического диска, для которого будет создан дамп. Формат номера физического диска: \??\PHYSICALDRIVEN или PHYSICALDRIVEN, где N – порядковый номер диска. Например: \??\PHYSICALDRIVE0, PHYSICALDRIVE1. Формат имени логического диска: N:, где N – буквенное обозначение логического диска. Например, C:. Если вы создаете дамп для логического диска, с которого осуществляется загрузка операционной системы, в качестве имени диска используйте переменную %SystemDrive%.
`--format`	Параметр передает формат файла с дампом диска. Возможные значения: RAW или EWF. Если параметр не задан, программа создает дамп диска в формате RAW.
`--max-size`	Параметр передает максимальное допустимое значение размера дампа диска в байтах. Если параметр не задан, программа создает дамп диска с максимальным размером 1 099 511 627 776 байт.
`--segment-size`	Параметр передает максимальное значение размера частей дампа диска в байтах. При этом минимальный размер частей дампа должен быть больше 33 554 432 байт. Если параметр задан, программа разбивает дамп диска на части указанного размера и архивирует их. Размер архивированных частей дампа меньше указанного с помощью параметра значения. Если параметр не задан, программа не производит разбиение дампа диска на части.
`--path`	Обязательный параметр. Параметр передает полный путь к локальной или сетевой папке, в которую программа сохраняет дамп диска. Имя сетевой папки должно быть указано в UNC-формате.
`--user`	Параметр передает логин для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа диска необходим доступ к папке для учетной записи SYSTEM.
`--pwd`	Параметр передает пароль для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа диска необходим доступ к папке для учетной записи SYSTEM.

Коды возврата команды `--memory-dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Kaspersky Endpoint Agent не выполняет шифрование и сжатие файла дампа памяти. Если необходимо, вы можете настроить шифрование и сжатие папки для сохранения дампа памяти с помощью сторонних инструментов.

Чтобы Kaspersky Endpoint Agent мог сохранять файл дампа памяти в сетевую папку в зашифрованном виде, требуется настроить использование SMB-протокола версии 3 или выше.

Указание источника параметров Сетевой изоляции и Запрета запуска

Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска с указанного с помощью командной строки источника, если неактивна политика Kaspersky Endpoint Agent в Kaspersky Security Center.

► *Чтобы указать источник параметров Сетевой изоляции и Запрета запуска:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите команду:

   ```
   agent.exe --message-broker=global --priority-server=<kata|kics>
   ```

4. Нажмите на клавишу **ENTER**.

   Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска по следующим правилам:

   - Если настроена интеграция только с сервером KATA, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере с установленным KATA Central Node.
   - Если настроена интеграция только с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере с установленным KICS for Networks.
   - Если настроена интеграция и с сервером KATA, и с сервером KICS for Networks, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные на сервере, указанном с помощью параметра `--priority-server`.
   - Если интеграция с сервером KATA и сервером KICS for Networks не настроена, Kaspersky Endpoint Agent применяет параметры Сетевой изоляции и Запрета запуска, определенные локально на узле с установленным Kaspersky Endpoint Agent с помощью командной строки или в свойствах узла в Консоли администрирования Kaspersky Security Center или Kaspersky Security Center Web Console.

Управление параметрами интеграции с SIEM

► *Чтобы управлять параметрами интеграции Kaspersky Endpoint Agent с SIEM через интерфейс командной строки Kaspersky Endpoint Agent:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду:

   ```
   agent.exe --message-broker=<enable|disable|show> --type=<syslog> [--tls=<yes|no>] --servers=<tcp|udp>://<адрес>:<порт>[;<tcp|udp>://<адрес>:<порт>[; …]] [--timeout=<максимальное время ожидания ответа SIEM-сервера] [--pinned-certificate=<полный путь к файлу TLS-сертификата>] [--client-certificate=<полный путь к PFX-файлу>] --client-password=<пароль для доступа к PFX-файлу>
   ```
4. Нажмите на клавишу **ENTER**.

Таблица 27. Параметры команды `--message-broker` для управления интеграцией с SIEM

Параметр	Описание
`--message-broker=<enable|disable|show>`	Обязательный параметр. Позволяет включить, выключить и просмотреть статус интеграции Kaspersky Endpoint Agent с SIEM. • `--message-broker=<enable>` включает интеграцию. • `--message-broker=<disable>` выключает интеграцию. • `--message-broker=<show>` отображает состояние интеграции Kaspersky Endpoint Agent с SIEM.
`--type=<syslog>`	Обязательный параметр. Указывает, что настраивается интеграция программы Kaspersky Endpoint Agent с SIEM-системой по протоколу syslog.
`--tls=<yes|no>`	Необязательный параметр. Позволяет включить или выключить использование доверенного соединения Kaspersky Endpoint Agent с SIEM-сервером. • `--tls=<yes>` включает использование доверенного соединения. • `--tls=<no>` выключает использование доверенного соединения.
`--servers=<tcp|udp>://<адрес>:<порт>[;<tcp|udp>://<адрес>:<порт>[; …]]`	Обязательный параметр. Позволяет добавить один или несколько SIEM-серверов. Если протокол передачи данных не указан, по умолчанию используется TCP. Kaspersky Endpoint Agent подключается к первому серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму серверу и так далее по списку.
`--timeout=<максимальное время ожидания ответа SIEM-сервера>`	Необязательный параметр. Позволяет задать максимальное время ожидания ответа SIEM-сервера в миллисекундах. Значение по умолчанию равно 10000 миллисекунд.
`--pinned-certificate=<полный путь к файлу TLS-сертификата>`	Обязательный параметр, если передан параметр `--tls` со значением `<yes>`. Позволяет добавить TLS-сертификат соединения Kaspersky Endpoint Agent с SIEM-сервером.
`--client-certificate=<полный путь к PFX-файлу>`	Необязательный параметр. Позволяет добавить файл формата PFX, в котором в зашифрованном виде хранится сертификат клиента для защиты соединения Kaspersky Endpoint Agent с SIEM-сервером.
`--client-password=<пароль для доступа к PFX-файлу>`	Обязательный параметр, если передан параметр `--client-certificate`. Позволяет указать пароль для доступа к PFX-файлу.

Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA

Kaspersky Industrial CyberSecurity for Nodes 3.2 может передавать состояние безопасности (сведения об обнаруженных угрозах) автоматизированной системы управления технологическим процессом (АСУ ТП) в Kaspersky Security Center. Если настроена передача сведений об угрозах в Kaspersky Security Center, вы можете настроить в системе SCADA получение информации об угрозах АСУ ТП из Kaspersky Security Center.

Просмотр состояния безопасности АСУ ТП в Kaspersky Security Center

► *Чтобы просмотреть состояние безопасности АСУ ТП в Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите узел **Управляемые устройства**.
3. В списке компьютеров выберите компьютер, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes 3.2.

Информация о состоянии безопасности отобразится в панели результатов справа.

Статус компьютера с Kaspersky Industrial CyberSecurity for Nodes 3.2 отображает состояние безопасности АСУ ТП. Цвет значка компьютера соответствует одному из двух возможных состояний безопасности АСУ ТП:

- Зеленый: OK. На компьютере с Kaspersky Industrial CyberSecurity for Nodes 3.2 нет неподтвержденных событий с критическим уровнем важности (инцидентов Kaspersky Security Center).
- Красный: критический. На компьютере с Kaspersky Industrial CyberSecurity for Nodes 3.2 есть неподтвержденные события с критическим уровнем важности (инциденты Kaspersky Security Center).

kaspersky

Просмотр состояния безопасности АСУ ТП через систему SCADA

► *Чтобы настроить получение и отображение состояния безопасности АСУ ТП в системе SCADA, выполните следующие действия:*

1. Установите Kaspersky Security Gateway. (см. раздел "Установка Kaspersky Security Gateway с помощью мастера установки" на стр. 335)
2. Настройте подключение к системе SCADA (см. раздел "Настройка подключения к системе SCADA" на стр. 877) и использование протоколов связи (см. раздел "Настройка параметров передачи данных с использованием протоколов связи" на стр. 879) для передачи сообщений и отображения информации о состоянии защиты промышленных сетей и сетевых узлов, полученной от Kaspersky Industrial CyberSecurity for Nodes.

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы компьютера, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.

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

Консоль Kaspersky Industrial CyberSecurity for Nodes

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

В одну Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток Kaspersky Industrial CyberSecurity for Nodes, чтобы управлять из нее защитой нескольких компьютеров, на которых установлена Kaspersky Industrial CyberSecurity for Nodes.

Консоль Kaspersky Industrial CyberSecurity for Nodes входит в набор компонентов "Средства администрирования".

Утилита командной строки

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

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

Kaspersky Security Center

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

Вам потребуется установить следующие компоненты:

- Модуль интеграции с Агентом администрирования Kaspersky Security Center. Этот компонент входит в набор программных компонентов Kaspersky Industrial CyberSecurity for Nodes. Он обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes с Агентом администрирования. Установите Модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемом компьютере.
- Агент администрирования Kaspersky Security Center. Установите его на каждом защищаемом компьютере. Этот компонент будет обеспечивать взаимодействие между Kaspersky Industrial CyberSecurity for Nodes, установленным на компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- Плагин управления Kaspersky Industrial CyberSecurity for Nodes. Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Industrial CyberSecurity for Nodes. Он обеспечивает интерфейс управления программой через Консоль администрирования Kaspersky Security Center. Файл установки плагина \plugin\klcfginst.exe входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes.
- Веб-плагин управления Kaspersky Industrial CyberSecurity for Nodes. Дополнительно на компьютер, на котором установлена Kaspersky Security Center Web Console, установите веб-плагин управления Kaspersky Industrial CyberSecurity for Nodes. Он обеспечивает интерфейс управления программой через Kaspersky Security Center Web Console. Архив для установки веб-плагина \plugin\archive.zip входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

Установка программы

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

В этом разделе

kaspersky

Планирование установки программы

В этом разделе описаны средства администрирования Kaspersky Industrial CyberSecurity for Nodes, особенности установки Kaspersky Industrial CyberSecurity for Nodes с помощью мастера установки (см. раздел "Установка программы с помощью мастера" на стр. 295), из командной строки (см. раздел "Установка программы из командной строки" на стр. 307), с помощью Kaspersky Security Center (см. раздел "Установка программы с помощью Kaspersky Security Center" на стр. 323) и через групповые политики Active Directory (см. раздел "Установка программы через групповые политики Active Directory" на стр. 328).

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

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Industrial CyberSecurity for Nodes и для настройки программы.
2. Определите, какие программные компоненты требуется установить (см. раздел "Коды программных компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows" на стр. 308).
3. Выберите способ установки.

В этом разделе

Выбор средств администрирования

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

Консоль Kaspersky Industrial CyberSecurity for Nodes

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

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

Консоль программы входит в набор компонентов "Средства администрирования".

Утилита командной строки

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

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

Kaspersky Security Center

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

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center**. Этот компонент входит в группу программных компонентов Kaspersky Industrial CyberSecurity for Nodes. Он позволяет Kaspersky Industrial CyberSecurity for Nodes взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемый компьютер.
- **Агент администрирования Kaspersky Security Center**. Установите его на каждом защищаемом компьютере. Этот компонент будет обеспечивать взаимодействие между программой Kaspersky Industrial CyberSecurity for Nodes, установленной на защищаемом компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин управления Kaspersky Industrial CyberSecurity for Nodes 3.2**. Дополнительно на защищаемом компьютере, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Industrial CyberSecurity for Nodes для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления \plugin\klcfginst.exe входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Коды программных компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows" на стр. 308), необходимо выбрать способ установки программы.

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

- Потребуется ли вам задать специальные параметры установки Kaspersky Industrial CyberSecurity for Nodes или вы будете использовать рекомендуемые параметры установки (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 314).
- Будут ли параметры установки едиными для всех защищаемых компьютеров или индивидуальными для каждого защищаемого компьютера.

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

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

Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Программные компоненты Kaspersky Industrial CyberSecurity for Nodes" на стр. 309) из файла \exec\setup.exe, входящего в комплект поставки, на защищаемом компьютере.
- Консоль Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Установка Консоли Kaspersky Industrial CyberSecurity for Nodes" на стр. 298) из файла \client\setup.exe, входящего в комплект поставки, на защищаемом компьютере или другом устройстве в локальной сети.

Запуск из командной строки файла пакета установки с параметрами установки

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

Вы можете установить Консоль программы на защищаемом компьютере или на рабочем месте администратора.

Вы также можете использовать команды для установки Kaspersky Industrial CyberSecurity for Nodes и Консоли программы (см. раздел "Установка программы из командной строки" на стр. 307).

Централизованная установка через Kaspersky Security Center

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

Защищаемые компьютеры, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center (см. раздел "Установка программы с помощью Kaspersky Security Center" на стр. 323), могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене, а также вообще не принадлежать ни к одному домену.

Централизованная установка через групповые политики Active Directory

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

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

Защищаемые компьютеры, на которых программа Kaspersky Industrial CyberSecurity for Nodes была установлена с помощью групповых политик Active Directory (см. раздел "Установка программы через групповые политики Active Directory" на стр. 328), должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске защищаемого компьютера, перед входом в Microsoft Windows.

kaspersky

Обновление Kaspersky Industrial CyberSecurity for Nodes

Обновление до Kaspersky Industrial CyberSecurity for Nodes 3.2 доступно для программы версии 2.6 и выше. Обновление выполняется путем установки новой версии программы поверх установленной версии программы и не требует перезагрузки компьютера.

По умолчанию программа создает новую папку установки с именем новой версии программы на основе пути к существующей папке установки программы. Вы можете вручную задать новый путь для папки установки программы.

В процессе обновления Kaspersky Industrial CyberSecurity for Nodes до версии 3.2 установленная раннее версия программы автоматически удаляется.

Если у вас установлена Kaspersky Industrial CyberSecurity for Nodes версии ниже 2.6, перед установкой новой версии программы необходимо сначала удалить установленную программу.

При обновлении Kaspersky Industrial CyberSecurity for Nodes версии 2.6 и выше, защищенной паролем, необходимо передать установщику этот пароль.

При обновлении программы действующая лицензия автоматически применяется к Kaspersky Industrial CyberSecurity for Nodes 3.2, и использование новых компонентов и задач программы доступно в полном объеме. Срок действия лицензии остается без изменений.

При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности (например, недоступно обновление баз программы).

Миграция значений параметров обновляемой версии программы

Во время обновления программы остаются неизмененными:

- параметры программы и задач;
- журналы выполнения задач и системного аудита, а также записи в Журнале событий Windows;
- содержимое карантина и резервного хранилища;
- учетные записи, с правами которых запускаются задачи;
- права на управление программой;
- параметры уведомлений о работе задач программы.

Во время обновления программы сбрасываются или изменяются до значений по умолчанию для новой версии программы:

- все счетчики, в том числе статусы состояния антивирусных баз;
- данные об установленных обновлениях программных модулей и антивирусных баз;
- статусы выполнения задач;
- права на управление службой Kaspersky Security;
- параметры программы и задач, настроенные через реестр;
- параметры программы и задач, измененные в процессе установки критических исправлений.

Миграция списка заблокированных сетевых сессий

Во время обновления программы не переносится список заблокированных сетевых сессий клиентских компьютеров.

Параметры автоматической разблокировки доступа к заблокированным сетевым файловым ресурсам остаются неизмененными во время обновления программы.

Если вы обновляете Kaspersky Industrial CyberSecurity for Nodes версии 2.6 или 3.0, учитывайте, что в новой версии программы изменен механизм блокирования сетевых сессий клиентских компьютеров, со стороны которых была обнаружена вредоносная файловая активность или активность шифрования:

- отсутствует задача Блокирование доступа к сетевым файловым ресурсам;
- параметр, включающий блокирование сетевых сессий, доступен в задачах Постоянная защита файлов и Защита от шифрования;
- скомпрометированные сетевые сессии указаны в списке заблокированных сетевых сессий;
- параметры автоматической разблокировки доступа к скомпрометированным сетевым сессиям клиентского компьютера настраиваются в свойствах списка заблокированных сетевых сессий.

Миграция значений параметров и правил Контроля запуска программ

Во время обновления программы правила контроля запуска программ переносятся без изменений.

Во время обновления программы рекомендуем остановить задачу Контроль запуска программ, если она выполняется в активном режиме, или изменить режим работы задачи на *Только статистика*.

После завершения обновления программы рекомендуем проверить перенесенные правила контроля запуска программ и их работу в режиме *Только статистика*.

Миграция значений параметров и правил Управления сетевым экраном

Во время обновления программы правила задачи управления сетевым экраном переносятся без изменений.

Если компонент Управление сетевым экраном не был установлен в предыдущей версии программы, после обновления программы задача Управление сетевым экраном работает в режиме **Отслеживать статус работы брандмауэра Windows**.

Если компонент Управление сетевым экраном был установлен в предыдущей версии программы, после обновления программы задача Управление сетевым экраном работает в режиме **Контролировать работу брандмауэра Windows**.

Положение о Kaspersky Security Network

Задача Использование KSN может быть остановлена после обновления программы, если в Kaspersky Industrial CyberSecurity for Nodes 3.2 добавлены функции, отсутствующие в обновляемой версии программы и требующие предоставления дополнительной информации. Чтобы продолжить использование KSN после обновления программы, необходимо прочитать и принять условия Положения о KSN.

kaspersky

Об обновлении средств администрирования Kaspersky Industrial CyberSecurity for Nodes

Обновление Плагина управления и Консоли Kaspersky Industrial CyberSecurity for Nodes до версии 3.2 доступно для Плагина управления и Консоли программы версии 2.6 и выше.

При этом:

- Значения параметров Плагина управления и Консоли программы версии 2.6 и выше остаются неизменными.
- Плагин управления и Консоль программы версии 3.2 могут управлять Kaspersky Industrial CyberSecurity for Nodes версии 2.6 и выше.
- Плагин управления и Консоль программы версии 2.6 и выше могут управлять Kaspersky Industrial CyberSecurity for Nodes версии 3.2.

Обновление выполняется путем установки новой версии Плагина управления или Консоли программы поверх установленной версии и не требует перезагрузки компьютера.

Установка программы с помощью мастера

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

В этом разделе

Установка с помощью мастера установки

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

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

1. Установите Kaspersky Industrial CyberSecurity for Nodes на защищаемом компьютере.
2. На устройства, с которых вы планируете управлять Kaspersky Industrial CyberSecurity for Nodes, установите Консоль программы.
3. Если вы установили Консоль программы не на защищаемом компьютере, а на другом устройстве сети, выполните дополнительную настройку, чтобы пользователи Консоли программы могли удаленно управлять Kaspersky Industrial CyberSecurity for Nodes.
4. Выполните действия после установки Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

В этом разделе

Установка Kaspersky Industrial CyberSecurity for Nodes

Перед установкой Kaspersky Industrial CyberSecurity for Nodes выполните следующие действия:

1. Убедитесь, что на защищаемом компьютере не установлены другие антивирусные программы.
2. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом компьютере.

После выполнения описанных выше действий перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Industrial CyberSecurity for Nodes. Вы можете прервать установку Kaspersky Industrial CyberSecurity for Nodes на любом этапе работы мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Можно более детально ознакомиться с параметрами установки (удаления) (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 314).

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с помощью мастера установки, выполните следующие действия:*

1. На защищаемом компьютере запустите файл setupui.exe.
2. В открывшемся окне в разделе **Установка** перейдите по ссылке **установить Kaspersky Industrial CyberSecurity for Nodes**.
3. В открывшемся окне приветствия мастера установки Kaspersky Industrial CyberSecurity for Nodes нажмите на кнопку **Далее**.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

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

6. Нажмите на кнопку **Далее**.

   Откроется окно **Быстрая проверка устройства перед началом установки**.

7. В окне **Быстрая проверка устройства перед началом установки** установите флажок **Проверить устройство на вирусы**, чтобы проверить на наличие угроз системную память и загрузочные секторы локальных дисков защищаемого компьютера. Нажмите на кнопку **Далее**. По окончании проверки откроется окно с результатами проверки.

   В окне содержится информация о проверенных объектах на управляемом компьютере: общее количество проверенных объектов, количество обнаруженных угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или потенциально опасных процессов, которые программа Kaspersky Industrial CyberSecurity for Nodes удалила из памяти, и количество опасных или потенциально опасных процессов, которые программе не удалось удалить.

   Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

8. В окне **Далее** нажмите на кнопку **Быстрая проверка устройства перед началом установки**.

   Откроется окно **Выборочная установка**.

9. Выберите компоненты, которые вы хотите установить.

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

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

10. Чтобы отменить все изменения, в окне **Сбросить** нажмите на кнопку **Выборочная установка**. Нажмите на кнопку **Далее**.

11. В окне **Выбор папки назначения** выполните следующие действия:

    - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes.
    - Если требуется, нажмите на кнопку **Диск** для просмотра информации о доступном пространстве на локальных жестких дисках.

    Нажмите на кнопку **Далее**.

12. В окне **Дополнительные параметры установки** настройте параметры Постоянной защиты файлов:

    - **Включить Постоянную защиту файлов после установки программы**

      a. Выберите режим работы Постоянной защиты файлов.

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

- **Добавить к исключениям файлы, рекомендованные Microsoft**
- **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**.

  Нажмите на кнопку **Далее**.

13. В окне **Импорт параметров из конфигурационного файла** выполните следующие действия:
    a. Если вы хотите импортировать параметры Kaspersky Industrial CyberSecurity for Nodes из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.
    b. Нажмите на кнопку **Далее**.
14. В окне **Активация программы** выполните одно из следующих действий:
    - Если вы хотите активировать программу, укажите путь к файлу ключа Kaspersky Industrial CyberSecurity for Nodes.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
    - Если вы предварительно сохранили файл ключа в папке \exec комплекта поставки, имя этого файла отобразится в поле **Ключ**.

      Чтобы добавить ключ с помощью файла ключа из другой папки, укажите путь к этому файлу.

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

      Нажмите на кнопку **Далее**, чтобы добавить файл ключа в программу.
15. В окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Industrial CyberSecurity for Nodes.
16. По завершении установки откроется окно **Установка завершена**.
17. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. По завершении установки программа Kaspersky Industrial CyberSecurity for Nodes готова к работе, если вы добавили ключ активации.

Установка Консоли Kaspersky Industrial CyberSecurity for Nodes

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

► *Чтобы установить Консоль программы, выполните следующие действия:*

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.
2. На защищаемом компьютере запустите файл setupui.exe.

Откроется окно программы-приветствия.

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

   Откроется окно приветствия мастера установки.

4. Нажмите на кнопку **Далее**.
5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и, чтобы продолжить установку, установите флажок **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры установки**.

7. В окне **Дополнительные параметры установки** выполните следующие действия:
   - Если вы планируете с помощью Консоли программы управлять программой Kaspersky Industrial CyberSecurity for Nodes, установленной на удаленном устройстве, установите флажок **Разрешить удаленный доступ**.
   - Чтобы открыть окно **Выборочная установка** и выбрать компоненты:
     a. Нажмите на кнопку **Дополнительно**.

        Откроется окно **Выборочная установка**.

     b. В списке выберите набор компонентов «Средства администрирования».

        По умолчанию устанавливаются все компоненты.

     c. Нажмите на кнопку **Далее**.

   > Можно ознакомиться с более подробной информацией о компонентах Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Коды программных компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows" на стр. 308).

8. В окне **Выбор папки назначения** выполните следующие действия:
   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
   b. Нажмите на кнопку **Далее**.
9. В окне **Готовность к установке** нажмите на кнопку **Установить**.

   Мастер приступит к установке выбранных компонентов.

10. Нажмите на кнопку **Готово**.

    Работа мастера установки будет завершена. Консоль программы будет установлена на защищаемом компьютере.

Если вы установили набор Средства администрирования не на защищаемом компьютере, а на другом устройстве сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли программы на другое устройство" на стр. 300).

kaspersky

Дополнительная настройка после установки Консоли программы на другое устройство

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

- На защищаемом компьютере добавьте пользователей Kaspersky Industrial CyberSecurity for Nodes в группу KICS Administrators .
- Включите сетевые соединения для службы Kaspersky Security Management Service (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 983), если на защищаемом компьютере используется брандмауэр Windows или сетевой экран стороннего поставщика.
- Если во время установки Консоли программы на устройство под управлением Microsoft Windows не был установлен флажок **Разрешить удаленный доступ**, вручную включите сетевые соединения для Консоли программы через сетевой экран устройства.

Консоль программы на удаленном устройстве использует протокол DCOM для получения информации о событиях Kaspersky Industrial CyberSecurity for Nodes, например, о проверенных объектах или о завершении задач, от службы Kaspersky Security Management на защищаемом компьютере. Необходимо разрешить сетевые соединения для Консоли программы в параметрах брандмауэра Windows, чтобы устанавливать соединения между Консолью программы и службой Kaspersky Security Management.

На удаленном устройстве, на котором установлена Консоль программы, выполните следующие действия:

- Убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM).
- В параметрах брандмауэра Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes – kavfsrcn.exe.

  Устройство, на котором установлена Консоль программы, обменивается информацией с защищаемым компьютером через порт TCP 135.
- Чтобы разрешить подключение, настройте правило исходящего подключения для брандмауэра Windows.

  В отличие от стандартных служб TCP/IP и UDP/IP, где для каждого протокола имеется фиксированный порт, DCOM динамически назначает порты удаленным COM-объектам. Если между клиентским устройством (на котором установлена Консоль программы) и DCOM-устройством (защищаемым компьютером) находится сетевой экран, нужно открыть широкий диапазон портов.

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

► *Если Консоль программы открыта во время настройки соединения между защищаемым компьютером и устройством, на котором установлена Консоль программы, выполните следующие действия:*

1. Закройте Консоль программы.

2. Дождитесь завершения процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes – kavfsrcn.exe.
3. Перезапустите Консоль программы.

   Будут применены новые параметры соединения.

В этом разделе

Разрешение анонимного удаленного доступа к программам COM

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы разрешить анонимный удаленный доступ к программам COM, выполните следующие действия:*

1. На удаленном устройстве, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes, откройте консоль Службы компонентов.
2. Выберите **Пуск** → **Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **OK**.
5. В консоли **Службы компонентов** защищаемого компьютера разверните узел **Компьютеры**.
6. Откройте контекстное меню узла **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в блоке параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.
10. Нажмите на кнопку **OK**.

Разрешение сетевых соединений для процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы открыть TCP-порт 135 в брандмауэре Windows и разрешить сетевые соединения для процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. На удаленном устройстве закройте Консоль Kaspersky Industrial CyberSecurity for Nodes.
2. Выполните одно из следующих действий:
   - В Microsoft Windows XP с пакетом обновлений 2 и выше:
     a. Выберите **Пуск** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** (или Параметры брандмауэра Windows) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
     c. В поле **Имя** укажите имя порта RPC (TCP/135) или задайте другое имя, например, DCOM Kaspersky Industrial CyberSecurity for Nodes, а в поле **Номер порта** укажите номер порта: 135.
     d. Выберите протокол **TCP**.
     e. Нажмите на кнопку **OK**.
     f. На закладке **Исключения** нажмите на кнопку **Добавить**.
   - В Microsoft Windows 7 и выше:
     a. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
     c. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.
3. В окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Industrial CyberSecurity for Nodes с помощью Microsoft Management Console.
4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **OK** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

Добавление правила исходящего подключения для брандмауэра Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы добавить правило исходящего подключения для брандмауэра Windows, выполните следующие действия:*

1. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
2. В окне **Брандмауэр Windows** перейдите по ссылке **Дополнительные параметры**.

   Откроется окно **Брандмауэр Windows в режиме повышенной безопасности**.
3. Выберите вложенный узел **Правила для исходящего подключения**.
4. На панели **Действия** выберите пункт **Создать правило**.

5. В открывшемся окне **Мастер создания правила для нового исходящего подключения** выберите параметр **Порт** и нажмите на кнопку **Далее**.
6. Выберите протокол **TCP**.
7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.
8. В окне **Действие** выберите пункт **Разрешить подключение**.
9. Сохраните созданное правило и закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Брандмауэр Windows не разрешает установку сетевых соединений между Консолью программы и службой Kaspersky Security Management.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Industrial CyberSecurity for Nodes был установлен флажок **Включить Постоянную защиту файлов после установки программы** (по умолчанию), программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes выполняет задачу Проверка важных областей.

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

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

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

  Далее программа будет обновлять базы каждый час согласно расписанию, установленному в задаче по умолчанию.
- Выполнить Проверку важных областей, если перед установкой Kaspersky Industrial CyberSecurity for Nodes на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

Запуск и настройка задачи Обновление баз программы

► *Чтобы обновить базы программы после установки, выполните следующие действия:*

1. В свойствах задачи обновления баз программы настройте соединение с источником обновлений – HTTP- или FTP-серверами обновлений "Лаборатории Касперского".
2. Запустите задачу Обновление баз программы.

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

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

1. Откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
3. Выберите закладку **Параметры соединения**.
4. В разделе **Параметры прокси-сервера** установите флажок **Использовать указанный прокси-сервер**.
5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.
6. В разделе **Параметры аутентификации на прокси-сервере** выберите требуемый метод аутентификации из раскрывающегося списка:
   - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Industrial CyberSecurity for Nodes будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи. По умолчанию задача запускается под учетной записью **Локальная система** (**SYSTEM**).
   - **Использовать NTLM-аутентификацию с именем пользователя и паролем**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Industrial CyberSecurity for Nodes будет использовать указанную учетную запись для доступа к прокси-серверу. Введите имя и пароль пользователя или выберите пользователя в списке.
   - **Использовать имя пользователя и пароль**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.
7. В окне **Параметры программы** нажмите на кнопку **OK**.

► *Чтобы настроить соединение с серверами обновлений "Лаборатории Касперского" в задаче обновления баз программы, выполните следующие действия:*

1. Запустите Консоль программы одним из следующих способов:
   - Откройте Консоль программы на защищаемом компьютере. Для этого в меню **Пуск** выберите **Все программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Средства администрирования** > **Консоль Kaspersky Industrial CyberSecurity for Nodes 3.2**.

- Если Консоль программы запущена не на защищаемом устройстве, подключитесь к защищаемому устройству:

  a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.

  b. Выберите пункт **Подключиться к другому компьютеру**.

  c. В диалоговом окне **Выбор защищаемого устройства** выберите вариант **Другое устройство** и в поле ввода укажите сетевое имя защищаемого компьютера.

  > Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 983), укажите учетную запись, которая обладает этими правами.

  Откроется окно Консоли программы.

2. В дереве Консоли программы разверните узел **Обновление**.
3. Выберите вложенный узел **Обновление баз программы**.
4. В панели результатов перейдите по ссылке **Свойства**.
5. В открывшемся окне **Параметры задачи** выберите закладку **Параметры соединения**.
6. Выберите **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Параметры соединения с источником обновлений в задаче Обновление баз программы будут сохранены.

► *Чтобы запустить задачу Обновление баз программы, выполните следующие действия:*

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

Задача Обновление баз программы будет запущена.

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

Проверка важных областей

После того как вы обновили базы Kaspersky Industrial CyberSecurity for Nodes, проверьте защищаемый компьютер на наличие вредоносных программ с помощью задачи Проверка важных областей.

► *Чтобы запустить задачу Проверка важных областей, выполните следующие действия:*

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

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

► *Чтобы просмотреть журнал выполнения задачи,*

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

Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes

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

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

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

1. В меню **Пуск** выберите **Все программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Изменение или удаление Kaspersky Industrial CyberSecurity for Nodes**.

   Откроется окно мастера установки программы **Восстановление или удаление**.

2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

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

   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:
     - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;
     - пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если требуется установить группу компонентов.
   - Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

   Нажмите на кнопку **Далее**.

4. В окне **Готовность к установке** подтвердите изменение состава компонентов программы, нажав на кнопку **Установить**.

5. В окне, открывшемся по завершении установки, нажмите на кнопку **ОК**.

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

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

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

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Industrial CyberSecurity for Nodes**.
3. Выберите **Изменение или удаление Kaspersky Industrial CyberSecurity for Nodes**.

   Откроется окно мастера установки программы **Восстановление или удаление**.
4. Выберите вариант **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

   Откроется окно **Восстановление установленных компонентов**.
5. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если вы хотите сбросить параметры программы и восстановить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию. Нажмите на кнопку **Далее**.
6. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
7. В окне, открывшемся по завершении операции восстановления, нажмите на кнопку **OK**.

Программа Kaspersky Industrial CyberSecurity for Nodes будет восстановлена с указанными параметрами.

Установка программы из командной строки

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

kaspersky

В этом разделе

Об установке Kaspersky Industrial CyberSecurity for Nodes из командной строки

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes, а также добавить или удалить его компоненты, запустив файл инсталляционного пакета \exec\kics_x86.msi или \exec\kics_x64.msi из командной строки и указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом компьютере или на другом устройстве в сети, чтобы работать с Консолью программы локально или удаленно. Для этого используйте пакет установки \client\kicstools.msi

Выполняйте установку с правами учетной записи, входящей в группу администраторов на защищаемом компьютере, на котором установлена программа.

Если вы запустите на защищаемом компьютере один из файлов \exec\kics_x86.msi или \exec\kics_X64.msi без дополнительных ключей, Kaspersky Industrial CyberSecurity for Nodes будет установлен с параметрами установки по умолчанию.

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

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

Файлы \product\kics_x86.msi и \product\kics_x64.msi предназначены для установки Kaspersky Industrial CyberSecurity for Nodes.

Файлы \client\kicstools_x86.msi и \client\kicstools_x64.msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приведены коды компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Industrial CyberSecurity for Nodes из командной строки.

kaspersky

В этом разделе

Программные компоненты Kaspersky Industrial CyberSecurity for Nodes

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

Таблица 28. Описание программных компонентов Kaspersky Industrial CyberSecurity for Nodes

Компонент	Код	Функции компонента
Основная функциональность	Core	Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.
Контроль запуска программ	AppCtrl	Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает его в соответствии с заданными правилами контроля запуска программ. Компонент реализуется в задаче Контроль запуска программ.
Контроль устройств	DevCtrl	Этот компонент отслеживает попытки подключения внешних устройств к защищаемому компьютеру и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств. Компонент реализуется в задаче Контроль устройств.
Антивирусная защита	AVProtection	Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: Проверка по требованию Постоянная защита файлов
AMSI-защита	ScriptChecker	Этот компонент контролирует выполнение скриптов, созданных по технологиям Microsoft Windows (Active Scripting), таких как VBScript или JScript. Программа может также обрабатывать скрипты PowerShell и скрипты, работающие в программах Microsoft Office в операционных системах с установленным компонентом Antimalware Scan Interface (далее AMSI). Можно разрешить или запретить исполнение опасных или предположительно опасных скриптов.
Портативный сканер	Сканер	Этот компонент исследует изолированные устройства и проводит проверки состояния безопасности. Можно выполнять проверку нескольких устройств подряд. Портативный сканер формирует отдельный отчет для каждого проверяемого устройства. Сканер применяет установленный по умолчанию уровень безопасности – лечить. Если не удалось вылечить – удалять.

Компонент	Код	Функции компонента
Проверка по требованию	Ods	Этот компонент устанавливает системные файлы Kaspersky Industrial CyberSecurity for Nodes и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого компьютера, выполняемая по требованию).
Постоянная защита файлов	Oas	Этот компонент выполняет антивирусную проверку файлов на защищаемом компьютере при обращении к этим файлам. Компонент реализует задачу Постоянная защита файлов.
Защита от шифрования	AntiCryptor	Этот компонент вносит в список заблокированных узлов имена удаленных устройств, проявляющих вредоносную активность. При установке программы на устройства с операционной системой Windows XP SP2 компонент не устанавливается. Компонент реализует задачу Защита от шифрования.
Использование Kaspersky Security Network	Ksn	Этот компонент реализует защиту на основе облачных технологий "Лаборатории Касперского". Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).
Мониторинг файловых операций	Fim	Этот компонент позволяет регистрировать операции, производимые над файлами в выбранной области мониторинга. Компонент реализует задачу Мониторинг файловых операций.
Мониторинг доступа к реестру	RegMonitor	Компонент позволяет отслеживать действия, выполняемые с указанными ветвями и ключами реестра в областях мониторинга, заданных в параметрах задачи. Компонент осуществляет Мониторинг доступа к реестру.
Защита от эксплойтов	AntiExploit	Этот компонент обеспечивает управление параметрами защиты процессов в памяти устройства.
Контроль Wi-Fi	WiFiControl	Этот компонент контролирует попытки подключения защищаемого компьютера к сетям Wi-Fi.

Компонент	Код	Функции компонента
Управление сетевым экраном	Firewall	Этот компонент предоставляет возможность управления брандмауэром Windows через графический интерфейс Kaspersky Industrial CyberSecurity for Nodes. Компонент реализует задачу Управление сетевым экраном.
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Этот компонент обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes с Агентом администрирования Kaspersky Security Center. Вы можете установить этот компонент на защищаемом компьютере, если вы планируете управлять программой через Kaspersky Security Center.
Анализ журналов	Log Inspection	Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.
Получение данных о проектах ПЛК	Plc	Этот компонент позволяет получать данные об актуальных проектах ПЛК, используемых в промышленной сети.
Проверка целостности проектов ПЛК	Plc	Этот компонент позволяет проверять целостность проектов ПЛК, используемых в промышленной системе.
Набор счетчиков производительности программы Системный монитор	PerfMonCounters	Компонент устанавливает набор счетчиков производительности программы Системный монитор. Счетчики производительности позволяют измерять производительность Kaspersky Industrial CyberSecurity for Nodes и находить возможные узкие места на защищаемом устройстве при совместной работе Kaspersky Industrial CyberSecurity for Nodes с другими программами.
Поддержка SNMP-протокола	SnmpSupport	Компонент публикует счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Этот компонент можно установить на защищаемый компьютер, только если на нем уже установлена служба SNMP.

Компонент	Код	Функции компонента
Значок Kaspersky Industrial CyberSecurity for Nodes в области уведомлений	TrayApp	Компонент отображает значок Kaspersky Industrial CyberSecurity for Nodes в области уведомлений панели задач защищаемого компьютера. Значок Kaspersky Industrial CyberSecurity for Nodes показывает состояние защиты устройства, позволяет открыть Консоль Kaspersky Industrial CyberSecurity for Nodes (если она установлена) и окно О программе.

Программные компоненты набора Средства администрирования

В следующей таблице приведены коды и описание программных компонентов набора Средства администрирования.

Таблица 29. Описание программных компонентов набора Средства администрирования

Компонент	Код	Функции компонента
Оснастка Kaspersky Industrial CyberSecurity for Nodes	MmcSnapin	Компонент устанавливает оснастку Консоли управления Microsoft (MMC) для управления программой с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes. Если при установке набора "Средства администрирования" из командной строки, вы укажете другие компоненты набора, но не укажите компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически.
Руководство администратора	Help	Kaspersky Industrial CyberSecurity for Nodes добавляет ярлык для перехода на веб-сайт "Лаборатории Касперского", где документ "Руководство администратора" доступен в формате онлайн справки. Этот ярлык доступен из меню **Пуск**.

kaspersky

Параметры установки и удаления и ключи командной строки для службы установщика Windows

В этом разделе описаны параметры установки и удаления Kaspersky Industrial CyberSecurity for Nodes, их значения по умолчанию, указаны ключи для изменения параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Industrial CyberSecurity for Nodes из командной строки.

Параметры установки и ключи командной строки для установщика Windows

- Согласие с условиями Лицензионного соглашения: необходимо принять условия для установки Kaspersky Industrial CyberSecurity for Nodes.

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

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

- Согласие с условиями Политики конфиденциальности: необходимо принять условия для установки Kaspersky Industrial CyberSecurity for Nodes.

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

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

- Разрешить установку Kaspersky Industrial CyberSecurity for Nodes, если не установлено обновление KB4528760. Дополнительная информация об обновлении KB4528760 приведена на веб-сайте Microsoft https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760.

  Возможны следующие значения ключа командной строки `SKIPCVEWINDOWS10=<значение>`:

  - `0` – отменить установку Kaspersky Industrial CyberSecurity for Nodes, если не установлено обновление KB4528760 (значение по умолчанию).
  - `1` – разрешить установку Kaspersky Industrial CyberSecurity for Nodes, если не установлено обновление KB4528760.

  > Обновление KB4528760 исправляет уязвимость безопасности CVE-2020-0601. Дополнительная информация об уязвимости в системе безопасности CVE-2020-0601 приведена на веб-сайте Microsoft https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760.

- Установка Kaspersky Industrial CyberSecurity for Nodes с восстановленными параметрами предыдущей версии при обновлении.

  Возможны следующие значения ключа командной строки `RESTOREDEFSETTINGS=<значение>`:

  - `0` – все данные из предыдущей версии переносятся в новую версию при обновлении (значение по умолчанию).
  - `1` – только файл с данными активации и закрытыми ключами переносится в новую версию при обновлении ([диск]:\ProgramData\Kaspersky Lab\<продукт>\<версия>\Data\product.dat). Все остальные данные из предыдущей версии, такие как настройки, антивирусные базы, отчеты, объекты карантина и резервного хранилища, удаляются.

- Установка Kaspersky Industrial CyberSecurity for Nodes с сохранением отчетов из предыдущих версий при обновлении.

  Возможны следующие значения ключа командной строки KEEP_REPORTS=<значение>:

  - 0 – все данные из предыдущей версии, кроме отчетов ([диск]:\ProgramData\Kaspersky Lab\<продукт>\<версия>\Reports), переносятся в новую версию при обновлении. Отчеты удаляются.
  - 1 – все данные из предыдущей версии, такие как настройки, антивирусные базы, отчеты, объекты карантина и резервного хранилища, переносятся в новую версию при обновлении (значение по умолчанию).
- Установка Kaspersky Industrial CyberSecurity for Nodes с предварительной проверкой активных процессов и загрузочных секторов локальных дисков.

  Возможны следующие значения ключа командной строки PRESCAN=<значение>:

  - 0 – не выполнять предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки (значение по умолчанию).
  - 1 – выполнить предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки.
- Папка, в которую будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes при установке. Вы можете указать другую папку.

  Значение по умолчанию для ключа командной строки INSTALLDIR=<полный путь к папке>:

  - Kaspersky Industrial CyberSecurity for Nodes: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes
  - Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%
- Запуск задачи Постоянная защита файлов сразу после запуска Kaspersky Industrial CyberSecurity for Nodes.

  Возможны следующие значения ключа командной строки RUNRTP=<значение>:

  - 1 – запустить (значение по умолчанию).
  - 0 – не запускать.
- Режим работы задачи Постоянная защита файлов.

  Возможны следующие значения ключа командной строки RTP_BLOCKING=<значение>:

  - 1 – Рекомендуемый (значение по умолчанию).
  - 0 – Только сообщать.

- Объекты, исключаемые из области защиты в соответствии с рекомендациями корпорации Microsoft. В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать корпорация Microsoft. Некоторые программы на защищаемом компьютере могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, используемые этими программами. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.

  Возможны следующие значения ключа командной строки `ADDMSEXCLUSION=<значение>`:

  - `1` – исключить (значение по умолчанию).
  - `0` – не исключать.

- Объекты, исключаемые из области защиты в соответствии с рекомендациями "Лаборатории Касперского". В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать "Лаборатория Касперского".

  Возможны следующие значения ключа командной строки `ADDKLEXCLUSION=<значение>`:

  - `1` – исключить (значение по умолчанию).
  - `0` – не исключать.

- Разрешить удаленное подключение к Консоли программы По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом компьютере, не разрешено. Во время установки можно разрешить подключение. Kaspersky Industrial CyberSecurity for Nodes создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.

  Возможны следующие значения ключа командной строки `ALLOWREMOTECON=<значение>`:

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Путь к файлу ключа (`LICENSEKEYPATH`). По умолчанию установщик Windows пытается найти файл с расширением .key в папке \exec комплекта поставки. Если в папке \exec имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Можно предварительно сохранить файл ключа в папке \exec или указать другой путь к файлу ключа с помощью параметра **Добавить ключ**. Вы можете добавить ключ после установки Kaspersky Industrial CyberSecurity for Nodes с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ во время установки программы, после установки Kaspersky Industrial CyberSecurity for Nodes не будет функционировать.

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

  Значение по умолчанию для параметра `CONFIGPATH=<имя конфигурационного файла>` не указано.

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

  - **Действия над зараженными и другими обнаруженными объектами: Только уведомлять**
  - **Действия над возможно зараженными объектами: Только уведомлять**

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

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

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

- Параметр включения сетевых соединений для Консоли программы используется для установки Консоли Kaspersky Industrial CyberSecurity for Nodes на другое устройство. Вы можете удаленно управлять защитой устройства с другого устройства, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes. В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла kavfsrcn.exe для удаленного управления Kaspersky Industrial CyberSecurity for Nodes и предоставлен доступ к DCOM-программам. После завершения установки добавьте пользователей в KICS Administrators группу KAVWSEE Administrators, чтобы разрешить им управлять программой удаленно, а также разрешите на защищаемом устройстве сетевые подключения к службе Kaspersky Security Management (файл kavfsgt.exe). Можно более детально ознакомиться с дополнительной настройкой при установке Kaspersky Industrial CyberSecurity for Nodes на другое устройство (см. раздел "Дополнительная настройка после установки Консоли программы на другое устройство" на стр. 300).

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

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Отключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на защищаемый компьютер в фоновом режиме. Независимо от значения данного параметра, при установке Kaspersky Industrial CyberSecurity for Nodes программа всегда предупреждает о других версиях программы, установленных на этом же защищаемом компьютере.

Возможны следующие значения ключа командной строки SKIPINCOMPATIBLESW=<значение>:

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

Параметры удаления и ключи командной строки для установщика Windows

- Восстановление содержимого карантина.

  Возможны следующие значения ключа командной строки RESTOREQTN=<значение>:

  - 0 – удалить содержимое карантина (значение по умолчанию).
  - 1 – восстановить содержимое карантина в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную подпапку \Quarantine.
- Восстановление содержимого резервного хранилища.

  Возможны следующие значения ключа командной строки RESTOREBCK=<значение>:

  - 0 – удалить содержимое резервного хранилища (значение по умолчанию).
  - 1 – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную папку \Backup.
- Ввод текущего пароля для подтверждения операции удаления (при включенной функции защиты паролем).

  Значение по умолчанию для ключа UNLOCK_PASSWORD=<указанный пароль> не задано.
- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

  Значение по умолчанию для ключа командной строки RESTOREPATH=<полный путь к папке> – %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Restored

Примеры команд установки Kaspersky Industrial CyberSecurity for Nodes

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

На защищаемом компьютере под управлением 32-разрядной версии Microsoft Windows запускайте файлы с суффиксом x86 из комплекта поставки. На защищаемом компьютере под управлением 64-разрядной версии Microsoft Windows запускайте файлы с суффиксом x64 из комплекта поставки.

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

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

```
\exec\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes можно установить со следующими параметрами:

- Установить только компоненты Постоянная защита файлов и Проверка по требованию.
- Не запускать Постоянную защиту файлов при запуске Kaspersky Industrial CyberSecurity for Nodes.
- Не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

► *Чтобы установить компоненты, например Контроль устройств, выполните следующую команду:*

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

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

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

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

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

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

Список команд для установки: запуск msi-файла

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию и показать интерфейс установки, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с рекомендованными параметрами установки и включить ротацию файлов трассировки при достижении ими заданного максимального количества, выполните следующую команду:*

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

Параметр `TRACE_FOLDER` является обязательным.

Для параметра `TRACE_MAX_ROLL_COUNT` действуют следующие правила:

- Если параметр указан, включается ротация файлов трассировки при достижении ими максимального количества, указанного в параметре. Доступный диапазон значений параметра: от 1 до 999.
- Если в качестве максимального количества файлов трассировки указано значение 0, ротация файлов трассировки будет отключена.
- Если параметр указан, но его значение недопустимо или превышает диапазон допустимых значений от 1 до 999 файлов, ротация файлов трассировки включается с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.
- Если параметр не указан:
  - Если на устройстве уже настроена ротация файлов трассировки, ее параметры не изменяются. Программа будет игнорировать вводимые параметры.
  - Если ротация файлов трассировки на устройстве не настроена, параметр ротации будет включен с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и активировать его с помощью файла ключа C:\0000000A.key, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с предварительной проверкой активных процессов и загрузочных секторов локальных дисков, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes в папку установки C:\KICS, выполните следующую команду:*

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

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

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

► *Чтобы установить Консоль Kaspersky Industrial CyberSecurity for Nodes, выполните следующую команду:*

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

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

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

► *Чтобы установить исправление, если программа Kaspersky Industrial CyberSecurity for Nodes защищена паролем, выполните следующую команду:*

```
msiexec /p "<msp путь к имени файла>" UNLOCK_PASSWORD=<пароль>
```

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Industrial CyberSecurity for Nodes был установлен флажок **Включить Постоянную защиту файлов после установки программы**, программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes выполняет задачу Проверка важных областей.

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

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

  Например, вы можете запустить задачу Обновление баз программы, выполнив следующую команду:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
  /PROXYUSER:inetuser /PROXYPWD:123456
  ```

  При этом обновления баз Kaspersky Industrial CyberSecurity for Nodes будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080) с использованием для доступа к серверу встроенной в Windows проверки подлинности NTLM с учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить Проверку важных областей, если перед установкой Kaspersky Industrial CyberSecurity for Nodes на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.

► *Чтобы выполнить задачу Проверка важных областей с помощью командной строки, выполните следующую команду:*

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

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

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

kaspersky

Добавление и удаление компонентов. Примеры команд

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

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

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

или

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

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

► *Чтобы удалить установленные компоненты, выполните следующую команду:*

```
msiexec /i kics.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,Bases,Core,CoreBLF
iles,CoreFolders,CoreWPFiles,DevCtrl,Drivers,Drivers.klelam,Fim,Ksn,LogIns
pector,Oas,Ods,PMenus,PatchExe,RamDisk,Shell,SnmpSupport,TrayApp
ADD_ADV=IDS,RegMonitor REMOVE=Firewall,PerfMonCounters EULA=1
PRIVACYPOLICY=1 /qn
```

Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

Таблица 30. Коды возврата

Код	Описание
1324	Имя папки назначения содержит недопустимые символы.
25001	Недостаточно прав для установки Kaspersky Industrial CyberSecurity for Nodes. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Не удается установить Kaspersky Industrial CyberSecurity for Nodes на устройство под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows.
25004	Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующее программное обеспечение: <список несовместимого программного обеспечения>.
25010	Указанный путь не может быть использован для сохранения объектов на карантине.
25011	Имя папки для сохранения объектов на карантине содержит недопустимые символы.
26251	Не удалось загрузить DLL для Счетчиков производительности.
26252	Не удалось загрузить DLL для Счетчиков производительности.
27300	Драйвер не может быть установлен.
27301	Драйвер не может быть удален.
27302	Невозможно установить сетевой компонент. Достигнуто максимальное пороговое значение поддерживаемого количества устройств фильтрации.
27303	Антивирусные базы не найдены.

Установка программы с помощью Kaspersky Security Center

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

В этом разделе

kaspersky

Общие сведения об установке через Kaspersky Security Center

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

После выполнения задачи удаленной установки программа Kaspersky Industrial CyberSecurity for Nodes будет установлена с одинаковыми параметрами на несколько защищаемых компьютеров.

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

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

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

Права для установки Kaspersky Industrial CyberSecurity for Nodes

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

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

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

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

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

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

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

kaspersky

Установка Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center

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

Если вы планируете в дальнейшем управлять Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На защищаемом компьютере с установленным Сервером администрирования Kaspersky Security Center также установлен Плагин управления (файл \plugin\klcfginst.exe комплекта поставки Kaspersky Industrial CyberSecurity for Nodes).
- На защищаемых компьютерах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых компьютерах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Industrial CyberSecurity for Nodes с помощью задачи удаленной установки.

Можно также объединить устройства в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с помощью задачи удаленной установки, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Дополнительно**.
3. Разверните вложенный узел **Удаленная установка**.
4. В панели результатов вложенного узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.
5. Выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. Введите имя инсталляционного пакета.
7. Выберите файл kics.kud из комплекта поставки Kaspersky Industrial CyberSecurity for Nodes в качестве файла инсталляционного пакета.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
8. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

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

9. Чтобы изменить набор устанавливаемых компонентов (см. раздел "Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes" на стр. 306) Kaspersky Industrial CyberSecurity for Nodes и настроить параметры по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 314) в инсталляционном пакете, выполните следующие действия:

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

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

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

   d. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Industrial CyberSecurity for Nodes, которые вы хотите установить.

   e. При необходимости измените режим работы Постоянной защиты файлов:

      iv. Нажмите на кнопку справа от флажка **Постоянная защита файлов**.

      v. В окне **Выбор уровня безопасности** в раскрывающемся списке **Уровень безопасности** выберите нужный вариант.

   f. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.

      Путь к папке назначения может содержать системные переменные окружения. Если указанной папки не существует на защищаемом компьютере, она будет создана.

   g. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:

      - **Выполнить антивирусную проверку защищаемого устройства перед началом установки.**
      - **Включить постоянную защиту после установки программы**.
      - **Добавить к исключениям файлы, рекомендованные Microsoft**.
      - **Добавить к исключениям файлы, рекомендованные Лабораторией Касперского**.
      - **Использовать режим пониженного потребления ресурсов Агентом KSC.**
      - **Выполнять рекомендуемое действие во время проверки при запуске ОС**.

   h. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.

10. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes на защищаемые компьютеры (группу администрирования). Настройте параметры задачи.

    Подробная информация о создании и настройке задачи удаленной установки приведена в *Справке Kaspersky Security Center*.

11. Запустите задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes.

Программа Kaspersky Industrial CyberSecurity for Nodes будет установлена на указанные в задаче защищаемые компьютеры.

kaspersky

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

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

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

1. Создать задачу Обновление баз программы для группы защищаемых компьютеров, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
2. Создать групповую задачу проверки по требованию со статусом Проверка важных областей. Kaspersky Security Center оценивает состояние безопасности каждого защищаемого устройства группы по результатам выполнения этой задачи, а не по результатам задачи Проверка важных областей.
3. Создать новую политику для группы защищаемых компьютеров. В свойствах политики в разделе **Параметры программы** выключить запуск по расписанию локальных системных задач проверки по требованию и задачи Обновление баз программы на защищаемых компьютерах группы администрирования в подразделе **Запуск локальных системных задач**.

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

Установка Консоли программы через Kaspersky Security Center

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

► *Чтобы установить Консоль программы с помощью задачи удаленной установки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.
2. Разверните вложенный узел **Удаленная установка**.
3. В панели результатов вложенного узла Инсталляционные пакеты нажмите на кнопку **Создать инсталляционный пакет**. При создании нового инсталляционного пакета:
   a. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет для указанного исполняемого файла** в качестве типа пакета.
   b. Введите имя инсталляционного пакета.
   c. В папке комплекта поставки Kaspersky Industrial CyberSecurity for Nodes выберите файл \client\setup.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.

d. Чтобы установить Консоль программы, в поле **Параметры запуска исполняемого файла (необязательно)** укажите ключ командной строки ADDLOCAL. Консоль программы устанавливается в папку установки по умолчанию. Укажите параметр "EULA=1". В противном случае установка компонентов невозможна.

```
/s /p "ADDLOCAL=MmcSnapin EULA=1"
```

При необходимости в поле **Параметры запуска исполняемого файла (необязательно)** можно указать параметр командной строки ADDLOCAL, чтобы изменить набор устанавливаемых компонентов, и параметр командной строки INSTALLDIR, чтобы указать папку назначения, отличную от заданной по умолчанию. Например, чтобы выполнить автономную установку Консоли программы в папку C:\KasperskyConsole, используйте следующие ключи командной строки:

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

4. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли программы на выбранные защищаемые компьютеры (группу администрирования). Настройте параметры задачи.

> Подробная информация о создании и настройке задач удаленной установки приведена в Справке Kaspersky Security Center.

5. Запустите задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче защищаемые устройства.

Установка программы через групповые политики Active Directory

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

В этом разделе

Установка Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory

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

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

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

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes, используйте пакет установки kics_x86.msi или kics_x64.msi. Чтобы установить Консоль программы, используйте пакет установки kicstools.msi

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes (Консоль программы), выполните следующие действия:*

1. Сохраните msi-файл, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папку общего доступа на контроллере домена.
2. Сохраните файл ключа (см. раздел "О файле ключа" на стр. 474) в эту же общую папку на контроллере домена.
3. В этой же папке общего доступа на контроллере домена создайте файл install_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

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

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

Программа Kaspersky Industrial CyberSecurity for Nodes будет установлена на защищаемые устройства группы после их перезагрузки.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

После установки Kaspersky Industrial CyberSecurity for Nodes на защищаемых компьютерах рекомендуется сразу обновить базы программы и выполнить проверку важных областей компьютера. Эти действия (см. раздел "Действия после установки Kaspersky Industrial CyberSecurity for Nodes" на стр. 303) можно выполнить из Консоли программы.

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

kaspersky

Журналы установки Kaspersky Industrial CyberSecurity for Nodes

Если вы выполняете установку Kaspersky Industrial CyberSecurity for Nodes с помощью мастера установки, служба установщика Windows создает журнал установки. Файл журнала с именем kics_v3.2_install_<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала) сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление** для Консоли программы или для Kaspersky Industrial CyberSecurity for Nodes, в папке %temp% будет автоматически создан файл журнала с именем kics_3.2_maintenance.log.

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

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и создать файл журнала на диске C:\, выполните одну из следующих команд:*

- `msiexec /i kics_x86.msi /l*v C:\kics.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i kics_x64.msi /l*v C:\kics.log /qn EULA=1 PRIVACYPOLICY=1`

Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes

При совместной установке Kaspersky Industrial CyberSecurity for Nodes и набора "Средства администрирования", включающего Консоль программы, служба установщика Windows выполняет на защищаемом компьютере следующие изменения:

- создает папки Kaspersky Industrial CyberSecurity for Nodes на защищаемом компьютере и на защищаемом компьютере, на котором установлена Консоль программы;
- регистрирует службы Kaspersky Industrial CyberSecurity for Nodes;
- создает группу пользователей Kaspersky Industrial CyberSecurity for Nodes;
- регистрирует в системном реестре ключи Kaspersky Industrial CyberSecurity for Nodes.

Эти изменения описаны ниже.

kaspersky

Папки Kaspersky Industrial CyberSecurity for Nodes на защищаемом компьютере

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

- Заданная по умолчанию папка установки Kaspersky Industrial CyberSecurity for Nodes, содержащая исполняемые файлы Kaspersky Industrial CyberSecurity for Nodes в зависимости от разрядности операционной системы. По умолчанию используются следующие папки установки:
  - В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes
- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Industrial CyberSecurity for Nodes по протоколу SNMP.
  - %Kaspersky Industrial CyberSecurity for Nodes%\mibs
- 64-разрядные версии исполняемых файлов Kaspersky Industrial CyberSecurity for Nodes (папка создается только при установке Kaspersky Industrial CyberSecurity for Nodes в 64-разрядной версии Microsoft Windows).
  - %Kaspersky Industrial CyberSecurity for Nodes%\x64
- Служебные файлы Kaspersky Industrial CyberSecurity for Nodes:
  - %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Dskm

  Для Windows XP путь к папке Kaspersky Lab – %ALLUSERSPROFILE%\Application Data
- Файлы с параметрами источников обновлений:

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Update
- Обновления баз и программных модулей, загруженные с помощью задачи Копирование обновлений (папка создается при первой загрузке обновлений с помощью задачи Копирование обновлений).

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Update\Distribution
- Журналы выполнения задач и журнал системного аудита.

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Reports
- Набор используемых баз данных.

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Bases\Current
- Резервные копии баз; перезаписываются при каждом обновлении баз.

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Bases\Backup
- Временные файлы, создаваемые при выполнении задач обновления.

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Bases\Temp

- Объекты на карантине (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Quarantine

- Объекты в резервном хранилище (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Backup

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

  %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Restored

Папка, создаваемая при установке Консоли программы

Заданная по умолчанию папка установки Консоли программы, содержащая файлы набора "Средства администрирования", зависит от разрядности операционной системы. По умолчанию используются следующие папки установки:

- В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools
- В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools

Службы Kaspersky Industrial CyberSecurity for Nodes

Следующие службы Kaspersky Industrial CyberSecurity for Nodes запускаются под системной учетной записью Локальная система (SYSTEM).

- Kaspersky Security Service (KAVFS) – это основная служба Kaspersky Industrial CyberSecurity for Nodes, которая управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes.
- Служба Kaspersky Security Management (KAVFSGT) – это служба, предназначенная для управления Kaspersky Industrial CyberSecurity for Nodes через Консоль программы.
- Служба Kaspersky Security Exploit Prevention (KAVFSSLP)– это служба, исполняющая роль посредника при передаче параметров безопасности внешним агентам безопасности и при получении данных о событиях безопасности.

Группа Kaspersky Industrial CyberSecurity for Nodes

KICS Administrators – это группа на защищаемом компьютере, пользователи которой имеют полный доступ к службе Kaspersky Security Management и ко всем функциям Kaspersky Industrial CyberSecurity for Nodes.

Ключи системного реестра

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

- Свойства Kaspersky Industrial CyberSecurity for Nodes: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Параметры журнала событий Kaspersky Industrial CyberSecurity for Nodes (Kaspersky Event Log): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Свойства службы управления Kaspersky Industrial CyberSecurity for Nodes: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]

- Параметры счетчиков производительности:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Параметры компонента Поддержка SNMP-протокола:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\3.2\SnmpAgent]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\3.2\SnmpAgent]
- Параметры файла дампа:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\3.2\CrashDump]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\3.2\CrashDump]
- Параметры файла трассировки:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\3.2\Trace]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\3.2\Trace]
- Параметры задач и фукнций программы:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\3.2\Environment]

Процессы Kaspersky Industrial CyberSecurity for Nodes

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

Таблица 31. Процессы Kaspersky Industrial CyberSecurity for Nodes

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Industrial CyberSecurity for Nodes
kavtray.exe	Процесс значка области уведомлений
kavfsmui.exe	Процесс компонента Диагностическое окно
kavshell.exe	Процесс утилиты командной строки
kavfsrcn.exe	Процесс удаленного управления Kaspersky Industrial CyberSecurity for Nodes
kavfs.exe	Процесс службы Kaspersky Security
kavfsgt.exe	Процесс службы Kaspersky Security Management
kavfswh.exe	Процесс службы Kaspersky Security Exploit Prevention

kaspersky

Установка Kaspersky Security Gateway

В этом разделе приведены инструкции по установке Kaspersky Security Gateway.

В этом разделе

Обновление Kaspersky Security Gateway

Обновление до Kaspersky Security Gateway 3.2 доступно для версии 2.6 и выше. Обновление выполняется путем установки новой версии программы поверх установленной версии программы и не требует перезагрузки компьютера.

В процессе обновления Kaspersky Security Gateway до версии 3.2 установленная раннее версия программы автоматически удаляется.

Значения параметров обновляемой версии Kaspersky Security Gateway передаются без изменения в Kaspersky Security Gateway 3.2.

Установка Kaspersky Security Gateway с помощью мастера установки

► *Чтобы установить Kaspersky Security Gateway,*

запустите файл security_gateway.msi, входящий в комплект поставки.

Соответствующий мастер проведет вас по всем шагам установки. Мастер установки предложит настроить параметры установки. Следуйте инструкциям мастера.

Интерфейс мастера установки Kaspersky Security Gateway состоит из последовательных окон (шагов). Для перемещения между окнами мастера установки, используйте кнопки **Назад** и **Далее**. Чтобы закрыть мастер установки после завершения, нажмите на кнопку **Готово**. Чтобы выйти из мастера установки на любом этапе процесса установки, нажмите на кнопку **Отмена**.

kaspersky

В этом разделе

Шаг 1. Проверка требований к установке

Если среди обнаруженных программ есть предыдущая версия Kaspersky Security Gateway, **Установка программы** автоматически удаляет ее и устанавливает новую версию Kaspersky Security Gateway.

Если установлен Kaspersky Security Gateway 2.0 или более ранняя версия, мастер установки не сможет удалить ее и отменит установку. Перед установкой Kaspersky Security Gateway 3.2 вручную удалите Kaspersky Security Gateway 2.0 или более ранней версии.

Перед установкой или обновлением Kaspersky Security Gateway мастер установки проверяет выполнение следующих требований:

- Компьютер и установленные программы соответствуют аппаратным и программным требованиям.
- Учетная запись пользователя обладает необходимыми для установки приложений правами.

Если не выполнено какое-либо из предыдущих требований, на экране отображается соответствующее уведомление и процесс установки прерывается.

Шаг 2. Страница приветствия в начале установки

Если компьютер, на котором выполняется установка Kaspersky Security Gateway, полностью соответствует аппаратным и программным требованиям, откроется страница приветствия в начале установки. На странице приветствия сообщается о начале установки Kaspersky Security Gateway на компьютере.

Перейдите к следующему шагу мастера.

Шаг 3. Ознакомление с текстом Лицензионного соглашения и Политики конфиденциальности

На этом этапе рекомендуется ознакомиться с Политикой конфиденциальности и Лицензионным соглашением с "Лабораторией Касперского".

Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

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

Перейдите к следующему шагу мастера.

Шаг 4. Выбор папки назначения

На этом шаге вам необходимо указать путь к папке назначения, в которую будет установлен Kaspersky Security Gateway. Чтобы выбрать папку назначения, нажмите на кнопку **Обзор**.

Чтобы просмотреть информацию о доступном пространстве на локальных жестких дисках, нажмите на кнопку **Диск**. Информация отображается в открывшемся окне **Доступное дисковое пространство**.

Перейдите к следующему шагу мастера.

Шаг 5. Выбор компонентов

На этом шаге вы можете выбрать устанавливаемые компоненты Kaspersky Security Gateway. По умолчанию выбрана установка всех компонентов.

Чтобы выбрать устанавливаемый компонент, нажмите на значок рядом с названием компонента, чтобы открыть его контекстное меню. Затем выберите **Компонент будет установлен на локальный жесткий диск**. Более подробная информация о задачах, выполняемых выбранным компонентом, и свободном месте на диске, требуемом для установки компонента, приведена в нижней части страницы мастера установки.

Чтобы просмотреть подробную информацию о доступном пространстве на локальных жестких дисках, нажмите на кнопку **Диск**. Информация отображается в открывшемся окне **Доступное дисковое пространство**.

Чтобы отменить установку компонента, в контекстном меню выберите пункт **Компонент будет недоступен**.

Чтобы вернуться к списку компонентов, установленных по умолчанию, нажмите на кнопку **Сброс**.

Перейдите к следующему шагу мастера.

kaspersky

Шаг 6. Настройка подключения к системе SCADA

На этом шаге вам нужно указать адрес и TCP-порт компьютера, на котором будет установлен Kaspersky Security Gateway, для подключения к системе SCADA. Введите адрес (число от 0 до 65535) и TCP-порт (число от 0 до 65535) в соответствии с протоколом IEC 60870-5-104.

Чтобы запустить установку, нажмите на кнопку **Установить**.

Во время установки Kaspersky Security Gateway на компьютер могут быть разорваны текущие сетевые соединения. Большинство разорванных соединений восстанавливаются через непродолжительное время.

Шаг 7. Установка Kaspersky Security Gateway

Мастер установки копирует файлы Kaspersky Security Gateway на компьютер. Дождитесь завершения установки.

Завершите работу мастера.

Установка Kaspersky Security Gateway из командной строки

► *Чтобы установить Kaspersky Security Gateway из командной строки, выполните следующую команду:*

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

где `EULA=1 PRIVACYPOLICY=1` соответствует тому, что вы принимаете условия Лицензионного соглашения для Kaspersky Security Gateway между вами и "Лабораторией Касперского" и Политики конфиденциальности, описывающей обработку и передачу данных.

Устанавливая значение 1 для параметров, вы подтверждаете следующее:

- Вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.
- Вы полностью прочитали и понимаете Политику конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.

Для установки Kaspersky Security Gateway необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.

Текст Лицензионного соглашения и Политики конфиденциальности включен в комплект поставки.

kaspersky

Процедура приемки

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

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел «Приложение. Значения параметров программы в сертифицированной конфигурации» на стр. 1059).

Вы можете производить настройку параметров для всех защищаемых компьютеров с помощью политики в Kaspersky Security Center или для одного компьютера с помощью локальной Консоли администратора, установленной на этом компьютере.

Настройка прав доступа

По умолчанию доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes, управлению службами Kaspersky Security (KAVFS) и Kaspersky Security Management (KAVFSGT) имеют пользователи, входящие в группу Администраторы на защищаемом компьютере, пользователи группы KICS Administrators, созданной на защищаемом копмьютере при установке Kaspersky Industrial CyberSecurity for Nodes, а также системная группа SYSTEM.

Пользователи-администраторы, осуществляющие контроль за безопасностью, должны быть добавлены в группу KICS Administrators.

► *Чтобы добавить пользователя в группу KICS Administrators:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Изменить права пользователей на управление программой**.
3. В открывшемся окне **Разрешения для группы Kaspersky Industrial CyberSecurity for Nodes** в списке **Группы или пользователи** выберите группу KICS Administrators.
4. Нажмите на кнопку **Добавить**.
5. В открывшемся окне введите название учетной записи, которую необходимо добавить.

6. В блоке **Разрешения для группы KICS Administrators** убедитесь, что установлены флажки **Разрешить** для следующих пунктов:
   - **Полный контроль**: полный набор прав на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Security.
   - **Чтение**:
     - следующие права на управление Kaspersky Industrial CyberSecurity for Nodes: Чтение статистики, Чтение параметров, Чтение журналов и Чтение прав;
     - следующие права 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 кроме Изменение прав;
     - следующие права 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, Пользовательские запросы к службе.
7. В окне **Разрешения для группы Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **Применить**.

► *Чтобы настроить доступ к службам Kaspersky Industrial CyberSecurity for Nodes:*

1. В контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Изменить права пользователей на управление программой**.
2. Выполните шаги 3-7 инструкции для добавления пользователя в группу KICS Administrators.

Для всех пользователей и групп, кроме KICS Administrators и SYSTEM, установите флажки **Запретить** для всех пунктов.

Сигналы тревоги

► *Чтобы настроить уведомления о событиях при обнаружении тревоги, выполните следующие действия:*

1. В дереве консоли Kaspersky Industrial CyberSecurity for Nodes откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.
2. Откроется окно Параметры журналов.

3. На закладке **Уведомления** в блоке **Уведомление администраторов** установите флажок **Путем запуска исполняемого файла для следующих типов событий**:
   - Обнаружен объект.
   - Объект не вылечен.
   - Объект не удален.
   - Объект не помещен на карантин.
   - Объект не помещен в резервное хранилище.
   - Запуск программы запрещен.
   - Запуск программы запрещен по прецеденту.
   - Запуск недоверенного устройства запрещен.
   - Обнаружен объект, недоверенный в KSN
4. Нажмите на кнопку **Настройка**.

   Откроется окно Дополнительные параметры.
5. Выберите закладку **Исполняемый файл** и выполните следующие действия:
   a. В поле **Командная строка** укажите исполняемый файл, который программа будет запускать при обнаружении событий нарушения безопасности.

      Запускаемая программа должна обеспечивать непрерывную выдачу сигнала нарушения безопасности.
   b. В блоке **Запуск с правами** укажите данные учетной записи Администратора.
   c. Нажмите на кнопку **ОК**.
6. На закладке **Уведомления** нажмите на кнопку **Текст сообщения**.
7. В открывшемся окне укажите информацию, которую Kaspersky Industrial CyberSecurity for Nodes будет передавать в составе сигнала тревоги.

   Убедитесь, что в тексте сообщения присутствуют переменные `Тип обнаруженного объекта (%VIRUS_TYPE%)`, `Обнаружено (%VIRUS_NAME%)` и `Событие (%EVENT_TYPE%)`. Если данные переменные отсутствуют, добавьте их с помощью раскрывающегося списка по кнопке **Макрос**. Удаление перечисленных переменных приводит к выходу программы из сертифицируемого состояния.
8. Нажмите на кнопку **ОК**.

   Настройки уведомлений администраторов будут сохранены.

Сообщение сигнала тревоги не содержит данных о действиях по обработке. Kaspersky Industrial CyberSecurity for Nodes сообщает о неудачном результате обработки посредством отдельного сигнала тревоги. Отсутствие сигнала тревоги о неудачной обработке события означает, что объект был обработан в соответствии с настроенными параметрами защиты и проверки.

При неудачном результате обработки Kaspersky Industrial CyberSecurity for Nodes отображает одно из следующих событий:

- Срок действия лицензии истек.
- Базы программы сильно устарели.

- Внутренняя ошибка.
- Внутренняя ошибка программы.
- Базы программы устарели.
- Срок действия лицензии скоро истечет.
- Базы повреждены.
- Целостность программного модуля нарушена.

События аудита

Kaspersky Industrial CyberSecurity for Nodes ведет аудит событий, связанных с управлением программой. Для функционирования в сертифицированном состоянии программа должна фиксировать все события для компонентов Постоянная защита, Проверка по требованию, Контроль запуска программ.

► *Чтобы настроить события аудита перчисленных компонентов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры Журналов**.
3. На закладке **Общие**, установите флажок **Все события для следующих компонентов**:
   - Постоянная защита файлов;
   - Проверка по требованию;
   - Контроль запуска программ.
4. Нажмите на кнопку **ОК**.

Постоянная защита файлов

Для приведения программы в сертифицируемое состояние, требуется произвести дополнительную настройку параметров задачи. По умолчанию, задача Постоянная защита файлов не выполняет проверку архивов.

► *Чтобы добавить архивы к проверяемым объектам, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes разверните узел **Постоянная защита**.
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.

5. На закладке **Общие** в блоке **Защита составных объектов** установите флажок **Все / Только новые архивы**.

   Параметр **Только новые архивы** доступен, если снят флажок **Проверка только новых и и измененных файлов**.

6. Нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes будет выполнять проверку архивов ZIP, CAB, RAR, ARJ- и других форматов.

Проверка по требованию

Kaspersky Industrial CyberSecurity for Nodes проверяет указанную область, файлы и оперативную память защищаемого устройства, а также объекты автозапуска на наличие вирусов и других угроз компьютерной безопасности.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Industrial CyberSecurity for Nodes. Программа проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Industrial CyberSecurity for Nodes создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет их резервными копиями.
- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы в системных папках, например, в папке %windir%\system32. Kaspersky Industrial CyberSecurity for Nodes применяет параметры безопасности, соответствующие рекомендуемому уровню. Вы можете изменять параметры задачи Проверка важных областей.
- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Industrial CyberSecurity for Nodes на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом устройстве.

Kaspersky Industrial CyberSecurity for Nodes может одновременно выполнять несколько задач проверки по требованию.

► *Чтобы проверить работоспособность проверки по требованию, выполните следующие действия:*

1. Загрузите файл eicar.com со страницы сайта EICAR.
2. Сохраните файл eicar.com в папке на локальном диске.

   Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

3. Загрузите файл eicar.com со страницы сайта EICAR.
4. Сохраните файл eicar.com в папке на локальном диске.

   Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

5. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes разверните узел **Проверка по требованию**.
6. Добавьте задачу проверки по требованию.
7. В узле **Проверка по требованию** выберите добавленную задачу.
8. Выберите **Настроить область проверки**.
9. В открывшемся окне **Настройка области проверки** выберите **Область проверки** → **Мой компьютер**.
10. Нажмите на кнопку **Изменить**.
11. Перейдите с узла **Предопределённая область: Мой компьютер** на **Диск**, **папка или сетевой объект**.
12. Укажите путь к папке с файлом eicar.com.
13. Сохраните установленные настройки.
14. Запустите добавленную задачу.
15. Когда Kaspersky Industrial CyberSecurity for Nodes завершит задачу, проверьте журнал выполнения.

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

- Файл eicar.com удален с жесткого диска компьютера.
- В Консоли Kaspersky Industrial CyberSecurity for Nodes журнал выполнения задачи получил статус *Критический*;
- В журнале выполнения задачи появилась строка с информацией об угрозе в файле eicar.com.

► *Чтобы просмотреть журнал выполнения задачи:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes разверните узел **Проверка по требованию**.
2. Выберите созданную задачу проверки по требованию.
3. В панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

kaspersky

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

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

Тестовый файл EICAR не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR http://www.eicar.org/anti_virus_test_file.htm.

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

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

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

Для того чтобы Kaspersky Industrial CyberSecurity for Nodes обработал файл eicar.com с префиксом, в блоке параметров безопасности Защита объектов установите значение Все объекты для задач Kaspersky Industrial CyberSecurity for Nodes "Постоянная защита файлов и задач проверки по требованию".

Таблица 32. Префиксы в файлах EICAR

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

► *Чтобы проверить функцию Постоянная защита, выполните следующие действия:*

1. Загрузите файл eicar.com со страницы сайта EICAR.
2. Сохраните файл eicar.com в папке на локальном диске.

   Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

3. Если вы хотите также проверить работу уведомлений пользователей сети, убедитесь в том, что и на защищаемом компьютере, и на компьютере, на котором вы сохранили файл eicar.com, включена Служба сообщений Microsoft Windows.
4. Откройте Консоль Kaspersky Industrial CyberSecurity for Nodes.
5. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого компьютера одним из следующих способов:
   - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на компьютер, подключившись к компьютеру с помощью программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).
   - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с компьютера, на котором вы его сохранили, через сетевое окружение этого компьютера.

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

- Файл eicar.com удален с жесткого диска компьютера.
- В Консоли Kaspersky Industrial CyberSecurity for Nodes журнал выполнения задачи получил статус *Критический*;

- В журнале выполнения задачи появилась строка с информацией об угрозе в файле eicar.com.
- На компьютере, с которого вы скопировали файл, появилось сообщение Службы сообщений Microsoft Windows следующего содержания: Kaspersky Industrial CyberSecurity for Nodes заблокировала доступ к <путь к файлу eicar.com> на компьютере <сетевое имя компьютера> в <время возникновения события>. Причина: Обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <Имя пользователя>. Имя компьютера: <сетевое имя компьютера, с которого вы скопировали файл>.

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

► *Чтобы просмотреть журнал выполнения задачи:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes разверните узел **Проверка по требованию**.
2. Выберите созданную задачу проверки по требованию.
3. В панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

► *Чтобы проверить функцию Проверка по требованию, выполните следующие действия:*

1. Загрузите файл eicar.com со страницы сайта EICAR.
2. Сохраните его в папке общего доступа на локальном диске любого из компьютеров сети.

   Перед сохранением файла в папке убедитесь, что постоянная защита файлов в этой папке отключена.

3. Откройте Консоль Kaspersky Industrial CyberSecurity for Nodes.
4. Разверните узел **Проверка по требованию**.
5. Выберите вложенный узел **Проверка важных областей**.
6. На закладке **Настройка** области проверки откройте контекстное меню на узле **Сетевое окружение**.
7. Выберите **Добавить сетевой файл**.
8. Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention).
9. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.
10. Запустите задачу Проверка важных областей.

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

- Файл eicar.com удален с жесткого диска компьютера.
- В Консоли Kaspersky Industrial CyberSecurity for Nodes журнал выполнения задачи получил статус *Критический*;
- В журнале выполнения задачи появилась строка с информацией об угрозе в файле eicar.com.

kaspersky

Проверка целостности компонентов программы

Программа Kaspersky Industrial CyberSecurity for Nodes содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленник может подменить один или несколько модулей или файлов программы модулями или файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов программы, в Kaspersky Industrial CyberSecurity for Nodes предусмотрена проверка целостности компонентов программы. Программа проверяет модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Целостность компонентов программы проверяется с помощью инструмента integrity_checker.exe, использующего для проверки файл манифеста integrity_check_manifest.xml, защищенный криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с правами Администратора.

Инструмент поставляется отдельно от Kaspersky Industrial CyberSecurity for Nodes на сертифицированном CD-диске.

Инструмент проверки целостности рекомендуется запускать с сертифицированного CD-диска, чтобы гарантировать целостность самого инструмента. При запуске инструмента с CD-диска необходимо указать полный путь к файлу манифеста в директории программы.

► *Чтобы проверить целостность компонентов программы:*

1. Задайте папку установки программы через пользовательскую переменную окружения при помощи команды:

   ```
   set ProductRoot=<путь к папке установки программы>
   ```

   По умолчанию используются следующие папки установки Kaspersky Industrial CyberSecurity for Nodes:

   - в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes;
   - в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.

По умолчанию используются следующие папки установки Консоли управления Kaspersky Industrial CyberSecurity for Nodes:

- в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools;
- в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools.

По умолчанию используются следующие папки установки Плагина управления Kaspersky Industrial CyberSecurity for Nodes:

- в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kics3.2.plg;
- в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kics3.2.plg.

По умолчанию используется следующая папка установки Веб-плагина управления Kaspersky Industrial CyberSecurity for Nodes:

- %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kics_windows.

По умолчанию используются следующие папки установки Kaspersky Security Gateway:

- в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Gateway;
- в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Gateway.

По умолчанию используются следующие папки установки Kaspersky Endpoint Agent:

- в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Agent;
- в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Agent.

По умолчанию используются следующие папки установки Плагина управления Kaspersky Endpoint Agent:

- в 32-разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\soyuz4.0.plg;
- в 64-разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\soyuz4.0.plg.

По умолчанию используется следующая папка установки Веб-плагина управления Kaspersky Endpoint Agent:

- %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\soyuz_windows.

2. Запустите проверку целостности компонента программы при помощи команды:

```
integrity_checker.exe --manifest <путь к файлу integrity_check_manifest.xml>
[--define <код компонента программы>],
```

где параметр `--manifest <путь к файлу integrity_check_manifest.xml>` используется для указания пути к файлу integrity_check_manifest.xml, если он расположен не в одной папке с integrity_checker.exe.

Коды компонентов программы указаны в статье Программные компоненты Kaspersky Industrial CyberSecurity for Nodes (на стр. 309).

Вы можете указать сразу несколько компонентов программы, для каждого указывая ключ `--define`.

Инструмент проверки целостности можно запустить со следующими дополнительными параметрами:

- `--help` – показать справку для параметров инструмента.
- `--verbose` – применить вывод расширенной информации о выполненных действиях и результатах. Если вы не укажите этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <имя файла>`, где `<имя файла>` – имя файла, используемое для записи событий, произошедших во время проверки. По умолчанию события передаются в стандартный поток stdout.

Пример команды:

```
integrity_checker.exe integrity_check_manifest.xml --define AntiCryptor
--define DeviceControl --trace=.\AntiCryptor_integrity_check_trace.log
```

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

Этот раздел содержит информацию о правах на управление Kaspersky Industrial CyberSecurity for Nodes 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

По умолчанию пользователи, входящие в группу "Администраторы" на защищаемом сервере, имеют доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes.

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

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

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

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

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Industrial CyberSecurity for Nodes.

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

Таблица 33. Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Industrial CyberSecurity for Nodes.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes. • Редактировать настройки программы.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Industrial CyberSecurity for Nodes и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Industrial CyberSecurity for Nodes.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Industrial CyberSecurity for Nodes.
Чтение прав	Возможность просматривать список пользователей Kaspersky Industrial CyberSecurity for Nodes 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.

kaspersky

О правах доступа на управление службой Kaspersky Security

При установке Kaspersky Industrial CyberSecurity for Nodes регистрирует в Windows службу Kaspersky Security (KAVFS), так как программа включает в себя функциональные компоненты, запускаемые при старте операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности на защищаемом компьютере через управление службой Kaspersky Security, вы можете ограничивать права на управление службой Kaspersky Security с помощью локальной Консоли Kaspersky Industrial CyberSecurity for Nodes или плагина управления Kaspersky Security Center.

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.

Вы не можете удалять учетную запись пользователя SYSTEM, а также редактировать права данной учетной записи. Если в учетную запись SYSTEM были внесены изменения, при сохранении настроек будут восстановлены максимальные права данной учетной записи.

Пользователи, которые имеют доступ к функции уровня **Изменение прав**, могут предоставлять доступ к управлению службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом компьютере или компьютере, входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Industrial CyberSecurity for Nodes один из следующих предустановленных уровней доступа на управление службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей службы Kaspersky Security, а также запускать и останавливать работу службы Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры работы и права пользователей службы Kaspersky Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей службы Kaspersky Security.
- **Исполнение** – возможность запускать и останавливать работу службы Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: давать или ограничивать права на управление службой Kaspersky Security (см. таблицу ниже).

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

Таблица 34. Разграничение прав доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

Функция	Описание
Чтение настроек службы	Возможность просматривать общие параметры работы и права пользователей службы Kaspersky Security.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения Kaspersky Security у Диспетчера управления службами Microsoft Windows.
Запрос статуса у службы	Возможность запрашивать статус выполнения службы у службы Kaspersky Security.
Перечисление зависимых служб	Возможность просматривать список служб, от которых зависит служба Kaspersky Security, а также служб, зависимых от службы Kaspersky Security.
Изменение параметров службы	Возможность просматривать и изменять общие параметры работы и права пользователей службы Kaspersky Security.
Запуск службы	Возможность запускать выполнение службы Kaspersky Security.
Остановка службы	Возможность останавливать выполнение службы Kaspersky Security.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение службы Kaspersky Security.
Чтение прав	Возможность просматривать список пользователей службы Kaspersky Security и права доступа каждого пользователя.
Изменение прав	Возможности: • добавлять и удалять пользователей службы Kaspersky Security; • изменять права доступа пользователей к службе Kaspersky Security.
Удаление службы	Возможность удаления службы Kaspersky Security в Диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.

kaspersky

О правах доступа к службе Kaspersky Security

Вы можете просмотреть список служб Kaspersky Industrial CyberSecurity for Nodes.

При установке Kaspersky Industrial CyberSecurity for Nodes регистрирует службу управления программой Kaspersky Security Management (KAVFSGT). Чтобы управлять программой через Консоль Kaspersky Industrial CyberSecurity for Nodes, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Industrial CyberSecurity for Nodes, 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.

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

Вы не можете разрешать или запрещать пользователям доступ к службе Kaspersky Security Management, настраивая параметры Kaspersky Industrial CyberSecurity for Nodes.

Вы можете соединиться с Kaspersky Industrial CyberSecurity for Nodesc локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с таким же именем и таким же паролем.

Настройка прав доступа для Kaspersky Industrial CyberSecurity for Nodes и службы Kaspersky Security

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.

2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Если вы хотите настроить параметры политики для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства**: **<Имя политики>**.
   - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы**.

   > Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Дополнительные возможности** 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.
   - 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"**.

4. 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**.

5. Нажмите на кнопку **Применить**.

   Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Security, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Если вы хотите настроить параметры политики для группы компьютеров, выберите закладку **Политики** и откройте **Свойства: <Имя политики>**.
   - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы**.

   > Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Дополнительные возможности** 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.
   - Выберите пункт **Изменить права пользователей на управление Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes"**.
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 или службой Kaspersky Security.
   - **Чтение**:
     - следующие права на управление Kaspersky Industrial CyberSecurity for Nodes: **Чтение статистики**, **Чтение параметров**, **Чтение журналов** и **Чтение прав**;
     - следующие права 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, кроме **Изменение прав**;
     - следующие права 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**, **Пользовательские 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** выберите нужного пользователя или группу.
   b. Нажмите на кнопку **Изменить**.
   c. В открывшемся окне перейдите по ссылке **Показать особые разрешения**.
   d. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить** или **Запретить**).
   e. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
   f. Нажмите на кнопку **ОК**.
   g. В окне **Дополнительные параметры безопасности для Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **ОК.**

7. В окне **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes"** нажмите на кнопку **Применить**.

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

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

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей. Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к локальной Консоли Kaspersky Industrial CyberSecurity for Nodes;
- изменение компонентного состава Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Industrial CyberSecurity for Nodes хранит заданный пароль в виде контрольной суммы, рассчитанной при задании пароля.

Вы можете экспортировать и импортировать параметры программы, защищенной паролем. Конфигурационный файл, созданный по результатам экспорта параметров защищенной программы, содержит значение контрольной суммы пароля и значение модификатора, используемого для удлинения строки пароля.

Kaspersky Industrial CyberSecurity for Nodes не контролирует стойкость пароля и не блокирует ввод пароля при многократных попытках некорректного ввода.

При создании пароля рекомендуется соблюдать следующие условия:

- Пароль не должен содержать имя учетной записи или имя компьютера.
- Длина пароля должна быть не менее 8 символов.
- Пароль содержит символы, соответствующие по крайней мере трем из следующих категорий:
  - прописные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы восклицательного знака (!), знака доллара ($), решетки (#) и знака процента (%).

Вы можете экспортировать и импортировать параметры программы, защищенной паролем. Конфигурационный файл, созданный по результатам экспорта параметров защищенной программы, содержит значение контрольной суммы пароля и значение модификатора, используемого для удлинения строки пароля.

Не изменяйте значение контрольной суммы или модификатора в конфигурационном файле. Импорт параметров пароля, измененных вручную, может привести к полному блокированию доступа к управлению программой.

► *Чтобы сбросить заданный пароль, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы**.
3. В блоке **Безопасность** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В блоке **Параметры применения пароля** установите флажок **Использовать защиту паролем**. Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям <PRODUCT_NAME_GEN
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **ОК**.

   Настроенные параметры будут сохранены. Kaspersky Industrial CyberSecurity for Nodes будет запрашивать пароль при доступе к защищаемым операциям.

Разрешение сетевых соединений для службы Kaspersky Security Management

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы разрешить сетевые соединения для службы Kaspersky Security Management на защищаемом компьютере, выполните следующие действия:*

1. На защищаемом компьютере под управлением Microsoft Windows выберите пункт **Пуск → Панель управления → Безопасность → Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** выберите пункт **Изменить параметры**.

3. На закладке **Исключения** в списке предустановленных исключений установите флажки **COM + Сетевой доступ**, **Windows Management Instrumentation (WMI)** и **Remote Administration**.
4. Нажмите на кнопку **Добавить программу**.
5. В окне **Добавление программы** выберите файл kavfsgt.exe. Этот файл хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Industrial CyberSecurity for Nodes.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Параметры брандмауэра Windows**.

Сетевые соединения для службы Kaspersky Security Management на защищаемом компьютере будут разрешены.

Интерфейс программы

Программой Kaspersky Industrial CyberSecurity for Nodes можно управлять с помощью следующих интерфейсов:

- Локальная Консоль программы.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center Web Console.

Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Industrial CyberSecurity for Nodes, а также настраивать параметры программы, изменять набор доступных компонентов программы, добавлять ключи, запускать и останавливать задачи.

Программой можно управлять из Kaspersky Security Center с помощью плагина управления Kaspersky Industrial CyberSecurity for Nodes. Подробная информация об интерфейсе Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (далее также Веб-консоль) – это веб-приложение, предназначенное для централизованного выполнения основных задач по управлению и поддержке системы безопасности сети организации. Веб-консоль – это компонент Kaspersky Security Center, обеспечивающий пользовательский интерфейс. Подробная информация о Kaspersky Security Center Web Console приведена в *справке Kaspersky Security Center*.

Веб-консоль позволяет выполнять следующие действия:

- Контролировать состояние системы безопасности организации.
- Устанавливать программы "Лаборатории Касперского" на устройства в сети.
- Управлять установленными приложениями.
- Просматривать отчеты о состоянии системы безопасности.

kaspersky

В этом разделе

Сравнение средств управления Kaspersky Security Center и их ограничения

Набор функций, доступных в Kaspersky Industrial CyberSecurity for Nodes, зависит от средств управления (см. таблицу ниже).

Программой можно управлять с помощью следующих консолей Kaspersky Security Center:

- Консоль администрирования. Оснастка Консоли управления Microsoft (MMC), установленная на рабочем месте администратора.
- Веб-консоль. Компонент Kaspersky Security Center, установленный на Сервере администрирования. Веб-консоль позволяет работать через браузер на любом компьютере, имеющем доступ к Серверу администрирования.

kaspersky

Таблица 35. Сравнение функций Kaspersky Industrial CyberSecurity for Nodes в зависимости от средств управления

Функция	Kaspersky Security Center	
	Консоль администрирования	Веб-консоль
Постоянная защита компьютераа		
Постоянная защита файлов	✓	✓
Использование KSN	✓	✓
Защита трафика	✓	✓
Защита от эксплойтов	✓	✓
Защита от сетевых угроз	✓	✓
AMSI-защита	✓	✓
Контроль активности на компьютерах		
Контроль запуска программ	✓	✓
Контроль устройств	✓	✓
Контроль активности в сети		
Управление сетевым экраном	✓	✓
Защита от шифрования	✓	✓
Диагностика системы		
Мониторинг файловых операций	✓	✓
Анализ журналов	✓	✓
Журналы и уведомления		
Журналы	✓	✓
Уведомления	✓	✓
Хранилища		
Карантин	✓	✓
Резервное хранилище	✓	✓
Заблокированные сетевые сеансы	✓	✓

Функция	Kaspersky Security Center	
	Консоль администрирования	Веб-консоль
Дополнительные возможности		
Управление иерархическим хранилищем	✓	✓
Доверенная зона	✓	✓
Проверка съемных дисков	✓	✓
Kaspersky Endpoint Agent	✓	✓
Задачи		
Активация программы	✓	✓
Проверка целостности программы	✓	✓
Мониторинг целостности файлов на основе эталона	✓	✓
Копирование обновлений	✓	✓
Обновление баз программы	✓	✓
Проверка по требованию	✓	✓
Откат обновления баз программы	✓	✓
Формирование правил контроля запуска программ	✓	✓
Формирование правил контроля устройств	✓	✓
Обновление модулей программы	✓	✓

Ограничения Веб-плагина

Веб-плагин Kaspersky Industrial CyberSecurity for Nodes имеет следующие ограничения по сравнению с Плагином управления Kaspersky Industrial CyberSecurity for Nodes:

- Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
- Для задачи Постоянная защита файлов нельзя изменить стандартный уровень безопасности.
- Для задачи Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.
- Для задачи Контроль устройств нельзя сформировать правила на основе подключенных устройств или данных системы.

Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Industrial CyberSecurity for Nodes и об управлении программой, установленной на защищаемом компьютере или группе защищаемых компьютеров.

kaspersky

В этом разделе

Управление Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center

Вы можете централизованно управлять несколькими защищаемыми компьютерами с установленной программой Kaspersky Industrial CyberSecurity for Nodes, объединенными в группу администрирования, с помощью Плагина управления Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Security Center также позволяет отдельно настраивать параметры каждого защищаемого компьютера, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center. Группа администрирования включает устройства с установленной программой Kaspersky Industrial CyberSecurity for Nodes, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого компьютера недоступны для настройки, если работа Kaspersky Industrial CyberSecurity for Nodes на этом защищаемом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center.

  С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, и параметры запуска локальных системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

  С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.
- **С помощью окна свойств отдельного устройства**. В окне **Свойства: <Имя защищаемого устройства>** можно удаленно настроить параметры задачи для отдельного защищаемого компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры программы, так и параметры всех задач Kaspersky Industrial CyberSecurity for Nodes, если выбранный защищаемый компьютер не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры для группы защищаемых компьютеров или для отдельных защищаемых компьютеров.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Security Center Web Console.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к общим параметрам из политики

► *Чтобы открыть параметры программы Kaspersky Industrial CyberSecurity for Nodes из политики, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.

4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. Нажмите на кнопку **Настройка** для группы параметров, которую вы хотите настроить.

Переход к общим параметрам из окна свойств программы

► *Чтобы открыть окно свойств Kaspersky Industrial CyberSecurity for Nodes для отдельного защищаемого компьютера, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Industrial CyberSecurity for Nodes 3.2**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры Kaspersky Industrial CyberSecurity for Nodes 3.2**.
7. Перейдите в раздел **Параметры программы**.

Настройка общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

В этом разделе

kaspersky

Настройка параметров масштабируемости, интерфейса и проверки в Kaspersky Security Center

► *Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** в блоке **Масштабируемость, интерфейс и настройки сканирования** нажмите на кнопку **Настройка**.
5. В окне **Дополнительные параметры программы** на закладке **Общие** настройте следующие параметры:
   - В разделе **Параметры масштабируемости** настройте параметры, определяющие количество процессов, которые использует Kaspersky Industrial CyberSecurity for Nodes:
     - **Определять параметры масштабируемости автоматически**

       Kaspersky Industrial CyberSecurity for Nodes автоматически регулирует количество используемых процессов.

       Это значение установлено по умолчанию.
     - **Указать количество рабочих процессов вручную**

       Kaspersky Industrial CyberSecurity for Nodes контролирует количество активных рабочих процессов в соответствии с указанными значениями.

       - **Количество процессов для постоянной защиты**

         Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

       - **Количество процессов для фоновых задач проверки по требованию**

         Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
   - В разделе **Взаимодействие с пользователем** настройте отображение Значка области уведомлений в панели задач: снимите или установите флажок **Показывать Значок области уведомлений**.
6. На закладке **Сканирование** настройте следующие параметры:

- **Восстанавливать атрибуты файлов после сканирования**

  Когда Kaspersky Industrial CyberSecurity for Nodes выполняет задачи проверки по требованию, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Industrial CyberSecurity for Nodes возвращает исходное значение времени последнего обращения к файлу.

  Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.

  По умолчанию эта опция включена.

- **Ограничивать сканирующий поток в использовании CPU**

  Kaspersky Industrial CyberSecurity for Nodes ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)** .

  Включение этой опции может негативно сказаться на производительности Kaspersky Industrial CyberSecurity for Nodes.

  По умолчанию эта опция выключена.

- **Предельное значение (в процентах)**

  Максимально допустимое значение загрузки процессора программой Kaspersky Industrial CyberSecurity for Nodes.

  Это поле доступно, если выбран параметр **Ограничивать сканирующий поток в использовании CPU**.

- **Папка для временных файлов, создаваемых при сканировании**

  Папка, в которую программа Kaspersky Industrial CyberSecurity for Nodes распаковывает файлы архивов при проверке.

  По умолчанию используется папка C:\Windows\Temp.

7. Нажмите на кнопку **OK**.

Настроенные параметры программы будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам

программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

4. В разделе **Параметры программы** в подразделе **Настройка** нажмите на кнопку **Безопасность и надежность**.
5. В окне **Параметры безопасности** настройте следующие параметры:
   - В разделе **Самозащита** включите или отключите функцию **Защищать процессы программы от внешних угроз** .
   - В разделе **Самозащита** задайте пароль для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.
   - В разделе **Параметры применения пароля** настройте параметры восстановления задач Kaspersky Industrial CyberSecurity for Nodes в случае сбоев в работе программы или аварийного завершения работы программы.
     - **Выполнять восстановление задач**

       Флажок включает или выключает восстановление задач Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes автоматически восстанавливает задачи Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не восстанавливает задачи Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы.

       По умолчанию флажок установлен.

     - **Параметры надежности**

       Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Industrial CyberSecurity for Nodes. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.
   - В разделе **Выполнять восстановление задач проверки по требованию не более (раз)** задайте ограничение нагрузки на защищаемый компьютер со стороны Kaspersky Industrial CyberSecurity for Nodes при переходе на источник бесперебойного питания:
     - **Не запускать задачи проверки по расписанию**

       Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого компьютера на источник бесперебойного питания до восстановления стандартного режима питания.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes не запускает задачи проверки по расписанию при переходе защищаемого компьютера на источник бесперебойного питания до восстановления стандартного режима питания.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes запускает задачи проверки по расписанию вне зависимости от режима питания.

       По умолчанию флажок установлен.

     - **Остановить выполняемые задачи проверки**

       Флажок включает или выключает выполнение запущенных задач проверки при

переходе защищаемого компьютера на источник бесперебойного питания.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes останавливает выполнение запущенных задач проверки при переходе защищаемого компьютера на источник бесперебойного питания.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes продолжает выполнение запущенных задач проверки при переходе защищаемого компьютера на источник бесперебойного питания.

По умолчанию флажок установлен.

- В разделе **Самозащита** задайте пароль для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.

6. Нажмите на кнопку **ОК**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Industrial CyberSecurity for Nodes к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Параметры программы** в подразделе **Настройка** нажмите на кнопку **Параметры соединения**.

   Откроется окно **Параметры соединения**.
5. В окне **Параметры соединения** настройте следующие параметры:
   - В разделе **Параметры прокси-сервера** задайте параметры использования прокси-сервера:
     - **Не использовать прокси-сервер**;

       Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
     - Использовать указанный прокси-сервер;

       Если выбран этот вариант, для соединения с KSN Kaspersky Industrial CyberSecurity for Nodes использует параметры прокси-сервера, указанные вручную.

- **IP-адрес или символьное имя прокси-сервера и номер порта**;
- **Не использовать прокси-сервер для локальных адресов**.

  Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Industrial CyberSecurity for Nodes.

  Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Industrial CyberSecurity for Nodes, происходит напрямую. Прокси-сервер не используется.

  Если флажок снят, для подключения к локальным устройствам используется прокси-сервер.

  По умолчанию флажок установлен.

- В разделе **Параметры аутентификации на прокси-сервере** задайте параметры аутентификации:
  - Выберите параметры аутентификации в раскрывающемся списке.
    - **Не использовать аутентификацию** – проверка подлинности не производится. Этот режим выбран по умолчанию.
    - **Использовать NTLM-аутентификацию** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
    - **Использовать NTLM-аутентификацию с именем пользователя и паролем** – проверка подлинности по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
    - **Использовать имя пользователя и пароль** – проверка подлинности с помощью имени пользователя и пароля.
  - Если требуется, укажите имя пользователя и пароль.
- В разделе **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

6. Нажмите на кнопку **OK**.

Настроенные параметры соединения будут сохранены.

Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещен политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике. Kaspersky Industrial CyberSecurity for Nodes будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с параметрами расписания по умолчанию.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если защищаемое устройство исключено из группы администрирования, расписание локальных системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию локальных системных задач Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.
2. На закладке **Политики** в контекстном меню политики, для которой вы хотите настроить запуск по расписанию локальных системных задач Kaspersky Industrial CyberSecurity for Nodes для группы защищаемых устройств, выберите пункт **Свойства**.
3. В окне **Свойства: <Имя политики>** выберите раздел **Параметры программы**. В разделе **Запуск локальных системных задач** нажмите на кнопку **Настройка** и выполните одно из следующих действий:
   - Установите флажки **Задачи проверки по требованию** и **Задачи обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
   - Снимите флажки **Задачи проверки по требованию** и **Задачи обновления и копирования обновлений**, чтобы запретить запуск по расписанию перечисленных задач.

   Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.
4. Убедитесь, что настраиваемая политика активна и применена к выбранной группе защищаемых устройств.
5. Нажмите на кнопку **OK**.

Настроенные параметры расписания выбранных задач будут применены.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

► *Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.
5. В окне **Резервное хранилище** на закладке **Параметры хранилищ** настройте следующие параметры резервного хранилища:
   - Если вы хотите задать папку-местоположение резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого компьютера или введите полный путь к ней.
   - Чтобы задать максимальный размер резервного хранилища, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.
   - Чтобы задать порог свободного места в резервном хранилище:
     - Укажите значение параметра **Максимальный размер резервного хранилища (МБ)**.
     - Установите флажок **Порог доступного пространства (МБ)**.
     - Укажите минимальное значение свободного места в папке резервного хранилища в мегабайтах.
   - Чтобы указать папку для восстановленных объектов, выполните одно из следующих действий:
     - В разделе **Параметры восстановления объектов** выберите нужную папку на локальном диске защищаемого устройства.
     - Введите имя папки и полный путь к ней в поле **Папка, в которую восстанавливаются объекты**.
6. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие параметры карантина:
   - Чтобы изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого компьютера.

- Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.
- Чтобы задать минимальный объем свободного места в карантине, установите флажки **Максимальный размер карантина (МБ)** и **Порог доступного пространства (МБ)**, затем в поле ввода укажите значение в мегабайтах.
- Чтобы изменить папку, в которую восстанавливаются объекты из карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого компьютера.

7. Нажмите на кнопку **OK**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Industrial CyberSecurity for Nodes на нескольких защищаемых компьютерах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Industrial CyberSecurity for Nodes на всех защищаемых компьютерах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *активная* в Консоли администрирования.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Industrial CyberSecurity for Nodes. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых компьютерах: *Запретить изменение параметров*. После применения политики Kaspersky Industrial CyberSecurity for Nodes использует на защищаемых компьютерах значения параметров, для которых в свойствах политики вы установили значок 🔒. В этом случае Kaspersky Industrial CyberSecurity for Nodes не использует значения параметров, действовавшие до применения политики. Kaspersky Industrial CyberSecurity for Nodes не применяет значения параметров активной политики, для которых в свойствах политики установлен значок 🔓.

Если политика активна, то значения параметров, отмеченные в политике значком 🔒, отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком 🔓) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком 🔒, также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемый компьютер с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры задачи Постоянная защита компьютера, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

В этом разделе

Создание политики

Перед созданием политики необходимо установить плагин администрирования klcfginst.exe.

Создание новой политики состоит из следующих этапов:

1. Создание политики с помощью мастера создания политик. В окнах Мастера установки вы можете настроить постоянную защиту компьютера.
2. Настройка параметров политики. В окне **Свойства: <Имя политики>** созданной политики вы можете настроить следующие параметры:
   - Параметры задачи Постоянная защита компьютера.
   - Общие параметры Kaspersky Industrial CyberSecurity for Nodes.
   - Параметры карантина и резервного хранилища.
   - Уровень детализации в журналах выполнения задач.
   - Уведомления пользователя и администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

► *Чтобы создать политику для группы защищаемых компьютеров, на которых установлена и запущена программа Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для защищаемых компьютеров которой вы хотите создать политику.
2. В панели результатов выбранной группы администрирования выберите закладку **Политики** и запустите мастер создания политик по ссылке **Создать политику**.

   Откроется окно **Мастер создания политики**.
3. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Industrial CyberSecurity for Nodes.
4. Нажмите на кнопку **Далее**.
5. В поле **Имя** укажите название групповой политики.

Имя политики не должно содержать следующие символы: " * < : > ? \ | .

6. Чтобы применить параметры политики, используемые в предыдущей версии программы, выполните следующие действия:
   a. Установите флажок **Использовать параметры политики, созданной для предыдущей версии программы**.
   b. Нажмите на кнопку **Выбрать**.
   c. Выберите политику, которую требуется применить.
   d. Нажмите на кнопку **Далее**.
7. В окне **Выбор типа операции** в блоке **Способ создания политики** выберите один из следующих вариантов:
   a. **Создать**, чтобы создать политику с заданными по умолчанию параметрами.
   b. **Импортировать политику, созданную с помощью Kaspersky Industrial CyberSecurity for Nodes**, чтобы использовать импортированную версию политики в качестве шаблона.
   c. Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в который вы сохранили параметры ранее созданной политики.
8. В окне **Выбор типа операции** в блоке **Параметры Постоянной защиты файлов** настройте параметры задачи:
   a. Снимите флажок **Запускать задачу по расписанию**, если желаете выключить запуск задачи по расписанию.
   b. Выберите режим работы задачи.

      Если режим работы задачи не выбран, вы не можете перейти на следующий шаг Мастера создания политики.

   c. Нажмите на кнопку **Далее**.
9. В окне **Постоянная защита компьютера** настройте параметры компонентов программы:
   a. Если необходимо, измените заданные по умолчанию параметры компонентов постоянной защиты компьютера:
      vi. Нажмите на кнопку **Настройка** в подразделе компонента программы.
      vii. В открывшемся окне настройте параметры компонента.
      viii. Нажмите на кнопку **ОК**.
   b. Разрешите или запретите применение параметров компонентов постоянной защиты компьютера на защищаемых устройствах сети:
      - Нажмите на кнопку 🔒, чтобы разрешить настройку параметров компонента программы на защищаемых устройствах сети и запретить применение параметров компонента программы, настроенных в политике.
      - Нажмите на кнопку 🔓, чтобы запретить настройку параметров компонента программы на защищаемых устройствах сети и разрешить применение параметров компонента программы, настроенных в политике.

c. Нажмите на кнопку **Далее**.

10. В окне **Целевая группа** в поле **Группа** укажите устройства, на которые будет распространена политика.
11. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:
    - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.
    - **Неактивная политика**, если сразу применять созданную политику не требуется. Вы сможете активировать эту политику позже.
    - Установите флажок **Открыть свойства политики сразу после создания**, чтобы автоматически закрыть **Мастер создания политики** и настроить новую политику после нажатия на кнопку **Далее**.
12. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик на закладке **Политики** выбранной группы администрирования. В окне **Свойства: <Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Industrial CyberSecurity for Nodes.

Разделы параметров политики Kaspersky Industrial CyberSecurity for Nodes

Общие

В разделе **Общие** можно настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров для родительских и дочерних политик.

Уведомление о событиях

В разделе **Уведомление о событиях** можно настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** можно настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

Таблица 36. Параметры в разделе Параметры программы

Раздел	Параметры
Масштабируемость, интерфейс и настройки сканирования	В подразделе **Масштабируемость, интерфейс и настройки сканирования** по кнопке **Настройка** вы можете настроить следующие параметры: • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
Безопасность и надежность	В подразделе **Безопасность и надежность** по кнопке **Настройка** вы можете настроить следующие параметры: • настроить параметры запуска задачи; • указать действия программы при переходе защищаемого компьютера на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.
Параметры соединения	В подразделе **Параметры соединения** по кнопке **Настройка** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск локальных системных задач	В подразделе **Запуск локальных системных задач** по кнопке **Настройка** можно разрешить или запретить запуск следующих локальных системных задач по расписанию, настроенному на защищаемых устройствах: • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Таблица 37. Параметры в разделе Дополнительные возможности

Раздел	Параметры
Доверенная зона	В подразделе **Настройка** по кнопке **Доверенная зона** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных дисков	В подразделе **Проверка съемных дисков** по кнопке **Настройка** вы можете настроить параметры проверки съемных дисков.
Права пользователей на управление программой	В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Industrial CyberSecurity for Nodes.
Права пользователей на управление службой Kaspersky Security Service	В подразделе **Права пользователей на управление службой Kaspersky Security Service** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.
Хранилища	В подразделе **Хранилища** по кнопке **Настройка** можно настроить следующие параметры карантина, резервного хранилища и заблокированных сетевых сеансов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить продолжительность блокировки сетевых сеансов.

Постоянная защита компьютера

Таблица 38. Параметры в разделе Постоянная защита компьютера

Раздел	Параметры
Постоянная защита файлов	В подразделе **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную; • настроить параметры запуска задачи.
Использование KSN	В подразделе **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать действия над объектами, недоверенными в KSN; • настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN. Нажмите на кнопку **Обработка данных**, чтобы принять или отклонить Положение о KSN, а также настроить параметры передачи данных.
Защита от эксплойтов	В подразделе **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.

Контроль активности на компьютерах

Таблица 39. Параметры в разделе Контроль активности на компьютерах

Раздел	Параметры
Контроль запуска программ	В подразделе **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • настроить параметры запуска задачи.
Контроль устройств	В подразделе **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры запуска задачи.
Контроль Wi-Fi	В подразделе **Контроль Wi-Fi** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • управлять режимами работы компонента; • настроить правила контроля Wi-Fi сетей.

Контроль активности в сети

Таблица 40. Параметры в разделе Контроль активности в сети

Раздел	Параметры
Управление сетевым экраном	В подразделе **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • настроить правила сетевого экрана; • настроить параметры запуска задачи.
Защита от шифрования	В подразделе **Защита от шифрования** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; настроить область защиты от вредоносного шифрования; • настроить параметры запуска задачи.

Диагностика системы

Таблица 41. Параметры в разделе Диагностика системы

Раздел	Параметры
Мониторинг файловых операций	В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере.
Анализ журналов	В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого компьютера на основе результатов анализа журнала событий Windows.

Журналы и уведомления

Таблица 42. Параметры в разделе Журналы и уведомления

Раздел	Параметры
Журналы выполнения задач	В подразделе **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач. • указать параметры интеграции SIEM-системы с Kaspersky Security Center.
Уведомления о событиях	В подразделе **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и запрещено недоверенное устройство* и *Сетевая сессия добавлена в список недоверенных*; • указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В разделе **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, включая объекты карантина и резервного хранилища, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования.
Инциденты	В подразделе **Инциденты** по кнопке **Настройка** можно выбрать уведомления, на основе которых программа будет формировать инциденты на стороне Kaspersky Security Center.

История ревизий

В разделе **История ревизий** можно управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Настройка политики

► *Чтобы настроить параметры политики, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:
   - Выберите параметр **Свойства** в контекстном меню политики.
   - Перейдите по ссылке **Настроить параметры политики** в панели результатов выбранной политики.
   - Дважды щелкните мышью по нужной политике.
4. На закладке **Общие** в разделе **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
   - **Активная политика**, если вы хотите, чтобы политика применялась на всех защищаемых компьютерах, входящих в выбранную группу администрирования.
   - **Неактивная политика**, если вы хотите активировать политику позже на всех защищаемых компьютерах, входящих в выбранную группу администрирования.

   Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Industrial CyberSecurity for Nodes.
5. Настройте параметры программы в остальных разделах политики.

   Вы можете включать и выключать выполнение любой задачи на всех защищаемых компьютерах, входящих в группу администрирования, с помощью политики Kaspersky Security Center.
   Вы можете настроить применение параметров политики на всех защищаемых устройствах сети для каждого отдельного компонента программы.
6. Нажмите на кнопку **OK**.

Настроенные параметры будут применены в политике.

Создание и настройка задач в Kaspersky Security Center

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

kaspersky

В этом разделе

О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых компьютеров. Вы можете создавать задачи следующих типов в Kaspersky Security Center:

- Активация программы;
- Копирование обновлений;
- Обновление баз программы;
- Обновление модулей программы;
- Откат обновления баз программы;
- Проверка по требованию;
- Проверка целостности программы;
- Мониторинг целостности файлов на основе эталона;
- Формирование правил контроля запуска программ;
- Формирование правил контроля устройств.

Вы можете создать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого компьютера: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**.
- Для группы администрирования: в панели результатов узла выбранной группы защищаемых компьютеров на закладке **Задачи**.
- Для набора защищаемых компьютеров: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 373) по требованию на всех защищаемых компьютерах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center

► *Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый сервер.
     b. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства и выберите пункт **Свойства**.
     c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, для которой требуется создать задачу.
     c. В панели результатов перейдите на закладку **Задачи** и выберите пункт **Создать задачу**.
   - Чтобы создать задачу для произвольного набора защищаемых компьютеров, выполните следующие действия:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, к которой принадлежат защищаемые компьютеры.
     c. Выберите защищаемый компьютер или произвольный набор защищаемых компьютеров.
     d. В раскрывающемся списке **Выполнить действие** выберите **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Industrial CyberSecurity for Nodes 3.2** выберите тип создаваемой задачи.
3. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно **Настройка**. В зависимости от типа задачи параметры могут различаться.
   - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 570).
   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
     a. Выберите источник обновлений в окне **Источник обновлений**.
     b. Нажмите на кнопку **Настройка параметров соединения**. В окне **Настройка параметров соединения** настройте параметры доступа к прокси-серверу при подключении к источнику обновлений.

- Для создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Настройка параметров обновления модулей программы**.

  a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.

  b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого компьютера. Чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически запускала перезагрузку защищаемого компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.

  c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Industrial CyberSecurity for Nodes, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

  "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Настройка параметров копирования обновлений**.
- Для создания задачи Активация программы:

  a. В окне **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу.

  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.

- Создайте задачу Формирование правил контроля запуска программ (см. раздел "Создание задачи Формирование правил контроля запуска программ" на стр. 690).
- Создайте задачу Формирование правил контроля устройств (см. раздел "Создание правил с помощью задачи Формирование правил контроля устройств" на стр. 738).

4. Настройте расписание задачи (см. раздел "Настройка расписания задач" на стр. 404).

   Вы можете настраивать расписание для всех типов задач, кроме задачи Откат обновления баз программы.

5. Нажмите на кнопку **OK**.
6. Если задача создана для набора защищаемых компьютеров, выберите сеть (группу) защищаемых компьютеров, на которых она будет выполняться.
7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, которую вы хотите использовать для запуска задачи.
8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы " * < > ? \ | :).

   Рекомендуется включить в название задачи ее тип (например, Проверка по требованию общих папок).

9. В окне **Завершение создания задачи** выполните следующие действия:
   a. Установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите запустить задачу сразу после создания.
   b. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера

Если программа работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения для отдельного компьютера.

► *Чтобы перейти к параметрам локальной задачи для отдельного компьютера:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый компьютер.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - в контекстном меню на имени защищаемого компьютера выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
4. Перейдите в раздел **Задачи**.
5. В списке задач выберите локальную задачу, параметры которой требуется настроить, одним из следующих способов:
   - двойным щелчком мыши на названии задачи;
   - выберите задачу в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени задачи выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи>**.

► *Чтобы перейти к общим параметрам программы для отдельного компьютера:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый компьютер.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - в контекстном меню на имени защищаемого компьютера выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
4. Перейдите в раздел **Программы**.

5. В списке установленных программ выберите Kaspersky Industrial CyberSecurity for Nodes одним из следующих способов:
   - двойным щелчком мыши на имени Kaspersky Industrial CyberSecurity for Nodes;
   - выберите Kaspersky Industrial CyberSecurity for Nodes в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени Kaspersky Industrial CyberSecurity for Nodes выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Industrial CyberSecurity for Nodes**.

Настройка групповых задач в Kaspersky Security Center

► *Чтобы настроить групповую задачу для нескольких защищаемых компьютеров, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     - В разделе **Область проверки** настройте область проверки.
     - В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
     - В разделе **Настройка** настройте параметры источника обновлений и оптимизации дисковой подсистемы.
     - По кнопке **Настройка параметров соединения** настройте параметры соединения с источником обновлений.
   - Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:
     - Перейдите в раздел **Настройка параметров обновления модулей программы**.
     - Выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.

- Чтобы настроить задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку назначения.
- Чтобы настроить задачу Активация программы, выполните следующие действия:
  - В разделе **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу.
  - Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
- Чтобы настроить задачу автоматического формирования разрешающих правил контроля устройств, в разделе **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.

6. Настройте расписание задачи в разделе **Расписание**. Вы можете настраивать расписание для всех типов задач, кроме задачи Откат обновления баз программы.
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

Настроенные параметры групповых задач будут сохранены.

Настраиваемые параметры групповых задач приведены в следующей таблице.

Таблица 43. Параметры групповых задач Kaspersky Industrial CyberSecurity for Nodes

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Формирование правил контроля запуска программ	**Настройка**	При настройке параметров задачи Формирование правил контроля запуска программ вы можете выбрать способ создания разрешающих правил: • **Создавать разрешающие правила на основе запущенных программ** Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила. Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
		Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил. По умолчанию флажок снят. Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка. **Создавать разрешающие правила для программ из папок**
В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов	**Параметры**	Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ: • **Использовать цифровой сертификат** • **Использовать заголовок и отпечаток цифрового сертификата** • **Если сертификат отсутствует, использовать** • **Использовать хеш SHA256** • **Формировать правила для пользователя или группы пользователей** Вы можете настроить параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задачи.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
выбранных типов, расположенных в указанных папках.	**Расписание**	Вы можете настроить расписание запуска задачи.
Формирование правил контроля устройств	**Настройка**	• Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах. • Настройте параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задачи.
	Расписание	Вы можете настроить расписание запуска задачи.
Активация программы (см. раздел "Задача Активация программы" на стр. 399)	**Параметры активации**	Вы можете применить файл ключа для активации программы или продления срока действия лицензии.
	Расписание	Вы можете настроить расписание запуска задачи.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Копирование обновлений (см. раздел "Задачи обновления" на стр. 400)	**Источник обновлений**	Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Параметры соединения**	В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров копирования обновлений	Вы можете указать состав обновлений для копирования. В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Industrial CyberSecurity for Nodes будет сохранять скопированные обновления.
	Расписание	Вы можете настроить расписание запуска задачи.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Обновление баз программы (см. раздел "Задачи обновления" на стр. 400)	**Настройка**	В блоке параметров **Источник обновлений** можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему: • **Снизить нагрузку на дисковую подсистему** • **Объем оперативной памяти, используемой для оптимизации (МБ)**
	Окно **Параметры соединения**	В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Расписание	Вы можете настроить расписание запуска задачи.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Обновление модулей программы (см. раздел "Задачи обновления" на стр. 400)	**Источник обновлений**	Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Параметры соединения**	В блоке параметров **Параметры соединения с источниками обновлений** можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров обновления модулей программы	Вы можете указать действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Industrial CyberSecurity for Nodes получать информацию о доступных плановых обновлениях.
	Расписание	Вы можете настроить расписание запуска задачи.
Параметры проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 570)	**Область проверки**	Вы можете сформировать область проверки для задачи проверки по требованию и настроить параметры уровня безопасности.
	Окно **Настройка проверки по требованию**	В окне **Настройка проверки по требованию**, доступном из раздела **Область проверки**, вы можете выбрать один из стандартных уровней безопасности или настроить уровень безопасности вручную.

Типы задач Kaspersky Industrial CyberSecurity for Nodes	Раздел в окне Свойства: <Название задачи>	Параметры задачи
	Параметры	В блоке параметров **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка. В блоке **Интеграция с другими компонентами** можно настроить следующие параметры: • применение Доверенной зоны в задачах проверки по требованию; • применение служб KSN в задачах проверки по требованию; • указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.
	Расписание	Вы можете настроить расписание запуска задачи.
Проверка целостности программы (на стр. 402)	**Расписание**	Вы можете настроить расписание запуска задачи.
Мониторинг целостности файлов на основе эталона (см. раздел "Настройка задачи Мониторинг целостности файлов на основе эталона" на стр. 585)	**Расписание**	Вы можете настроить расписание запуска задачи.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**.

Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

kaspersky

В этом разделе

Задача Активация программы

► *Чтобы настроить задачу Активация программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
5. В разделе **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.
9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Задачи обновления

► *Чтобы настроить задачи Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
5. В разделе **Источник обновлений** выполните следующие действия:
   a. Выберите источник обновлений:
      - Сервер администрирования Kaspersky Security Center.
      - Серверы обновлений "Лаборатории Касперского".
      - Другие HTTP-,FTP-серверы и сетевые ресурсы.

      Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).

      Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
   b. Нажмите на кнопку **Настройка параметров соединения**.
   c. В открывшемся окне **Настройка параметров соединения** настройте использование прокси-сервера для подключения к серверам обновлений "Лаборатории Касперского" и другим серверам.
   d. Для задачи Обновление баз программы в разделе **Оптимизация использования дисковой подсистемы** настройте параметры функции, снижающей нагрузку на дисковую подсистему:

      Раздел **Оптимизация использования дисковой подсистемы** доступен только для задачи Обновление баз программы.

- **Снизить нагрузку на дисковую подсистему**

  Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

  Если флажок установлен, функция активна.

  По умолчанию флажок снят.

- **Объем оперативной памяти, используемой для оптимизации (МБ)**

  Объем оперативной памяти (в МБ), используемый программой для хранения файлов обновлений. По умолчанию задан объем 600 МБ. Минимальный объем составляет 400 МБ.

  При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

  - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении). Это приведет к завершению задачи с ошибкой.

    В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

  - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. Функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

    В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

6. Для задачи Обновление модулей программы в разделе **Настройка параметров обновления модулей программы** укажите действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей программы или при наличии информации о плановых обновлениях.

   Можно также настроить действия программы Kaspersky Industrial CyberSecurity for Nodes по завершении установки критических обновлений.

   Раздел **Настройка параметров обновления модулей программы** доступен только для задачи Обновление модулей программы.

7. Для задачи Копирование обновлений в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку, в которую будут сохранены обновления.

   Раздел **Настройка параметров копирования обновлений** доступен только для задачи Копирование обновлений.

8. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

9. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

10. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, контролируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

Проверка целостности программы

► *Чтобы настроить групповую задачу Проверка целостности программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

5. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу Проверка целостности программы.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

   Настроенные параметры групповых задач будут сохранены.

kaspersky

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Industrial CyberSecurity for Nodes возникла проблема (например, аварийное завершение программы), ее можно диагностировать. Для этого можно включить создание файлов трассировки и файла дампа процессов Kaspersky Industrial CyberSecurity for Nodes и отправить эти файлы на анализ в Службу технической поддержки.

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

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 389).
2. Откройте раздел **Диагностика сбоев**.
3. Чтобы отладочная информация записывалась в файл, в разделе **Параметры диагностики сбоев** установите флажок **Включить трассировку**.
4. В поле **Папка файлов трассировки** укажите абсолютный путь к локальной папке, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
5. Настройте уровень детализации отладочной информации.

   В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки. Параметр доступен, если установлен флажок **Включить трассировку**.

   Вы можете выбрать один из следующих режимов работы задачи:

   - **Полная информация** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки всю отладочную информацию.
   - **Краткая информация** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файл трассировки только информацию о критических событиях.

Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

По умолчанию установлен уровень детализации **Полная информация**.

6. Укажите **Максимальный размер файлов трассировки (МБ)**.

   Доступные значения: от 1 до 4095 МБ. По умолчанию максимальный размер файлов трассировки составляет 50 МБ.

7. Для удаления самых старых файлов трассировки при достижении максимального количества файлов установите флажок **Использовать вытеснение старых файлов журнала трассировки**.

8. Укажите значение **Максимальное количество файлов журнала трассировки**.

   Доступные значения: от 1 до 999. По умолчанию максимальное количество файлов составляет 5. Поле доступно, если установлен флажок **Использовать вытеснение старых файлов трассировки**.

9. Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.

10. В поле **Папка файлов дампа** укажите абсолютный путь к локальной папке, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы дампа.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

11. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом компьютере.

Работа с расписанием задач

Вы можете задать расписание для задач Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Плагина управления, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.

4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
      - **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
      - **После обновления баз программы**, если вы 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, дату и время запуска задачи, отобразится расчетное время очередного запуска задачи.
   Перейдите на закладку **Расписание** и откройте окно **Параметры задачи**. В поле **Следующий запуск** в верхней части окна отображается расчетное время запуска. Расчетное время следующего запуска задачи обновляется каждый раз, когда вы открываете окно.
   В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 373) запрещен действующей политикой Kaspersky Security Center.

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

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389)".

Включение и выключение запуска задач 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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.

6. Выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Industrial CyberSecurity for Nodes доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Отчет о статусе компонентов Kaspersky Industrial CyberSecurity for Nodes components

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. Выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 389).
3. Выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

► *Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:*

1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>** .
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых компьютерах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

► *Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 672).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>** .
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах в режиме тестирования** двойным щелчком мыши.

   Будет сформирован отчет.

5. Ознакомьтесь со следующими элементами отчета:
   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 672).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>** .
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

Работа с Консолью Kaspersky Industrial CyberSecurity for Nodes

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

В этом разделе

kaspersky

О Консоли Kaspersky Industrial CyberSecurity for Nodes

Консоль Kaspersky Industrial CyberSecurity for Nodes представляет собой изолированную оснастку, которую можно добавить в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом компьютере или на другом устройстве в сети организации.

После установки Консоли программы на другое устройство требуется дополнительная настройка.

Консоль программы и Kaspersky Industrial CyberSecurity for Nodes можно установить на разных защищаемых устройствах, принадлежащих к разным доменам. В этом случае возможны ограничения при передаче информации от программы в Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Industrial CyberSecurity for Nodes добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Industrial CyberSecurity for Nodes 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 только в Microsoft Management Console 32-разрядной версии. Чтобы добавить оснастку Kaspersky Industrial CyberSecurity for Nodes, откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

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

Интерфейс Консоли Kaspersky Industrial CyberSecurity for Nodes

В этом разделе описаны основные элементы интерфейса программы.

В этом разделе

Окно Консоли Kaspersky Industrial CyberSecurity for Nodes

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

Дерево Консоли

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

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

- **Постоянная защита компьютера**: 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**
  - **Защита от эксплойтов**
- **Контроль компьютера**: контроль программ, запускаемых на защищаемом устройстве, и подключаемых устройств. 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" на стр. 423) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль Kaspersky Industrial CyberSecurity for Nodes.
- **Диагностика системы**: настройка параметров контроля файловых операций и анализа журнала событий Windows.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Защита промышленной сети**получение информации о защищаемых ПЛК и проверка их целостности.
  - **Проверка целостности проектов ПЛК**
  - **Получение данных о проектах ПЛК**

- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка 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" на стр. 423), созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Industrial CyberSecurity for Nodes, а также копирование обновлений в папку локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также последней задачей **Откат обновления баз программы**:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

  В узле отображаются все пользовательские и групповые задачи обновлений (см. раздел "Категории задач Kaspersky Industrial CyberSecurity for Nodes" на стр. 423), сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.
- **Хранилища**: управление параметрами карантина, резервного копирования и списка заблокированных сетевых сеансов.
  - **Карантин**
  - **Резервное хранилище**
  - **Заблокированные сетевые сессии**
- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Industrial CyberSecurity for Nodes.
  - **Журнал событий безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование**: добавление и удаление ключей Kaspersky Industrial CyberSecurity for Nodes, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Industrial CyberSecurity for Nodes**, в панели результатов отобразится информация о текущем состоянии защиты (см. раздел "Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes" на стр. 435) устройства, информация о Kaspersky Industrial CyberSecurity for Nodes, состоянии защиты функциональных компонентов программы и статусе ключа.

Контекстное меню узла Kaspersky Industrial CyberSecurity for Nodes

С помощью пунктов контекстного меню узла **Kaspersky Industrial CyberSecurity for Nodes** можно выполнять следующие операции:

- **Запустить** / **Остановить**. Запустить или остановить (см. раздел "Запуск, приостановка, возобновление, остановка задач вручную" на стр. 424) выполнение задачи. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Подключиться к другому компьютеру**. Подключиться к другому устройству (см. раздел "Управление Kaspersky Industrial CyberSecurity for Nodes через Консоль программы, установленную на другом устройстве" на стр. 416), чтобы управлять установленной на нем программой Kaspersky Industrial CyberSecurity for Nodes. 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 задач вручную" на стр. 424). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настроить проверку съемных дисков**. Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. 562), подключенных к защищаемому устройству по USB.
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны (см. раздел "О доверенной зоне" на стр. 606).
- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.
- **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 и службой Kaspersky Security" на стр. 990).
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел "Экспорт параметров" на стр. 430). 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. 430). 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 и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли Kaspersky Industrial CyberSecurity for Nodes. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Industrial CyberSecurity for Nodes или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

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

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

Панель инструментов и контекстное меню задач Kaspersky Industrial CyberSecurity for Nodes

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

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

- **Возобновить** / **Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел "Запуск, приостановка, возобновление, остановка задач вручную" на стр. 424). 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 и настройка задачи проверки по требованию" на стр. 587). 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. 956). Операция доступна для всех задач.
- **Удалить задачу**. Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Шаблоны параметров**. Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. 431). Операция доступна для задачи Постоянная защита файлов и задач проверки по требованию.

Значок области уведомлений в панели задач

Каждый раз, когда Kaspersky Industrial CyberSecurity for Nodes автоматически запускается после перезагрузки защищаемого устройства, в области уведомлений 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 текущее состояние защиты устройства. Возможно два типа состояния:

 Активный (цветной значок), если работает минимум одна задача: Постоянная защита файлов, Контроль запуска программ.

 Неактивный (серый значок), если не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ.

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 44. Команды контекстного меню, отображаемые с помощью значка области уведомлений

Команда	Описание
Открыть Консоль управления	Открывает Консоль Kaspersky Industrial CyberSecurity for Nodes (если она установлена).
Открыть Диагностическое окно	Открывает Диагностическое окно программы.
О программе	Открывает окно **О программе** с информацией о Kaspersky Industrial CyberSecurity for Nodes. Для зарегистрированных пользователей Kaspersky Industrial CyberSecurity for Nodes 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 области уведомлений,*

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

Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

В общих параметрах Kaspersky Industrial CyberSecurity for Nodes можно включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки защищаемого компьютера.

kaspersky

Управление Kaspersky Industrial CyberSecurity for Nodes через Консоль программы, установленную на другом устройстве

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

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

- Пользователи Консоли программы на удаленном устройстве добавлены в группу KICS Administrators на защищаемом устройстве.
- 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 в окне мастера установки был установлен флажок **Разрешить удаленный доступ**.

Если программа Kaspersky Industrial CyberSecurity for Nodes на удаленном устройстве защищена паролем, введите пароль для получения доступа к управлению программой с помощью Консоли программы.

Настройка общих параметров программы в Консоли программы

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

Настройка параметров программы недоступна из Консоли программы, если изменение данных параметров запрещено активной политикой Kaspersky Security Center.

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

1. В дереве Консоли программы 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 Kaspersky Industrial CyberSecurity for Nodes согласно вашим требованиям:
   - На закладке **Масштабируемость и интерфейс** можно настроить следующие параметры:
     - В разделе **Параметры масштабируемости**:
       - Количество процессов для постоянной защиты компьютера

Таблица 45. Количество процессов для постоянной защиты

<table>
<tr><th>Параметр</th><th>Количество процессов для постоянной защиты</th></tr>
<tr><td>Описание</td><td>Этот параметр относится к группе Параметры масштабируемости Kaspersky Industrial CyberSecurity for Nodes.
С помощью этого параметра можно задать фиксированное количество процессов, в которых Kaspersky Industrial CyberSecurity for Nodes будет выполнять задачи постоянной защиты компьютера.
Более высокое значение повысит скорость проверки объектов в задачах постоянной защиты компьютера. Однако, чем больше процессов задействует Kaspersky Industrial CyberSecurity for Nodes, тем больше будет влияние на общую производительность защищаемого устройства и потребление оперативной памяти.
В Консоли администрирования Kaspersky Security Center параметр Количество процессов для постоянной защиты можно настроить только для программы Kaspersky Industrial CyberSecurity for Nodes, установленной на отдельном защищаемом устройстве (в окне Параметры программы). Нельзя изменить этот параметр в свойствах политики для группы защищаемых устройств.</td></tr>
<tr><td>Возможные значения</td><td>Возможные значения: 1-8.
Большее значение позволяет снизить влияние Kaspersky Industrial CyberSecurity for Nodes на скорость обмена данными между устройствами и защищаемым компьютером. Таким образом повысится быстродействие задачи постоянной защиты компьютеров. Однако задачи обновления и задачи проверки по требованию с приоритетом Средний будут выполняться в уже запущенных рабочих процессах Kaspersky Industrial CyberSecurity for Nodes. 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 приоритетом Низкий всегда выполняются в отдельных процессах.</td></tr>
<tr><td>Значение по умолчанию</td><td>Kaspersky Industrial CyberSecurity for Nodes выполняет масштабирование автоматически в зависимости от количества процессоров защищаемого устройства:
<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 46. 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. С помощью этого параметра можно указать максимальное количество процессов, для которых программа будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, определяемое этим параметром, не входит в общее количество процессов Kaspersky Industrial CyberSecurity for Nodes, заданное параметром Количество процессов для постоянной защиты сервера. Например, если вы установите следующие значения: • количество процессов для задач постоянной защиты компьютера – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты компьютера и одну задачу проверки по требованию в фоновом режиме, общее количество процессов kavfswp.exe для 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 разделе **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач при каждом запуске программы (см. раздел "Значок области уведомлений в панели задач" на стр. 414).
- На закладке **Безопасность и надежность** можно настроить следующие параметры:
  - В разделе **Самозащита** настройте защиту процессов программы.

Если функция **Защищать процессы программы от внешних угроз** включена, программа защищает процессы от внедрения кода и доступа к данным процессов.

При включении или выключении этой функции нет необходимости перезапускать службы программы, чтобы изменения вступили в силу.

Функция включена по умолчанию.

  - В разделе **Самозащита** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля" на стр. 992).
  - В разделе **Параметры применения пароля** укажите количество попыток восстановления задачи проверки по требованию после ее аварийного завершения.

Таблица 47. Восстановление задач

Параметр	Выполнять восстановление задач
Описание	Этот параметр относится к группе **Параметры применения пароля** Kaspersky Industrial CyberSecurity for Nodes. Он включает восстановление задач в случае их аварийного завершения 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, программа не восстанавливает задачи постоянной защиты компьютера и проверки по требованию. Если включено восстановление задач, программа пытается восстановить задачи постоянной защиты компьютера, до тех пор, пока они не будут успешно запущены. Также программа 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 разделе **Выполнять восстановление задач проверки по требованию не более (раз)** укажите действия Kaspersky Industrial CyberSecurity for Nodes при переходе на источник бесперебойного питания.

Таблица 48. Использование источника бесперебойного питания

Параметр	Выполнять восстановление задач проверки по требованию не более (раз)
Описание	Этот параметр определяет действия, которые Kaspersky Industrial CyberSecurity for Nodes выполняет, когда защищаемое устройство переходит на работу 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 защищаемого устройства от источника бесперебойного питания Kaspersky Industrial CyberSecurity for Nodes работает в следующем режиме: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию; • автоматически останавливает все выполняемые задачи проверки по требованию.

- На закладке **Настройки сканирования**:
  - **Восстанавливать атрибуты файлов после сканирования**

Когда Kaspersky Industrial CyberSecurity for Nodes выполняет задачи проверки по требованию, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Industrial CyberSecurity for Nodes возвращает исходное значение времени последнего обращения к файлу.

Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.

По умолчанию эта опция включена.

- **Ограничивать сканирующий поток в использовании CPU**

Kaspersky Industrial CyberSecurity for Nodes ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)** .

Включение этой опции может негативно сказаться на производительности Kaspersky Industrial CyberSecurity for Nodes.

По умолчанию эта опция выключена.

- **Предельное значение (в процентах)**

Максимально допустимое значение загрузки процессора программой Kaspersky Industrial CyberSecurity for Nodes.

Это поле доступно, если выбран параметр **Ограничивать сканирующий поток в использовании CPU**.

- **Папка для временных файлов, создаваемых при сканировании**

Папка, в которую программа Kaspersky Industrial CyberSecurity for Nodes распаковывает файлы архивов при проверке.

По умолчанию используется папка C:\Windows\Temp.

- На закладке **Параметры соединения**:
  - В разделе **Параметры прокси-сервера** укажите параметры прокси-сервера.
  - В разделе **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и данные, необходимые для аутентификации на прокси-сервере.
  - В разделе **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 **Включить трассировку**.
    - В поле ниже укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 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 сохраняет в файле трассировки.

      Вы можете выбрать один из следующих уровней детализации:

      - **Критические события** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки только информацию о критических событиях.
      - **Ошибки** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки информацию о критических событиях и ошибках.

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

Уровень детализации, требуемый для решения возникших проблем, определяет специалист Службы технической поддержки.

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

Раскрывающийся список доступен, если установлен флажок **Включить трассировку**.

- Укажите максимальный размер файлов трассировки.
- Укажите максимальное количество файлов в одном журнале трассировки. Kaspersky Industrial CyberSecurity for Nodes создает не более указанного максимального количества файлов трассировки для каждого отлаживаемого компонента.
- Укажите компоненты для отладки.

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

Таблица 49. Коды подсистем Kaspersky Industrial CyberSecurity for Nodes

Код подсистемы	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 (gui) и Плагина управления Kaspersky Industrial CyberSecurity for Nodes 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 применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes сохраняет отладочную информацию о работе всех компонентов Kaspersky Industrial CyberSecurity for Nodes.

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

- Если вы хотите, чтобы программа создавала файл дампа, установите флажок **Создавать файл дампа**.

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

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

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Industrial CyberSecurity for Nodes будут сохранены.

Управление задачами Kaspersky Industrial CyberSecurity for Nodes

В этом разделе приведена информация о создании, настройке, запуске и остановке задач Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

Категории задач Kaspersky Industrial CyberSecurity for Nodes

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

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли программы, 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: *локальные* и *групповые*.

Локальные задачи

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

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

Групповые задачи

Групповыми задачами и задачами для наборов защищаемых устройств можно управлять из Kaspersky Security Center. Все групповые задачи являются пользовательскими. Групповые задачи также отображаются в Консоли программы. В Консоли программы можно только просматривать состояние групповых задач. С помощью Консоли программы нельзя управлять или настраивать групповые задачи.

Запуск, приостановка, возобновление, остановка задач вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты компьютера и проверки по требованию. Никакие другие задачи нельзя приостановить или возобновить вручную.

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

1. В дереве Консоли программы откройте контекстное меню задачи.
2. Выберите одну из следующих команд: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 953).

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

Работа с расписанием задач

Вы можете задать расписание для задач Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

kaspersky

Настройка параметров расписания задач

В Консоли программы можно настроить расписание запуска локальных системных и пользовательских задач. Однако настроить расписание запуска групповых задач нельзя.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, для которой требуется настроить расписание.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Выполните следующие действия, чтобы настроить расписание:
   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась с периодичностью в заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, чтобы задача запускалась с периодичностью в заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, чтобы задача запускалась с периодичностью в заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
      - **После обновления баз программы**, 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 первого запуска задачи.

   После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
   В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию запрещен действующей политикой Kaspersky Security Center.
5. На закладке **Дополнительно** настройте следующие параметры расписания:
   - В разделе **Параметры остановки задачи**:
     a. Установите флажок **Длительность**. В полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с**. В полях справа укажите, когда требуется приостановить и возобновить выполнение задачи (в рамках 24 часов).

- В блоке **Дополнительные параметры**:
  a. Установите флажок **Отменить с** и укажите дату прекращения действия расписания.
  b. Установите флажок **Запускать пропущенные задачи**, чтобы запускать пропущенные задачи.
  c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **OK**.

Параметры расписания задачи будут сохранены.

Включение и выключение запуска задач по расписанию

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

► *Чтобы включить или выключить запуск задачи по расписанию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню настраиваемой задачи.
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**, чтобы включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, чтобы выключить запуск задачи по расписанию.

     Параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
4. Нажмите на кнопку **OK**.

Параметры расписания задачи 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

kaspersky

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись для запуска следующих задач Kaspersky Industrial CyberSecurity for Nodes:

- Формирование правил контроля запуска программ
- Формирование правил контроля устройств
- Проверка по требованию
- Обновление

По умолчанию указанные задачи выполняются с правами системной учетной записи.

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

- Для задачи **Обновление**: если в качестве источника обновления указана папка общего доступа на другом устройстве в сети.
- Для задачи **Обновление**: если для доступа к источнику обновлений используется прокси-сервер со встроенной в Windows проверкой подлинности NTLM.
- Для задач **Проверка по требованию**: если системная учетная запись не обладает правами доступа к проверяемым объектам (например, к файлам в папках общего доступа на защищаемом устройстве).
- Для задачи **Формирование правил контроля запуска программ**: если сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, находящийся в папке общего доступа на защищаемом устройстве).

Вы можете запускать 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 обращается к папкам общего доступа на другом устройстве в сети, если это устройство зарегистрировано в то же домене, что и защищаемый компьютер. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Industrial CyberSecurity for Nodes обращается к устройству с правами учетной записи **<имя домена \ имя устройства>**.

Указание учетной записи для запуска задачи

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

1. В дереве Консоли программы откройте контекстное меню задачи, которую вы хотите запустить с правами определенной учетной записи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.

3. В открывшемся окне на закладке **Запуск с правами** выполните следующие действия:
   a. Выберите вариант **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 пароль.
4. Нажмите на кнопку **OK**.

Изменения параметров задачи будут сохранены.

Импорт и экспорт параметров

В этом разделе приведена информация об экспорте параметров Kaspersky Industrial CyberSecurity for Nodes. Также описан экспорт параметров определенных программных компонентов в конфигурационный файл в формате XML и импорт этих параметров из конфигурационного файла в программу.

В этом разделе

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Industrial CyberSecurity for Nodes в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Industrial CyberSecurity for Nodes 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, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Industrial CyberSecurity for Nodes:

- Постоянная защита файлов
- Использование KSN
- Контроль устройств
- Контроль запуска программ
- Формирование правил контроля устройств
- Формирование правил контроля запуска программ
- Проверка по требованию
- Проверка целостности проектов ПЛК
- Получение данных о проектах ПЛК

- Контроль Wi-Fi
- Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes
- Карантин
- Резервное хранилище
- Журналы
- Уведомления администратора и пользователей
- Доверенная зона
- Защита от эксплойтов
- Список заблокированных сетевых сеансов
- Защита паролем

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

Вы не можете экспортировать параметры групповых задач.

Kaspersky Industrial CyberSecurity for Nodes 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. Пароли можно импортировать только с помощью программы Kaspersky Industrial CyberSecurity for Nodes, установленной на этом же защищаемом компьютере, если она не была переустановлена или обновлена.

Нельзя импортировать ранее сохраненные пароли с помощью программы Kaspersky Industrial CyberSecurity for Nodes, установленной на другом защищаемом устройстве. После импорта параметров на защищаемом устройстве 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 (например, созданного в программе Kaspersky Industrial CyberSecurity for Nodes, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Industrial CyberSecurity for Nodes 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 программы 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.
   - В контекстном меню требуемой задачи выберите пункт **Экспортировать параметры**, чтобы экспортировать параметры отдельного функционального компонента программы.
   - Чтобы экспортировать параметры доверенной зоны, выполните следующие действия:
     a. В дереве Консоли программы 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 мастера экспорта параметров.
2. Выполните инструкции, которые предлагает **Мастер экспорта параметров программы**: задайте имя и путь конфигурационного файла, в который вы хотите сохранить параметры.

   При указании пути можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя.

   > Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует параметры, используемые в политике.

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

Мастер экспорта параметров будет закрыт; экспортированные параметры будут сохранены.

Импорт параметров

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

1. В дереве Консоли программы 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.
   - В контекстном меню требуемой задачи выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента программы.

- Чтобы импортировать параметры доверенной зоны, выполните следующие действия:

  a. В дереве Консоли программы 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 мастера импорта параметров.

2. Выполните инструкции, которые предлагает **Мастер импорта параметров программы**: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После импорта общих параметров или параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes на защищаемый компьютер, восстановить их прежние значения невозможно.

3. В окне **Закрыть** нажмите на кнопку **Импорт параметров программы завершен**.

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.

4. В панели инструментов Консоли программы нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли программы.

Kaspersky Industrial CyberSecurity for Nodes не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом защищаемом компьютере или на этом же защищаемом компьютере, после того как на нем была переустановлена или обновлена программа Kaspersky Industrial CyberSecurity for Nodes. После завершения импорта пароли необходимо ввести 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.

В этом разделе

kaspersky

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства 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:

- Постоянная защита файлов
- Проверка при старте операционной системы
- Проверка важных областей
- Задачи проверки по требованию

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов защищаемого устройства, распространяются 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. 433).
- Если вложенные узлы виртуальные. В этом случае необходимо применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите создать шаблон параметров безопасности.
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 защищаемого 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 дополнительное описание шаблона.
7. Нажмите на кнопку **ОК**.

Шаблон параметров безопасности сохранен.

Просмотр параметров безопасности в шаблоне

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите просмотреть шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

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

Откроется окно **<Название шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне. На закладке **Параметры** приведен список параметров безопасности, сохраненных в шаблоне.

Применение шаблона параметров безопасности

► *Чтобы применить параметры безопасности из шаблона к выбранному узлу, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
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 защищаемого компьютера откройте контекстное меню узла или элемента, к которому вы хотите применить шаблон.
4. Выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов защищаемого компьютера. Значение на закладке **Уровень безопасности** для выбранного узла изменится на **Другой**.

Если значения параметры безопасности из шаблона применяются к родительскому узлу в дереве файловых ресурсов защищаемого компьютера, эти параметры распространяются на все вложенные узлы.

Можно настроить область защиты или область проверки вложенных узлов в дереве файловых ресурсов защищаемого устройства отдельно. В этом случае параметры безопасности из шаблона, примененного к родительскому узлу, не применяются автоматически к вложенным узлам.

► *Чтобы применить параметры безопасности из шаблона ко всем выбранным узлам, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
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 защищаемого компьютера выберите родительский узел, чтобы применить шаблон к этому узлу и к его вложенным узлам.
4. В контекстном меню выберите пункт **Применить шаблон → <Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов защищаемого компьютера. Значение на закладке **Уровень безопасности** для выбранного узла изменится на **Другой**.

Удаление шаблона параметров безопасности

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите удалить шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.

   Вы можете просмотреть шаблоны параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.
3. В списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

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

Выбранный шаблон будет удален.

Шаблон параметров безопасности можно применить для защиты или проверки узлов в дереве файловых ресурсов защищаемого компьютера. В этом случае настроенные для этих узлов параметры безопасности сохраняются после удаления шаблона.

kaspersky

Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes

► *Чтобы просмотреть информацию о состоянии защиты устройства в Kaspersky Industrial CyberSecurity for Nodes,*

выберите узел **Kaspersky Industrial CyberSecurity for Nodes** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes.

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

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

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле **Kaspersky Industrial CyberSecurity for Nodes**,*

в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Обновить**.

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

- статус использования Kaspersky Security Network;
- состояние защиты устройства;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля защищаемого компьютера;
- данные о лицензии;
- статус защиты промышленной сети;
- статус интеграции с Kaspersky Security Center: данные сервера с установленной программой Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В разделе **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *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.

Защита компьютера

В разделе **Защита компьютера** (см. таблицу ниже) отображается информация о текущем состоянии защиты устройства.

Таблица 50. Информация о состоянии защиты устройства

Раздел Защита	Информация
Индикатор состояния защиты устройства	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется. • Желтый цвет панели означает, что компонент Постоянная защита файлов не установлен и задача Проверка важных областей давно не выполнялась. • Красный цвет панели – задачи постоянной защиты файлов не выполняются.
Постоянная защита файлов	**Статус задачи** – текущее состояние задачи, например, Выполняется или Остановлена. **Обнаружено** – количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes. Например, если программа Kaspersky Industrial CyberSecurity for Nodes 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 проводилась* – 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: **Активный** или **Только статистика**. **Сетевых сессий заблокировано** – количество сетевых сеансов, которые продемонстрировали потенциально опасную активность и были заблокированы при попытке подключения к защищаемому компьютеру.
Объектов в резервном хранилище	*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 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 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.

Обновление

В разделе **Обновление** (см. таблицу ниже) отображается информация об актуальности баз и модулей программы.

Таблица 51. Информация о состоянии баз и модулей Kaspersky Industrial CyberSecurity for Nodes

Раздел Обновление	**Информация**
Индикатор состояния баз и модулей программы	Цвет панели с названием раздела 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 показывает, что 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 были обновлены не более чем 7 дней назад (по умолчанию). • **Базы программы устарели** – базы программы были обновлены от 7 до 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 обновления баз программы. Дата и время указаны в UTC-формате. **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, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Industrial CyberSecurity for Nodes.

Контроль

В разделе **Контроль** (см. таблицу ниже) отображается информация о задачах Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

Таблица 52. Информация о состоянии контроля защищаемого устройства

Раздел Контроль	**Информация**
Индикатор состояния контроля защищаемого устройства	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в активном режиме; компонент Защита от эксплойтов установлен и активен. • Желтый цвет панели отображается при наличии одного или нескольких из следующих условий: Защита от эксплойтов не запущена; Задача Контроль запуска программ запущена в режиме 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: **Активный** или **Только статистика**. **Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Industrial CyberSecurity for Nodes 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 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** или **Только статистика**. **Процессов защищено** – общее количество процессов, которые находятся под защитой и обрабатываются в соответствие с выбранным режимом.
Контроль устройств	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Контроль устройств: **Активный** или **Только статистика**. **Заблокировано устройств** – количество попыток подключений внешних устройств, заблокированных Kaspersky Industrial CyberSecurity for Nodes в ходе выполнения задачи Контроль устройств. Если количество заблокированных внешних устройств превышает 0, значение поля окрашивается в красный цвет.

Раздел Контроль	**Информация**
Управление сетевым экраном	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Заблокировано попыток подключения** – количество подключений к защищаемому компьютеру, которые были заблокированы 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.

Диагностика

В разделе **Диагностика** (см. таблицу ниже) отображается информация о задачах Мониторинг файловых операций и Анализ журналов.

Таблица 53. Информация о состоянии диагностики системы

Раздел Диагностика	**Информация**
Индикатор статуса диагностики	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задача выполняется. • Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие *Не выполняется*. • Красный – одна из задач завершена с ошибкой.
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированных файловых операций** – 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*. **Нарушения настроенных правил** – количество зафиксированных нарушений по данным журнала событий Windows, выявленных на основе заданных правил задачи или применения эвристического анализатора.

Закладка Защита индустриальной сети

В разделе **ПЛК в области защиты** отображается информация о списке ПЛК, включенных в область защиты.

Таблица 54. Информация о получении данных о ПЛК

Раздел ПЛК в области защиты	**Информация**
Индикатор статуса области защиты ПЛК	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет означает, что задача была успешно завершена минимум один раз. • Желтый цвет означает, что проверка ни разу не выполнялась. • Красный цвет означает, что задача завершена с ошибкой.
Получение данных о проекте ПЛК	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **ПЛК в списке** – количество ПЛК в области защиты.

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

Таблица 55. Информация о проверке целостности проектов ПЛК

Раздел Целостность проектов ПЛК	**Информация**
Индикатор статуса целостности ПЛК	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет означает, что задача была успешно завершена минимум один раз. • Желтый цвет означает, что проверка целостности ни разу не выполнялась. • Красный цвет означает, что задача завершена с ошибкой.
Проверка целостности проектов ПЛК	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **ПЛК в активной области защиты** – количество ПЛК в области защиты. **Нарушений целостности** – количество обнаруженных нарушений.

Информация о лицензии Kaspersky Industrial CyberSecurity for Nodes отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes**.

Вы можете настроить свойства Kaspersky Industrial CyberSecurity for Nodes, перейдя по ссылке Свойства программы (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 416).

Вы можете подключиться к другому защищаемому устройству, перейдя по ссылке Подключиться к другому компьютеру (см. раздел "Управление Kaspersky Industrial CyberSecurity for Nodes через Консоль программы, установленную на другом устройстве" на стр. 416).

kaspersky

Работа с Веб-плагином из Веб-консоли

Этот раздел содержит информацию о Плагине управления Kaspersky Industrial CyberSecurity for Nodes и об управлении программой, установленной на защищаемом компьютере или группе защищаемых компьютеров.

В этом разделе

Управление Kaspersky Industrial CyberSecurity for Nodes из Веб-консоли

Вы можете централизованно управлять несколькими защищаемыми компьютерами с установленной программой Kaspersky Industrial CyberSecurity for Nodes, объединенными в группу администрирования, с помощью Веб-плагина Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Security Center Web также позволяет отдельно настраивать параметры каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center Web Console. Группа администрирования включает устройства с установленной программой Kaspersky Industrial CyberSecurity for Nodes, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого компьютера недоступны для настройки, если работа Kaspersky Industrial CyberSecurity for Nodes на этом защищаемом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center Web Console следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне свойств устройства в Kaspersky Security Center Web Console. С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, и параметры запуска локальных системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств. С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых компьютеров, не входящих ни в одну группу администрирования.
- **С помощью окна свойств отдельного устройства**. В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры программы, так и параметры всех задач Kaspersky Industrial CyberSecurity for Nodes, если выбранный защищаемый компьютер не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых компьютеров, так и для отдельного защищаемого компьютера.

Ограничения Веб-плагина

Веб-плагин Kaspersky Industrial CyberSecurity for Nodes имеет следующие ограничения по сравнению с Плагином управления Kaspersky Industrial CyberSecurity for Nodes:

- Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
- Для задачи Постоянная защита файлов нельзя изменить стандартный уровень безопасности.
- Для задачи Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.
- Для задачи Контроль устройств нельзя сформировать правила на основе подключенных устройств или данных системы.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Security Center Web Console.

В этом разделе

kaspersky

Настройка общих параметров программы с помощью Веб-плагина

С помощью Веб-плагина можно настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes для группы защищаемых компьютеров или для отдельного защищаемого компьютера.

В этом разделе

Настройка параметров масштабируемости, интерфейса и проверки с помощью Веб-плагина

► *Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Масштабируемость, интерфейс, настройки сканирования**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 56. Параметры масштабируемости

Параметр	Описание
Определять параметры масштабируемости автоматически	Kaspersky Industrial CyberSecurity for Nodes автоматически регулирует количество используемых процессов. Это значение установлено по умолчанию.
Указать количество рабочих процессов вручную	Kaspersky Industrial CyberSecurity for Nodes контролирует количество активных рабочих процессов в соответствии с указанными значениями.
Количество процессов для постоянной защиты	Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
Количество процессов для фоновых задач проверки по требованию	Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
Показывать значок в панели задач	Настройте, будет ли Значок области уведомлений отображаться в панели задач.
Восстанавливать атрибуты файлов после сканирования	Когда Kaspersky Industrial CyberSecurity for Nodes выполняет задачи проверки по требованию, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Industrial CyberSecurity for Nodes возвращает исходное значение времени последнего обращения к файлу. Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов. По умолчанию эта опция включена.
Ограничивать сканирующий поток в использовании CPU	Kaspersky Industrial CyberSecurity for Nodes ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)** . Включение этой опции может негативно сказаться на производительности Kaspersky Industrial CyberSecurity for Nodes. По умолчанию эта опция выключена.
Предельное значение (в процентах)	Максимально допустимое значение загрузки процессора программой Kaspersky Industrial CyberSecurity for Nodes. Это поле доступно, если выбран параметр **Ограничивать сканирующий поток в использовании CPU**.
Папка для временных файлов, создаваемых при сканировании	Папка, в которую программа Kaspersky Industrial CyberSecurity for Nodes распаковывает файлы архивов при проверке. По умолчанию используется папка C:\Windows\Temp.
Параметры HSM-системы	Выберите тип доступа к иерархическому хранилищу.

Настройка параметров безопасности с помощью Веб-плагина

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Безопасность и надежность**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 57. Параметры безопасности

Параметр	Описание
Защищать процессы программы от внешних угроз	Если функция **Защищать процессы программы от внешних угроз** включена, программа защищает процессы от внедрения кода и доступа к данным процессов. При включении или выключении этой функции нет необходимости перезапускать службы программы, чтобы изменения вступили в силу. Функция включена по умолчанию.
Выполнять восстановление задач	Флажок включает или выключает восстановление задач Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes автоматически восстанавливает задачи Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не восстанавливает задачи Kaspersky Industrial CyberSecurity for Nodes после сбоя в работе программы или аварийного завершения работы программы. По умолчанию флажок установлен.
Выполнять восстановление задач проверки по требованию не более (раз), значение в диапазоне от 1 до 10	Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Industrial CyberSecurity for Nodes. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.
Не запускать задачи проверки по расписанию	Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого компьютера на источник бесперебойного питания до восстановления стандартного режима питания. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes не запускает задачи проверки по расписанию при переходе защищаемого компьютера на источник бесперебойного питания до восстановления стандартного режима питания. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes запускает задачи проверки по расписанию вне зависимости от режима питания. По умолчанию флажок установлен.

Параметр	Описание
Остановить выполняемые задачи проверки	Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого компьютера на источник бесперебойного питания. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes останавливает выполнение запущенных задач проверки при переходе защищаемого компьютера на источник бесперебойного питания. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes продолжает выполнение запущенных задач проверки при переходе защищаемого компьютера на источник бесперебойного питания. По умолчанию флажок установлен.
Использовать защиту паролем	Установить пароль для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.

Настройка параметров соединения с помощью Веб-плагина

Настроенные параметры соединения используются для подключения Kaspersky Industrial CyberSecurity for Nodes к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Масштабируемость, интерфейс, настройки сканирования**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 58. Параметры соединения

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, для соединения с KSN Kaspersky Industrial CyberSecurity for Nodes использует параметры прокси-сервера, указанные вручную.
Не использовать прокси-сервер для локальных адресов	Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Industrial CyberSecurity for Nodes. Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Industrial CyberSecurity for Nodes, происходит напрямую. Прокси-сервер не используется. Если флажок снят, для подключения к локальным устройствам используется прокси-сервер. По умолчанию флажок установлен.
Параметры аутентификации на прокси-сервере	Укажите параметры аутентификации
Не использовать аутентификацию	Проверка подлинности не выполняется. Этот режим выбран по умолчанию.
Использовать NTLM-аутентификацию	Проверка подлинности выполняться с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
Использовать NTLM-аутентификацию с именем пользователя и паролем	Проверка подлинности выполняется по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
Использовать имя пользователя и пароль	Проверка подлинности выполняется с помощью имени пользователя и пароля.

kaspersky

Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления. Запуск осуществляется по расписанию, настроенному локально на каждом защищаемом компьютере группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом компьютере по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Industrial CyberSecurity for Nodes будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если защищаемый компьютер исключен из группы администрирования, расписание локальных системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию локальных системных задач Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Запуск локальных системных задач**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 59. Параметры запуска локальных системных задач по расписанию

Параметр	Описание
Разрешить запуск задач проверки по требованию	Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач проверки по требованию.
Разрешить запуск задач обновления и копирования обновлений	Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач обновления и копирования обновлений.

Настройка параметров карантина и резервного хранилища с помощью Веб-плагина

Чтобы настроить общие параметры карантина и резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Параметры** в подразделе **Хранилища**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 60. Параметры карантина и резервного хранилища

Параметр	Описание
Папка резервного хранилища	Укажите папку резервного хранилища.
Максимальный размер резервного хранилища (МБ)	Укажите максимальный размер резервного хранилища.
Порог доступного пространства (МБ)	Укажите минимальное значение свободного места в папке резервного хранилища.
Папка, в которую восстанавливаются объекты	Укажите папку для восстановленных объектов.
Папка карантина	Укажите папку резервного хранилища.

Параметр	Описание
Максимальный размер карантина (МБ)	Укажите максимальный размер резервного хранилища.
Порог доступного пространства (МБ)	Укажите минимальное значение свободного места в папке резервного хранилища.
Папка, в которую восстанавливаются объекты	Укажите папку для восстановленных объектов.
Условия блокировки сетевых сессий	Укажите количество суток, часов и минут, по истечении которых заблокированные сетевые сеансы получат доступ к сетевым файловым ресурсам.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Industrial CyberSecurity for Nodes на нескольких защищаемых компьютерах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Industrial CyberSecurity for Nodes на всех защищаемых компьютерах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *активная* в Консоли администрирования.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Industrial CyberSecurity for Nodes. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых компьютерах: *Запретить изменение параметров*. После применения политики Kaspersky Industrial CyberSecurity for Nodes использует на защищаемых компьютерах параметры, для которых в свойствах политики вы установили значок . В этом случае выбранные параметры используются вместо параметров, действовавших до применения политики. Kaspersky Industrial CyberSecurity for Nodes не применяет параметры активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого компьютера.

Параметры, настроенные и переданные на защищаемый компьютер с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры для любой задачи постоянной защиты компьютера, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

В этом разделе

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Нажмите на кнопку **Добавить**.
3. Откроется окно **Новая политика**.
4. В разделе **Выбор программы** выберите Kaspersky Industrial CyberSecurity for Nodes и нажмите на кнопку **Далее**.
5. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.

     Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`
   - Выбрать статус политики:
     - **Активный**. После следующей синхронизации политика будет использоваться на компьютере в качестве активной политики.
     - **Неактивный**. Резервная политика. При необходимости можно перевести неактивную политику в активный статус.
     - **Для автономных пользователей**. Эта политика активируется, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если включен этот переключатель, значения параметров политики наследуются из политики верхнего уровня. Параметры политики недоступны для изменения, если для родительской политики установлен .

- **Принудительное наследование параметров в дочерних политиках**. Если переключатель включен, значения параметров политики распространяются на дочерние политики. В параметрах дочерней политики автоматически устанавливается флажок **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, за исключением параметров, отмеченных . Параметры дочерней политики недоступны для изменения, если для родительской политики установлен .

6. На закладке **Параметры программы** настройте параметры политики в соответствии с вашими требованиями.
7. Нажмите на кнопку **Сохранить**.

Созданная политика отобразится в списке политик на закладке **Политики и профили** выбранной группы администрирования. В окне **<Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Industrial CyberSecurity for Nodes.

Разделы параметров политики Kaspersky Industrial CyberSecurity for Nodes

Общие

В разделе **Общие** можно настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров для родительских и дочерних политик.

Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** можно настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

Таблица 61. Параметры активации программы

Раздел	Параметры
Масштабируемость, интерфейс, настройки сканирования	В подразделе **Масштабируемость, интерфейс, настройки сканирования** по кнопке **Параметры** вы можете настроить следующие параметры: • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
Безопасность и надежность	В подразделе **Безопасность и надежность** по кнопке **Параметры** вы можете настроить следующие параметры: • настроить параметры запуска задачи; • указать действия программы при переходе защищаемого компьютера на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.

Раздел	Параметры
Параметры соединения	В подразделе **Параметры соединения** по кнопке **Параметры** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск локальных системных задач	В подразделе **Запуск локальных системных задач** по кнопке **Параметры** можно разрешить или запретить запуск следующих локальных системных задач по расписанию, настроенному на защищаемых устройствах: • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Таблица 62. Дополнительные параметры

Раздел	Параметры
Доверенная зона	В подразделе **Параметры** по кнопке **Доверенная зона** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных дисков	В подразделе **Проверка съемных дисков** по кнопке **Параметры** вы можете настроить параметры проверки съемных дисков.
Права пользователей на управление программой	В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Industrial CyberSecurity for Nodes.

Раздел	Параметры
Права пользователей на управление службой Kaspersky Security Service	В подразделе **Права пользователей на управление службой Kaspersky Security Service** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.
Хранилища	В подразделе **Хранилища** по кнопке **Параметры** можно настроить следующие параметры карантина, резервного хранилища и заблокированных сетевых сеансов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить передачу информации об объектах карантина и резервного хранилища на Сервер администрирования; • настроить продолжительность блокировки сетевых сеансов.

Постоянная защита компьютера

Таблица 63. Параметры постоянной защиты сервера

Раздел	Параметры
Постоянная защита файлов	В подразделе **Постоянная защита файлов** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную; • настроить параметры запуска задачи.
Использование KSN	В подразделе **Использование KSN** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • указать действия над объектами, недоверенными в KSN; • настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.
Защита трафика	В подразделе **Защита трафика** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • Настройте режим работы задачи. • Настройте антивирусную защиту. • Включите защиту от почтовых угроз, антифишинговую проверку и проверку веб-адресов.

Раздел	Параметры
Защита от эксплойтов	В подразделе **Защита от эксплойтов** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.
AMSI-защита	В подразделе **AMSI-защита** по кнопке **Параметры** вы можете настроить следующие параметры запуска задач: • разрешить или запретить исполнение предположительно опасных скриптов; • настроить использование эвристического анализатора; • настроить применение доверенной зоны; • настроить параметры запуска задачи;

Контроль активности на компьютерах

Таблица 64. Параметры контроля активности на компьютерах

Раздел	Параметры
Контроль запуска программ	В подразделе **Контроль запуска программ** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • настроить параметры запуска задачи.
Контроль устройств	В подразделе **Контроль устройств** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры запуска задачи.

Контроль активности в сети

Таблица 65. Параметры контроля активности в сети

Раздел	Параметры
Управление сетевым экраном	В подразделе **Управление сетевым экраном** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • настроить правила сетевого экрана; • настроить параметры запуска задачи.

Раздел	Параметры
Защита от шифрования	В подразделе **Защита от шифрования** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • настроить область защиты от вредоносного шифрования; • настроить параметры запуска задачи.

Диагностика системы

Таблица 66. Параметры диагностики системы

Раздел	Параметры
Мониторинг файловых операций	В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере.
Анализ журналов	В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого компьютера на основе результатов анализа журнала событий Windows.

Журналы и уведомления

Таблица 67. Параметры журналов и уведомлений

Раздел	Параметры
Журналы выполнения задач	В подразделе **Журналы выполнения задач** по кнопке **Параметры** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач. • указать параметры интеграции SIEM-системы с Kaspersky Security Center.
Уведомления о событиях	В подразделе **Уведомления о событиях** по кнопке **Параметры** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и заблокировано недоверенное запоминающее устройство* и *Недоверенный узел в списке*; • указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В подразделе **Взаимодействие с Сервером администрирования** по кнопке **Параметры** вы можете выбрать типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования.

Подробная информация о задачах Защиты сетевых хранилищ приведена в документе *Руководство по внедрению Kaspersky Industrial CyberSecurity for Nodes для защиты сетевых хранилищ*.

Диагностика сбоев

Таблица 68. Параметры диагностики сбоев

Раздел	Параметры
Параметры диагностики сбоев	В разделе **Параметры диагностики сбоев** можно настроить следующие параметры: • включить и выключить трассировку; • задать папку файлов трассировки; • указать уровень детализации; • указать максимальный размер файлов трассировки; • удалить самые старые файлы трассировки; • указать максимальное количество файлов в журнале трассировки. Подробнее о параметрах и их ограничениях см. в описании конфигурации локальных параметров (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 416). Вы можете установить разные значения параметров на локальном устройстве и в групповой политике для нескольких устройств. Локальные настройки наследуют параметры групповой политики, настроенные на сервере Kaspersky Security Center.
Параметры файла дампа	В разделе **Параметры файла дампа** можно настроить следующие параметры: • создать файл дампа; • указать папку файла дампа. Подробнее о параметрах и их ограничениях см. в описании конфигурации локальных параметров (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 416). Вы можете установить разные значения параметров на локальном устройстве и в групповой политике для нескольких устройств. Значения локальных параметров наследуют значения параметров групповой политики, указанные на сервере Kaspersky Security Center.

История ревизий

В разделе **История ревизий** можно управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Создание и настройка задач в Kaspersky Security Center

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

kaspersky

В этом разделе

О создании задач с помощью Веб-плагина

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых компьютеров. Можно создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Мониторинг целостности файлов на основе эталона
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого компьютера: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**.
- Для группы администрирования: в панели результатов узла выбранной группы защищаемых компьютеров на закладке **Задачи**.
- Для набора защищаемых компьютеров: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 373) по требованию на всех защищаемых компьютерах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Создание задачи с помощью Веб-плагина

► *Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
     b. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемый компьютер.
     c. Выберите название защищаемого компьютера.
     d. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
     e. Нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
     b. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.
     c. Нажмите на кнопку **Добавить**.
   - Чтобы создать задачу для произвольного набора защищаемых компьютеров, выполните следующие действия:
     a. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
     b. Выберите выборку устройств, для которой требуется создать задачу.
     c. Нажмите на кнопку **Запустить**.
     d. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.
     e. Нажмите на кнопку **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В раскрывающемся списке **Программы** выберите **Kaspersky Industrial CyberSecurity for Nodes**.
3. В раскрывающемся списке **Тип задачи** выберите тип создаваемой задачи.

   Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно параметров.
4. В зависимости от выбранного типа задачи выполните одно из следующих действий:
   - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 570).
   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
     a. Выберите источник обновлений в разделе **Источник обновления баз программы**.
     b. В окне **Настройка параметров соединения** настройте параметры прокси-сервера.

- После создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Обновление модулей программы**:
  a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.
  b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого компьютера. Чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически запускала перезагрузку защищаемого компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.
  c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Industrial CyberSecurity for Nodes, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

  "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.
- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Копирование обновлений**.
- Для создания задачи Активация программы:
  a. В окне **Список ключей в хранилище ключей Kaspersky Security Center** укажите файл ключа, с помощью которого вы хотите активировать программу.
  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
- Создайте задачу Формирование правил контроля запуска программ и настройте ее параметры.
- Создайте задачу Формирование правил контроля устройств и настройте ее параметры.

5. Нажмите на кнопку **Далее**.
6. Если задача создана для набора защищаемых компьютеров, выберите сеть (группу) защищаемых компьютеров, на которых она будет выполняться.
7. Нажмите на кнопку **Далее**.
8. В окне **Завершение создания задачи** установите флажок **Перейти к параметрам задачи после создания**, чтобы настроить параметры задачи.
9. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Настройка групповых задач с помощью Веб-плагина

► *Чтобы настроить групповую задачу для нескольких защищаемых компьютеров, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     a. В разделе **Область проверки** настройте область проверки.
     b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
     a. В разделе **Источники обновлений** настройте параметры источника обновлений и прокси-сервера.
     b. В разделе **Оптимизация** настройте параметры оптимизации дисковой подсистемы.
   - Чтобы настроить задачу Обновление модулей программы, в разделе **Дополнительные параметры** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
   - Чтобы настроить задачу Копирование обновлений, в разделе **Параметры копирования обновлений** укажите состав обновлений и папку назначения.
   - Чтобы настроить задачу Активация программы, примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
   - Чтобы настроить автоматическое формирование разрешающих правил контроля устройств, укажите параметры, на основе которых будет сформирован список разрешающих правил.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. На закладке **Параметры** в разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры групповых задач будут сохранены.

В этом разделе

Настройка задачи Активация программы с помощью Веб-плагина

► *Чтобы настроить задачу Активация программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. В разделе **Общие** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
4. Настройте расписание задачи в разделе **Расписание**.
5. В окне **<Название задачи>** нажмите на кнопку **OK**.

Настройка задач обновления с помощью Веб-плагина

► *Чтобы настроить задачи Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. В разделе **Источники обновлений** настройте параметры источника обновлений:
   - В разделе **Источник обновления баз программы** укажите Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновлений: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

     Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     > Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).

   - В разделе **Настройка параметров соединения** настройте использование прокси-сервера для подключения к серверам обновлений "Лаборатории Касперского" и другим серверам.
4. В разделе **Оптимизация** для задачи Обновление баз программы можно настроить функцию, снижающую нагрузку на дисковую подсистему:
   - **Оптимизация использования дисковой подсистемы**

     Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.

   - **Объем оперативной памяти, используемой для оптимизации (400 - 9999 МБ)**

     Объем оперативной памяти (в МБ), используемый программой для хранения файлов обновлений. По умолчанию задан объем 600 МБ. Минимальный объем

составляет 400 МБ.

При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

- Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении). Это приведет к завершению задачи с ошибкой.

  В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. Функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

  В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В окне **<Название задачи>** нажмите на кнопку **OK**.

Настройка параметров диагностики сбоев с помощью Веб-плагина

Если в работе Kaspersky Industrial CyberSecurity for Nodes возникла проблема (например, аварийное завершение Kaspersky Industrial CyberSecurity for Nodes), ее можно диагностировать. Для этого можно включить создание файлов трассировки и файла дампа процессов Kaspersky Industrial CyberSecurity for Nodes и отправить эти файлы на анализ в Службу технической поддержки.

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

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 389).
2. Откройте раздел **Диагностика сбоев**.
3. Чтобы отладочная информация записывалась в файл, в разделе **Параметры диагностики сбоев** установите флажок **Включить трассировку**.
4. В поле **Папка файлов трассировки** укажите абсолютный путь к локальной папке, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
5. Настройте уровень детализации отладочной информации.

   В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки. Параметр доступен, если установлен флажок **Включить трассировку**.

   Вы можете выбрать один из следующих режимов работы задачи:

   - **Полная информация** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файле трассировки всю отладочную информацию.
   - **Краткая информация** – Kaspersky Industrial CyberSecurity for Nodes сохраняет в файл трассировки только информацию о критических событиях.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

   По умолчанию установлен уровень детализации **Полная информация**.
6. Укажите **Максимальный размер файлов трассировки (МБ)**.

   Доступные значения: от 1 до 4095 МБ. По умолчанию максимальный размер файлов трассировки составляет 50 МБ.
7. Для удаления самых старых файлов трассировки при достижении максимального количества файлов установите флажок **Использовать вытеснение старых файлов журнала трассировки**.
8. Укажите значение **Максимальное количество файлов журнала трассировки**.

   Доступные значения: от 1 до 999. По умолчанию максимальное количество файлов составляет 5. Поле доступно, если установлен флажок **Использовать вытеснение старых файлов журнала трассировки**.
9. Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.
10. В поле **Папка файлов дампа** укажите абсолютный путь к локальной папке, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы дампа.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
11. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом компьютере.

kaspersky

Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Industrial CyberSecurity for Nodes, а также настроить параметры запуска по расписанию.

В этом разделе

Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. В разделе **Расписание** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.
5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
      - **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
      - **После обновления баз программы**, если вы 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.

6. В разделе **Параметры остановки задачи**:
   a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
   b. Установите флажок **Приостановить задачу** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
7. В блоке **Дополнительные параметры расписания**:
   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 **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры запуска задачи.

Включение и выключение запуска задач 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 главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. Выберите раздел **Расписание**.
5. Выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

kaspersky

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Industrial CyberSecurity for Nodes доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Отчет о статусе компонентов Kaspersky Industrial CyberSecurity for Nodes components

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center Web Console присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть статус компонентов в параметрах программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Выберите название защищаемого компьютера.
3. На закладке **Общие** выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

   Информация о статусе компонента Защита от эксплойтов недоступна в этой таблице.

► *Чтобы просмотреть стандартный отчет Kaspersky Security Center Web Console, выполните следующие действия:*

1. Выберите **Мониторинг и отчетность** → **Отчеты**.
2. В списке выберите **Отчет о статусе компонентов программы** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
3. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых компьютерах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых компьютерах.

► *Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 672).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 672).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

kaspersky

Лицензирование программы

Программа остается в сертифицированном состоянии при условии активации только с помощью файла ключа.

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности, описывающих обработку и передачу данных, следующими способами:

- Во время установки Консоли Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Установка Kaspersky Industrial CyberSecurity for Nodes" на стр. 296).

- Из меню **Пуск** (**Все программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Лицензионное соглашение и Политика конфиденциальности**) после установки.
- Во время установки Kaspersky Security Gateway (см. раздел "Установка Kaspersky Security Gateway с помощью мастера установки" на стр. 335).
- Ознакомившись с документом license.txt, входящим в комплект поставки.
- На сайте "Лаборатории Касперского" (https://www.kaspersky.ru/business/eula https://www.kaspersky.ru/business/eula).

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Программа активируется с помощью файла ключа приобретаемой коммерческой лицензии.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, будет недоступно обновление баз Kaspersky Industrial CyberSecurity for Nodes). Чтобы продолжить использование Kaspersky Industrial CyberSecurity for Nodes в режиме полной функциональности, вам нужно продлить (см. раздел "Продление срока действия лицензии" на стр. 485) срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации (если применимо).

В Лицензионном сертификате содержится следующая информация о текущей лицензии:

- номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройства, на которых можно использовать программу с предоставленной лицензией);

- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- Тип лицензии.

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в программу с помощью файла ключа. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Специалисты "Лаборатории Касперского" могут поместить ключ в список запрещенных ключей из-за нарушения Лицензионного соглашения. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для коммерческой или пробной лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

О файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Industrial CyberSecurity for Nodes или после заказа пробной версии Kaspersky Industrial CyberSecurity for Nodes.

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

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

kaspersky

О коде активации

Код активации – уникальная последовательность из 20 символов (букв и цифр). Вам нужно ввести код активации, чтобы добавить ключ для активации Kaspersky Industrial CyberSecurity for Nodes. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Industrial CyberSecurity for Nodes или при заказе пробной версии Kaspersky Industrial CyberSecurity for Nodes.

Чтобы активировать программу с помощью кода активации, необходим доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Можно восстановить утерянный после установки программы код активации. Код активации может понадобиться, например, чтобы зарегистрировать Kaspersky CompanyAccount. Чтобы восстановить код активации, обратитесь к партнеру «Лаборатории Касперского», у которого вы приобрели лицензию.

О подписке

Подписка – это заказ на приобретение программы с определенными параметрами: дата окончания подписки и количество защищаемых устройств. Подписка предоставляет право на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Industrial CyberSecurity for Nodes можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или автоматически, а можно отказаться от нее. Можно также приостанавливать и возобновлять подписку. Управление подпиской доступно через поставщика услуг, вы не можете управлять подпиской самостоятельно.

В зависимости от поставщика услуг, набор возможных действий для управления подпиской может различаться. Поставщик услуг может предоставлять *льготный период* для продления подписки.

Льготный период – это временной период между окончанием и продлением подписки, в течение которого сохраняется функциональность программы.

Подписка может быть *ограниченной* или *неограниченной*.

Ограниченная подписка имеет ограниченный срок действия и не предусматривает автоматического продления.

Неограниченная подписка продлевается автоматически без вашего участия после своевременной оплаты и не имеет фиксированной даты окончания.

Статус подписки отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** и обновляется автоматически ежечасно. Вы не можете обновить статус подписки вручную.

О предоставлении данных

Принимая условия Лицензионного соглашения, вы соглашаетесь отправлять в автоматическом режиме следующие данные в "Лабораторию Касперского":

- для поддержки механизма получения обновлений – данные об установленной программе и лицензионном сертификате: идентификатор устанавливаемой программы и ее полная версия, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, уникальный идентификатор задачи обновления;

- для управления согласием на обработку данных – данные о статусе согласия с условиями Лицензионного соглашения и других документов, оговаривающих условия отправки данных: идентификатор и версия Лицензионного соглашения или другого документа, в рамках которого принимаются или отклоняются условия обработки данных; атрибут, обозначающий действие пользователя (подтверждение или отмена принятия условий); дата и время изменения статуса принятия условий обработки данных;
- Для активации программы с помощью кода активации – данные о типе, версии и локализации установленного приложения, версия установленных обновлений, идентификатор защищаемого устройства и идентификатор установки программы на защищаемом устройстве, код активации и уникальный идентификатор текущей лицензии, тип, версия и разрядность операционной системы, имя виртуальной среды при установке программы в виртуальной среде и идентификаторы компонентов программы, активных в момент предоставления информации.

Данные, получаемые от вас "Лабораторией Касперского" во время использования программы, защищаются и обрабатываются в соответствии с требованиями, установленными законодательством и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи. Более подробная информация об обработке, хранении и уничтожении информации, получаемой в процессе использования программы и передаваемой в "Лабораторию Касперского", приведена в Политике конфиденциальности на сайте www.kaspersky.com/Products-and-Services-Privacy-Policy.

Локальная обработка данных

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

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных, содержащихся в отчетах.

Таблица 69. Обработка и хранение данных, содержащихся в отчетах

Функциональная область	Аудит.
Тип использования	Kaspersky Industrial CyberSecurity for Nodes хранит данные локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о событиях программы, произошедших на управляемых защищаемых устройствах.
Хранилище	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<версия продукта>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • База данных Сервера администрирования
Меры безопасности	Список контроля доступа (Access-control list).
Период хранения	Kaspersky Industrial CyberSecurity for Nodes хранит данные до момента удаления Kaspersky Industrial CyberSecurity for Nodes. При удалении Kaspersky Industrial CyberSecurity for Nodes будут удалены все данные Kaspersky Industrial CyberSecurity for Nodes, хранящиеся на защищаемом устройстве.
Назначение	Обеспечение основных функций.

Kaspersky Industrial CyberSecurity for Nodes не удаляет события в журнале событий Windows.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит в отчетах следующие данные:

- Имена и атрибуты обрабатываемых файлов и полные пути к ним на проверяемом носителе.
- Действия, выполняемые над проверяемыми файлами программой Kaspersky Industrial CyberSecurity for Nodes.
- Действия, выполняемые пользователями над проверяемыми файлами на защищаемом компьютере.
- Информация об учетных записях пользователей, выполняющих действия в защищаемой сети или на защищаемом устройстве.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о процессах и скриптах, запущенных в системе: контрольные суммы (MD5, SHA-256) и полные пути к исполняемым файлам, информация о цифровых сертификатах.
- Параметры брандмауэра Windows.
- Записи журнала событий Windows.
- Имена учетных записей пользователей, выполняющих действия над проверяемыми файлами на защищаемом компьютере.

- Экземпляры запущенных исполняемых файлов, а также типы, имена, контрольные суммы и атрибуты этих файлов.
- Информация о сетевой активности: IP-адреса заблокированных внешних устройств, идентификаторы скомпрометированных сеансов входа, во время которых был выполнен доступ к общим защищаемым ресурсам.
- Информация о сетях Wi-Fi, к которым подключается защищаемый компьютер: сетевые имена и сетевые идентификаторы.
- Информация о проектах ПЛК, добавленных в область защиты, включая параметры подключения ПЛК (IP-адреса, номера шин и слотов) и контрольные суммы микропрограммного обеспечения.
- Информация о статусе USN-журнала Windows.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных о параметрах, указанных пользователями.

Kaspersky Industrial CyberSecurity for Nodes обрабатывает и хранит данные только о параметрах, указанных пользователями.

Таблица 70. Обработка и хранение данных о параметрах, указанных пользователями

Функциональная область	Автообновление, интеграция с изолированной средой.
Тип использования	Kaspersky Industrial CyberSecurity for Nodes хранит данные о параметрах локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о параметрах управляемых защищаемых устройств.
Хранилище	%ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<product version>\
Меры безопасности	Список контроля доступа (Access-control list).
Период хранения	Kaspersky Industrial CyberSecurity for Nodes хранит данные до момента удаления Kaspersky Industrial CyberSecurity for Nodes. При удалении Kaspersky Industrial CyberSecurity for Nodes будут удалены все данные Kaspersky Industrial CyberSecurity for Nodes, хранящиеся на защищаемом устройстве.
Назначение	Обеспечение основных функций.

Kaspersky Industrial CyberSecurity for Nodes не удаляет данные о параметрах, экспортируемых в конфигурационный файл.
Kaspersky Industrial CyberSecurity for Nodes не удаляет объекты на карантине и в резервном хранилище, если установлены флажки **Экспортировать объекты на карантине** и **Экспортировать объекты на карантине** в мастере установки.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит следующие данные о параметрах, указанных пользователями:

- Информация об объектах, помещенных на карантин или в резервное хранилище.
- Информация о параметрах, настроенных через Консоль программы или Плагин управления, например:
  - Пароль Kaspersky Industrial CyberSecurity for Nodes, имена учетных записей пользователей, с правами которых запускаются задачи Kaspersky Industrial CyberSecurity for Nodes.
  - Имя учетной записи пользователя, используемое для аутентификации на прокси-сервере.
  - Адреса сетевых папок или папок на HTTP- или FTP-серверах, используемых в качестве пользовательских источников обновлений.
  - Информация о сетях Wi-Fi.
  - Информация о проектах ПЛК, добавленных в область защиты, включая параметры подключения ПЛК и контрольные суммы микропрограммного обеспечения.
  - IP-адреса и идентификаторы заблокированных сеансов входа.
  - Параметры брандмауэра Windows.
  - Контрольные суммы (MD5, SHA-256) и пути к исполняемым файлам, добавленным в правила задачи Контроль запуска программ.
  - Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
  - Информация о папках, включенных в области задач Kaspersky Industrial CyberSecurity for Nodes.
  - Информация о событиях в журнале событий Windows.
  - Информация о файлах, обнаруженных с использованием технологий iSwift и iChecker.
  - Контрольные суммы (MD5, SHA-256) и пути к файлам, добавленным в доверенную зону.
  - Информация о добавленных лицензионных ключах.
  - Информация о цифровых сертификатах.
  - Контрольные суммы файлов, данные цифровых сертификатов, полные пути к файлам (база данных SDC, файлы для задачи Мониторинг целостности файлов на основе эталона).
  - Временные файлы, создаваемые программой при проверке архивов.
  - Информация в %SystemRoot%.
- Данные о файлах, обработанных Kaspersky Industrial CyberSecurity for Nodes, например, контрольные суммы (MD5, SHA-256) файлов, информация о цифровых сертификатах, полные пути к файлам.

Kaspersky Industrial CyberSecurity for Nodes обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий программы и получения диагностических данных. Обработка и защита локально обрабатываемых данных выполняются в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Industrial CyberSecurity for Nodes позволяет настроить уровень защиты данных, обрабатываемых локально: вы можете изменять права пользователей на доступ к обрабатываемым данным, изменять сроки хранения таких данных, частично или полностью отключать функциональность, в рамках которой выполняется регистрация данных, а также изменять путь к папке на диске, в которую выполняется запись данных, и ее атрибуты.

Детальная информация по настройке функциональности программы, в рамках которой выполняется обработка данных, содержится в соответствующих разделах настоящего Руководства.

Локальная обработка данных вспомогательными компонентами программы

В пакет установки Kaspersky Industrial CyberSecurity for Nodes включены вспомогательные компоненты программы, которые могут быть установлены на устройстве, даже если на нем не установлена программа Kaspersky Industrial CyberSecurity for Nodes.

При выполнении основных функций программы, описанных в настоящем Руководстве, вспомогательные компоненты программы локально обрабатывают и хранят набор данных на защищаемом устройстве, на котором они установлены, даже если они установлены отдельно от Kaspersky Industrial CyberSecurity for Nodes.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных, записываемых в файлы дампов и файлы трассировки.

По умолчанию, Kaspersky Industrial CyberSecurity for Nodes не записывает файлы дампов и файлы трассировки.

Таблица 71. Обработка и хранение данных, записываемых в файлы дампов и файлы трассировки

Хранилище	По умолчанию папка, в которую сохраняются файлы дампов и файлы трассировки, не указана. Можно указать папку.
Меры безопасности	Kaspersky Industrial CyberSecurity for Nodes не ограничивает доступ к файлам дампов и файлам трассировки.
Период хранения	Kaspersky Industrial CyberSecurity for Nodes не удаляет файлы дампов и файлы трассировки.
Назначение	Обеспечение технической поддержки.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит следующие данные, записанные в файлы дампов и файлы трассировки:

- Информация о действиях, выполняемых программой Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве.
- Информация об объектах, обработанных программой Kaspersky Industrial CyberSecurity for Nodes.
- Информация об ошибках, возникших во время работы программы Kaspersky Industrial CyberSecurity for Nodes.

Данные, обрабатываемые вспомогательными компонентами программы, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые вспомогательными компонентами программы в ходе работы, удаляются после удаления этих компонентов.

Исключение составляют файлы трассировки вспомогательных компонентов программы. Рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные вспомогательных компонентов программы, в соответствующих разделах настоящего Руководства.

Активация программы с помощью файла ключа

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes с помощью файла ключа.

Если в Kaspersky Industrial CyberSecurity for Nodes уже добавлен активный ключ и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее ключ будет удален.

Если в Kaspersky Industrial CyberSecurity for Nodes уже добавлен дополнительный ключ и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее дополнительный ключ будет удален.

Если в Kaspersky Industrial CyberSecurity for Nodes уже добавлены активный ключ и дополнительный ключ, а вы добавите новый ключ в качестве активного, то новый ключ заменит ранее добавленный активный ключ, а дополнительный ключ не будет удален.

► *Чтобы активировать Kaspersky Industrial CyberSecurity for Nodes с помощью файла ключа, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор**.
4. Выберите файл ключа с расширением key.

   Вы также можете добавить ключ в качестве дополнительного. Для этого установите флажок **Использовать в качестве дополнительного ключа**.

5. Нажмите на кнопку **ОК**.

   Будет применен выбранный файл ключа. Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

Активация программы с помощью кода активации

Для активации программы с помощью кода активации защищаемый компьютер должен быть подключен к интернету.

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes с помощью кода активации.

При активации этим способом Kaspersky Industrial CyberSecurity for Nodes отправляет данные на сервер активации для проверки введенного кода:

- В случае успешной проверки кода активации программа будет активирована.
- При сбое проверки кода активации отобразится соответствующее уведомление. В этом случае обратитесь к поставщику, у которого была приобретена лицензия на программу Kaspersky Industrial CyberSecurity for Nodes.
- В случае превышения количества активаций с помощью указанного кода активации, отображается соответствующее уведомление. Процесс активации программы будет прерван, и вам будет предложено обратиться в Службу технической поддержки.

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes, используя код активации в Консоли программы или создав групповую задачу Активация программы с помощью Плагина управления (см. раздел "Настройка групповых задач в Kaspersky Security Center" на стр. 390) или Веб-плагина (см. раздел "Настройка групповых задач с помощью Веб-плагина" на стр. 462).

► *Чтобы активировать Kaspersky Industrial CyberSecurity for Nodes с помощью кода активации в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить код активации**.
3. В открывшемся окне введите код активации в поле **Код активации**.
   - Чтобы применить код активации для добавления дополнительного ключа, установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы просмотреть информацию о лицензии, нажмите на кнопку **Показать информацию о лицензии**. Информация отобразится в блоке **Информация о лицензии**.
4. Нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes отправит информацию о примененном коде активации на сервер активации.

Просмотр информации о действующей лицензии

Просмотр статуса лицензии

Информация о статусе действующей лицензии отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** Консоли программы. Статус лицензии может принимать следующие значения:

- **Выполняется проверка статуса лицензии** – Kaspersky Industrial CyberSecurity for Nodes проверяет добавленный файл ключа и ожидает ответа о текущем статусе.
- **Дата окончания срока действия лицензии** – программа Kaspersky Industrial CyberSecurity for Nodes активирована до указанной даты. Статус выделен желтым цветом в следующих случаях:
  - до истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ;
  - Добавленный ключ помещен в список запрещенных и будет заблокирован.
- **Программа не активирована** – программа Kaspersky Industrial CyberSecurity for Nodes не активирована, поскольку не добавлен ключ. Статус выделен красным цветом.

- **Срок действия лицензии истек** – программа Kaspersky Industrial CyberSecurity for Nodes не активирована, поскольку истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – программа Kaspersky Industrial CyberSecurity for Nodes не активирована, поскольку нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. 472). Статус выделен красным цветом.
- **Ключ добавлен в запрещенный список** – добавленный файл ключа заблокирован и помещен в список запрещенных ключей специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.

Просмотр информации о действующей лицензии

► *Чтобы просмотреть информацию о действующей лицензии,*

в дереве Консоли программы разверните узел **Лицензирование**.

В панели результатов узла **Лицензирование** отобразится общая информация о действующей лицензии (см. таблицу ниже).

Таблица 72. Общая информация о лицензии в узле Лицензирование

Поле	Описание
Статус активации	Информация о статусе активации программы. Информация в графе Статус активации в панели управления узла Лицензирование может принимать следующие значения: • **Применено** – если вы активировали программу с помощью ключа. • **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.
Ключ	Номер ключа, с помощью которого вы активировали программу.
Тип лицензии	Тип лицензии: *Коммерческая*.
Дата окончания срока действия	Дата и время окончания срока действия лицензии, связанной с активным ключом.
Статус кода активации или ключа	Статус кода активации или ключа: *Активный* или *Дополнительный*.

► *Чтобы просмотреть подробную информацию о лицензии,*

в панели результатов узла **Лицензирование** откройте контекстное меню требуемой лицензии и выберите пункт **Свойства**.

В окне **Свойства ключа** на закладке **Общие** отображается подробная информация о действующей лицензии, а на закладке **Дополнительно** – информация о заказчике и контактная информация "Лаборатории Касперского" или партнера, у которого вы приобрели Kaspersky Industrial CyberSecurity for Nodes (см. таблицу ниже).

Таблица 73. Подробная информация о лицензии в окне Свойства <Номер ключа>

Поле	Описание
Закладка Общие	
Ключ	Номер ключа, с помощью которого вы активировали программу.
Дата добавления ключа	Дата добавления ключа в программу.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Истекает через (сут)	Число суток, оставшихся до даты окончания срока действия лицензии по активному ключу.
Дата окончания срока действия	Дата окончания срока действия лицензии по активному ключу. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если программе Kaspersky Industrial CyberSecurity for Nodes не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*.
Программа	Название программы, которая была активирована с помощью добавленного ключа.
Ограничение на использование ключа	Предусмотренное ограничение на использование ключа (если имеется).
Осуществление технической поддержки	Информация о том, оказывает ли "Лаборатории Касперского" или ее партнеры техническую поддержку заказчику по условиям предоставления лицензии.
Закладка Дополнительно	
Информация о лицензии	Номер и тип действующей лицензии.
Информация о поддержке	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
Информация о владельце	Информация о заказчике лицензии: имя заказчика и название организации, для которой приобретена лицензия.

kaspersky

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов:

- Останавливаются все задачи, за исключением задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы.
- Невозможно запустить ни одну задачу, кроме задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы. Эти задачи продолжат работать с использованием старых антивирусных баз.
- Функция Защита от эксплойтов ограничена:
  - Процессы защищаются до их перезапуска.
  - Новые процессы нельзя включить в область защиты.

Другие функции (хранилища, журналы, диагностические данные) по-прежнему доступны.

Продление срока действия лицензии

По умолчанию программа уведомляет вас о скором окончании срока действия лицензии за 14 дней до даты окончания срока действия лицензии. При этом статус **Дата окончания срока действия лицензии** в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** выделяется желтым цветом.

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью дополнительного ключа. Это позволяет не прерывать защиту компьютера на период после окончания срока действия используемой лицензии и до активации программы по новой лицензии.

► *Чтобы обновить лицензию, выполните следующие действия:*

1. Приобретите новый файл ключа.
2. В дереве Консоли программы выберите узел **Лицензирование**.
3. В контекстном меню узла **Лицензирование** выберите пункт **Добавить ключ**.
4. В открывшемся окне нажмите на кнопку **Обзор** и выберите новый файл ключа с расширением key.
5. Установите флажок **Использовать в качестве дополнительного ключа**.
6. Нажмите на кнопку **ОК**.

Дополнительный ключ будет добавлен и автоматически станет активным по истечении срока действия текущей лицензии на Kaspersky Industrial CyberSecurity for Nodes.

Убедитесь, что дата окончания срока действия дополнительного ключа наступает позже даты окончания срока действия активного ключа.

Нельзя использовать подписку для добавления дополнительного ключа.

kaspersky

Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Industrial CyberSecurity for Nodes добавлен дополнительный ключ, и вы удалите активный ключ, дополнительный ключ автоматически станет активным.

Если вы удалите добавленный ключ, вы можете его восстановить, повторно применив файл ключа.

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

1. В дереве Консоли программы выберите узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** в таблице с информацией о добавленных ключах выберите ключ, который вы хотите удалить.
3. В контекстном меню строки с информацией о выбранном ключе выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

Выбранный ключ будет удален.

Kaspersky Industrial CyberSecurity for Nodes автоматически регулирует количество используемых процессов.

Это значение установлено по умолчанию.

Kaspersky Industrial CyberSecurity for Nodes контролирует количество активных рабочих процессов в соответствии с указанными значениями.

Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

kaspersky

Запуск и остановка Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security.

В этом разделе

Запуск Плагина управления Kaspersky Industrial CyberSecurity for Nodes

Для запуска Плагина управления Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на защищаемое устройство администратора, он запускается вместе с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Запуск Консоли Kaspersky Industrial CyberSecurity for Nodes из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль программы из меню **Пуск**, выполните следующие действия:*

1. в меню **Пуск** выберите **Программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Средства администрирования** > **Консоль Kaspersky Industrial CyberSecurity for Nodes**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► *Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:*

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

Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом компьютере откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом устройстве, подключитесь к защищаемому компьютеру.

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

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

   Откроется окно **Выбор защищаемого устройства**.
3. В открывшемся окне выберите **Другое устройство**.
4. В поле ввода справа укажите сетевое имя защищаемого компьютера.
5. Нажмите на кнопку **ОК**.

Консоль программы подключится к защищаемому компьютеру.

Если учетная запись, используемая для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на защищаемом 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 сразу после 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 запускаются задачи Постоянная защита файлов и Проверка при старте 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 указано **При запуске программы**. Остальные задачи нужно 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, если вы входите в группу "Администраторы" на защищаемом компьютере.

► *Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите одну из следующих команд:
   - **Остановить программу**
   - **Запустить программу**

Служба Kaspersky Security будет запущена или остановлена.

Запуск компонентов Kaspersky Industrial CyberSecurity for Nodes при безопасном режиме загрузки операционной системы

В этом разделе приведена информация о работе Kaspersky Industrial CyberSecurity for Nodes при безопасном режиме загрузки операционной системы.

В этом разделе

О работе Kaspersky Industrial CyberSecurity for Nodes при безопасном режиме загрузки операционной системы

Компоненты Kaspersky Industrial CyberSecurity for Nodes можно запустить при загрузке операционной системы в безопасном режиме. Наряду со службой Kaspersky Security (kavfs.exe) загружается драйвер klam.sys. Драйвер используется для регистрации службы Kaspersky Security как защищенной службы при загрузке операционной системы. Дополнительные сведения приведены в разделе Регистрация службы Kaspersky Security как защищенной службы.

Kaspersky Industrial CyberSecurity for Nodes можно запустить при загрузке операционной системы в следующих безопасных режимах:

- Безопасный режим с типом загрузки "Минимальная" – стандартный вариант безопасного режима загрузки операционной системы. При этом Kaspersky Industrial CyberSecurity for Nodes может запускать следующие компоненты:
  - Постоянная защита файлов.
  - Проверка по требованию.
  - Контроль запуска программ и Формирование правил контроля запуска программ.
  - Анализ журналов.

- Мониторинг файловых операций.
- Мониторинг целостности файлов на основе эталона.
- Проверка целостности программы.

Безопасный режим с типом загрузки «Сеть» – загрузка операционной системы в безопасном режиме с поддержкой сетевых драйверов. В этом режиме помимо компонентов, запускаемых в безопасном режиме с типом загрузки «Минимальная», Kaspersky Industrial CyberSecurity for Nodes может запускать следующие компоненты:

- Обновление баз программы.
- Обновление модулей программы.

Запуск Kaspersky Industrial CyberSecurity for Nodes в безопасном режиме

По умолчанию, Kaspersky Industrial CyberSecurity for Nodes не запускается при загрузке операционной системы в безопасном режиме.

► *Чтобы запустить Kaspersky Industrial CyberSecurity for Nodes при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `1`.
5. Нажмите на кнопку **OK**.

► *Чтобы отменить запуск Kaspersky Industrial CyberSecurity for Nodes при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `0`.
5. Нажмите на кнопку **OK**.

kaspersky

Диагностическое окно

В этом разделе описано использование диагностического окна для просмотра статуса или текущей активности защищаемого компьютера и настройка записи файлов дампов и файлов трассировки.

В этом разделе

О диагностическом окне

Компонент Диагностическое окно (далее также CDI) устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы и может быть использован, даже если Консоль программы не установлена на защищаемом компьютере. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на защищаемом компьютере.

В диагностическом окне можно выполнять следующие действия:

- просматривать информацию об общем статусе программы (см. раздел "Просмотр состояния Kaspersky Industrial CyberSecurity for Nodes с помощью диагностического окна" на стр. 492);
- просматривать произошедшие инциденты безопасности (см. раздел "Просмотр статистики событий безопасности" на стр. 493);
- просматривать текущую активность на защищаемом (см. раздел "Просмотр текущей активности программы" на стр. 494) устройстве;
- запускать и останавливать запись файлов дампов и файлов трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 495);
- открывать Консоль программы;
- открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Industrial CyberSecurity for Nodes защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

kaspersky

Просмотр состояния Kaspersky Industrial CyberSecurity for Nodes с помощью диагностического окна

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

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

   Откроется **Диагностическое окно**.

На закладке **Статус защиты** можно просмотреть текущий статус ключа, а также статус задач постоянной защиты компьютера и задач обновления. Для уведомления о состояниях защиты используется цветовая индикация (см. таблицу ниже).

Таблица 74. Статус защиты в диагностическом окне

Раздел	Состояние

Статус постоянной защиты	Панель *зеленого* цвета отображается при любом из следующих сценариев (при выполнении любого из 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.

	Панель *желтого* цвета отображается, если выполнено одно или несколько из следующих условий: • Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию). • Задача Контроль запуска программ запущена в режиме **Только статистика**. • Защита от эксплойтов и задача Контроль запуска программ запущены в режиме **Только статистика**.
	Панель *красного* цвета отображается, если 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**.

Раздел	Состояние
Лицензирование	Панель *зеленого* цвета отображается при действующей лицензии.
	Панель *желтого* цвета отображается, если возникло одно из следующих событий: • *Выполняется проверка статуса лицензии*. • *До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации.* • *Добавленный ключ помещен в список запрещенных и будет заблокирован.*
	Панель *красного* цвета отображается, если возникло одно из следующих событий: • *Программа не активирована* • *Срок действия лицензии истек* • *Нарушено Лицензионное соглашение* • *Ключ добавлен в запрещенный список*
Обновление	Панель *зеленого* цвета отображается, если базы программы актуальны.
	Панель *желтого* цвета отображается, если базы программы устарели.
	Панель *красного* цвета отображается, если базы программы сильно устарели.

Просмотр статистики событий безопасности

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 в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Выберите закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

kaspersky

Просмотр текущей активности программы

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

Для отображения статуса активности программы используется цветовая индикация:

- В разделе **Задачи**:
  - *Зеленый цвет*. Не выполнены условия, при которых требовалась бы индикация красным цветом.
  - *Желтый цвет*. Проверка важных областей не проводилась давно.
  - *Красный цвет*. Выполнено как минимум одно из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В разделе **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

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

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

   Откроется **Диагностическое окно**.
3. Выберите закладку **Текущая активность программы**.
4. В разделе **Задачи** ознакомьтесь со следующей информацией:
   - **Проверка важных областей давно не выполнялась**.

     Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
   - **Выполняется сейчас**.
   - **Завершены с ошибкой**.
   - **Следующий запуск определен по расписанию**.
5. В разделе **Kaspersky Security Network** ознакомьтесь со следующей информацией:
   - **Включено с запросами файловой репутации** или **Не используется**.
   - **Включено с запросами файловой репутации**, **включена отправка статистики KSN.**
6. В разделе **Интеграция с Kaspersky Security Center** ознакомьтесь со следующей информацией:
   - **Разрешено локальное управление**.
   - **Применяется политика: <Имя Сервера администрирования>**.

kaspersky

Настройка записи файлов дампов и файлов трассировки

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

Вы можете также настроить диагностику сбоев в Консоли программы (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 416).

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

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

   Откроется **Диагностическое окно**.
3. Выберите закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
   a. Установите флажок **Записывать отладочную информацию в файл трассировки**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки.

      Трассировка будет включена для всех компонентов с параметрами по умолчанию: уровнем детализации *Отладка* и максимальным размером файла журнала 50 МБ.
5. Если требуется, настройте следующие параметры записи файлов дампов:
   a. Установите флажок **Создавать файл дампа во время сбоя в указанной папке**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файл дампа.
6. Нажмите на кнопку **Применить**.

   Новая конфигурация будет применена.

kaspersky

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 проверяет следующие объекты защищаемого устройства при доступе к ним:

- файлы;
- альтернативные потоки данных NTFS;
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;
- файлы-контейнеры Windows Server 2016 и Windows Server 2019.

При записи или считывании файла любой программой на защищаемом компьютере, Kaspersky Industrial CyberSecurity for Nodes перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Перед лечением или удалением Kaspersky Industrial CyberSecurity for Nodes сохраняет зашифрованную копию исходного файла в папку резервного хранилища.

Kaspersky Industrial CyberSecurity for Nodes перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016 и Windows Server 2019.

Контейнер – это изолированная среда, где программа может работать без прямого взаимодействия с операционной системой. Если контейнер расположен в области защиты задачи, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы контейнера, к которому получают доступ пользователи, на наличие компьютерных угроз. При обнаружении угрозы, программа пытается вылечить контейнер. Если лечение успешно, контейнер продолжает работу. Если лечение невозможно, контейнер выключается.

Kaspersky Industrial CyberSecurity for Nodes также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих параметрах.

Об области защиты и параметрах безопасности задачи

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы устройства. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов устройства, контролируемых Kaspersky Industrial CyberSecurity for Nodes. По умолчанию сетевые файловые ресурсы устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы перейти к отображению сетевых файловых ресурсов в виде дерева в Консоли программы,*

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

Независимо от того, отображаются ли файловые ресурсы защищаемого компьютера в виде списка или в виде дерева, значки узлов имеют следующие значения:

☑ 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 родительского узла (только при отображении 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.

С помощью Консоли программы можно также добавлять в область защиты виртуальные диски (см. раздел "Формирование виртуальной области защиты" на стр. 532). Имена виртуальных узлов отображаются синим цветом.

Параметры безопасности

Параметры безопасности задачи можно настроить как едиными для всех узлов или элементов, входящих в область защиты, так и индивидуальными для каждого узла или элемента в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- Выбрать один из трех стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 499).
- Настроить параметры безопасности вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 514) для выбранных узлов или элементов в дереве или списке файловых ресурсов (уровень безопасности изменится на **Другой**).

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

О виртуальной области защиты

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

Если все объекты устройства включены в область защиты, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для динамических узлов или если вы выбрали для защиты отдельные области устройства, то, для того чтобы включить в область защиты виртуальные диски, файлы или папки, вам нужно предварительно создать их в Консоли программы, то есть задать виртуальную область защиты. Созданные диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого компьютера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, все появившиеся в ней виртуальные папки или файлы не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

Стандартные области защиты

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы на жестких дисках устройства.
- **Съемные диски**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.

- **Сетевое окружение**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на устройстве. Kaspersky Industrial CyberSecurity for Nodes не защищает файлы, когда к ним обращаются программы с других защищаемых устройств.
- **Виртуальные диски**. Можно включать в область защиты виртуальные папки и файлы, а также диски, временно подключенные к устройству, например, общие диски кластера.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

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

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого компьютера в Консоли программы. Чтобы включить в область защиты объекты на виртуальном диске, включите в область защиты папку на устройстве, связанную с этим виртуальным диском.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов защищаемого компьютера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Industrial CyberSecurity for Nodes на защищаемых компьютерах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

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

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Только сообщать

Уровень безопасности **Только уведомлять** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

Таблица 75. Стандартные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности			
	Максимальное быстродействие	Рекомендуемый	Максимальная защита	Только сообщать
Защита объектов	По расширению	По формату	По формату	По формату
Проверка только новых и измененных файлов	Включено	Включено	Выключено	Включено
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Только сообщать
Действия над возможно зараженными объектами	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.	Только сообщать

Системно-критические объекты (СКО) нельзя удалить и процессы, относящиеся к таким объектам, не могут быть прекращены. СКО - это файлы, необходимые для работы операционной системы и Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

Параметры	Уровень безопасности			
	Максимальное быстродействие	Рекомендуемый	Максимальная защита	Только сообщать
Исключать файлы	Нет	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен	8 МБ
Альтернативные потоки NTFS	Да	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	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	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные
Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой	Нет	Нет	Да	Нет

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** и **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените параметры безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** или **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

kaspersky

Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*

- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*

- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

Параметры задачи Постоянная защита файлов по умолчанию

По умолчанию в задаче Постоянная защита файлов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 76. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Защищаемое устройство целиком, исключая виртуальные диски.	Используйте этот параметр, чтобы изменить область защиты.
Параметры безопасности	Единые для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла.
Режим защиты объектов	**Интеллектуальный режим**	Этот параметр используется, чтобы указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать эвристический анализатор, а также регулировать уровень анализа.
Применять доверенную зону	Применяется.	Единый список исключений, который можно применять в выбранных задачах.
Использовать KSN для защиты	Применяется.	Используйте этот параметр, чтобы повысить эффективность защиты устройства с помощью облачных служб Kaspersky Security Network (доступных, если принято Положение о KSN).
Расписание запуска задачи	При запуске программы.	Этот параметр используется, чтобы настроить запуск задачи по расписанию.
Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность	Не применяется.	Этот параметр используется, чтобы заблокировать текущий сеанс и добавить IP-адрес или локально уникальный идентификатор (LUID) узла, для которого была обнаружена вредоносная активность, в раздел Хранилище заблокированных хостов.
Запустить сканирование важных областей при обнаружении активного заражения	Применяется.	При обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes создает и запускает временную задачу Проверка важных областей.

kaspersky

Управление задачей Постоянная защита файлов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам политики для задачи Постоянная защита файлов

► *Чтобы перейти к параметрам задачи Постоянная защита файлов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

Если защищаемый компьютер работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров задачи Постоянная защита файлов для отдельного устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В блоке **Задачи** выберите задачу **Постоянная защита файлов**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

Настройка задачи Постоянная защита файлов

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Параметры перехвата** (см. раздел "**Выбор режима защиты**" на стр. 508)
     - **Эвристический анализатор** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 509)
     - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 509)

- На закладке **Управление задачей**:
  - Запуск задачи по расписанию (см. раздел "Настройка расписания задач" на стр. 404).

3. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Формирование области защиты" на стр. 528).
     - В открывшемся окне выберите, что требуется включить в область защиты задачи:
       - **Предопределенная область**
       - **Диск, папка или сетевой объект**
       - **Файл**
     - Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 499) или настройте параметры защиты вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 514).
4. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Выбор режима защиты

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**

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

- **При открытии и изменении**

  Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

  Этот вариант выбран по умолчанию.

- **При открытии**

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

- **При выполнении**

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

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

3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

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

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. На закладке **Общие** 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.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

   - Установите или снимите флажок **Применить 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 для задачи.

     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.

   - Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

- Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.

  Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Industrial CyberSecurity for Nodes удаляет эту временную задачу.

  Если флажок не установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes не создает и не запускает задачу Проверка важных областей.

  По умолчанию флажок установлен.

5. 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.

Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Плагина управления, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.

- **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
- **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
- **После обновления баз программы**, если вы 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, дату и время запуска задачи, отобразится расчетное время очередного запуска задачи.
Перейдите на закладку **Расписание** и откройте окно **Параметры задачи**. В поле **Следующий запуск** в верхней части окна отображается расчетное время запуска. Расчетное время следующего запуска задачи обновляется каждый раз, когда вы открываете окно.
В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 373) запрещен действующей политикой Kaspersky Security Center.

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

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389)".

kaspersky

Создание и настройка области защиты задачи

► *Чтобы создать и настроить область защиты задачи в Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. Выберите закладку **Область защиты**.

   Все элементы, на которые распространяется область защиты задачи, перечислены в таблице **Область защиты**.
3. Нажмите на кнопку **Добавить**, чтобы добавить в список новый элемент.

   Откроется окно **Добавление в область защиты**.
4. Выберите тип объектов для добавления в область защиты:
   - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
   - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
   - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

     Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.
5. Чтобы исключить отдельные элементы из области защиты, снимите флажки рядом с именами этих элементов или выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
6. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
7. Чтобы скрыть добавленную ранее область защиты или исключение в списке сетевых файловых ресурсов, в контекстном меню требуемой области защиты выберите пункт **Удалить область**.

   Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.
8. Нажмите на кнопку **OK**.

Окно Параметры области защиты закроется. Настроенные параметры будут сохранены.

Задачу **Постоянная защита файлов** можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранного в дереве файловых ресурсов узла можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. 507) **Свойства: Постоянная защита файлов**.
2. Выберите закладку **Область защиты**.
3. В списке защищаемых компьютеров выберите элемент, включенный в область защиты, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Свойства: Постоянная защита файлов**.

   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 задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 499) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. На закладке **Область защиты** выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
3. На закладке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями:
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 515)
   - Действия (см. раздел "Настройка действий" на стр. 518)
   - Производительность (см. раздел "Настройка производительности" на стр. 520)
5. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Новые параметры области защиты будут сохранены.

В этом разделе

Настройка общих параметров задачи

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

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите типы объектов, которые вы хотите включить в область защиты:
   - **Все объекты**

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

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

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

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

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

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

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет и защищает файлы, независимо от того, когда они были изменены.

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

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **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 проверяет архивы.

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

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка самораспаковывающихся архивов.

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

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

     Значение по умолчанию зависит от выбранного уровня защиты.

     Параметр доступен, 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 проверяет файлы почтовых баз.

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

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

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

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

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

     Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

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

  Если флажок не установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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 параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**.

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

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

     - **Лечить**
     - **Лечить. Удалять, если не удалось**.**Лечить. Удалять, если не удалось**
     - **Удалять**.

       Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**.

  Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**.

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

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

     - **Помещать на карантин**
     - **Удалять**.

       Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

     - **Рекомендуемое**.

       Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

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, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Industrial CyberSecurity for Nodes не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.

b. Нажмите на кнопку **Настройка**.

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

d. Нажмите на кнопку **OK**.

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

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

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

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

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

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

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 506).
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 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии

https://encyclopedia.kaspersky.ru/knowledge/classification/.

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

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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, продолжительность проверки не ограничена.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

  Исключение из проверки объектов больше указанного размера.

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

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

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

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

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

Управление задачей Постоянная защита файлов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну общих параметров задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Переход к параметрам области действия задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров области защиты для задачи Постоянная защита файлов, выполните следующие действия.*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

Настройка задачи Постоянная защита файлов

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 523).
2. На закладке **Общие** настройте следующие параметры задачи:
   - **Режим защиты объектов** (см. раздел "**Выбор режима защиты объектов**" на стр. 524)
   - **Эвристический анализатор** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 525)
   - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 525)
3. На закладках **Расписание** и **Дополнительно** настройте расписание задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
4. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.
5. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
6. Выполните следующие действия:
   - В дереве или списке файловых ресурсов устройства выберите узлы или элементы, которые вы хотите включить в область защиты задачи.

- Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 499) или настройте параметры защиты объекта вручную (см. раздел "Настройка параметров безопасности" на стр. 594).

7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 523).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**

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

     Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

     Этот вариант выбран по умолчанию.
   - **При открытии**

     Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии на чтение, выполнение и изменение.
   - **При выполнении**

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

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

3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

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

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 523).
2. На закладке **Общие** 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.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
4. В разделе **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 для задачи.

  По умолчанию флажок установлен.

  По ссылке **Доверенная зона** перейдите к параметрам доверенной зоны.

- 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.

- Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

  Флажок включает или выключает блокировку текущего сеанса и контролирует доступность общих сетевых ресурсов в рамках текущего сеанса.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes блокирует текущий сеанс и в рамках текущего сеанса делает недоступными общие сетевые ресурсы для узлов, для которых обнаружена вредоносная активность в разделе Хранилище заблокированных узлов.

  Если флажок снят, условия не применяются и Kaspersky Industrial CyberSecurity for Nodes работает в обычном режиме.

  По умолчанию флажок снят.

  Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

  Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

- Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.

  Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Industrial CyberSecurity for Nodes удаляет эту временную задачу.

  Если флажок не установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes не создает и не запускает задачу Проверка важных областей.

По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Настройка параметров расписания задач

В Консоли программы можно настроить расписание запуска локальных системных и пользовательских задач. Однако настроить расписание запуска групповых задач нельзя.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, для которой требуется настроить расписание.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Выполните следующие действия, чтобы настроить расписание:
   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась с периодичностью в заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, чтобы задача запускалась с периодичностью в заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, чтобы задача запускалась с периодичностью в заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
      - **После обновления баз программы**, 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 первого запуска задачи.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию запрещен действующей политикой Kaspersky Security Center.

5. На закладке **Дополнительно** настройте следующие параметры расписания:
   - В разделе **Параметры остановки задачи**:
     a. Установите флажок **Длительность**. В полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с**. В полях справа укажите, когда требуется приостановить и возобновить выполнение задачи (в рамках 24 часов).
   - В блоке **Дополнительные параметры**:
     c. Установите флажок **Отменить с** и укажите дату прекращения действия расписания.
     d. Установите флажок **Запускать пропущенные задачи**, чтобы запускать пропущенные задачи.
     e. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **ОК**.

Параметры расписания задачи будут сохранены.

Формирование области защиты

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

В этом разделе

Настройка отображения сетевых файловых ресурсов

► *Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области защиты, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

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

Формирование области защиты

Процедура формирования области действия задачи Постоянная защита файлов зависит от выбранного отображения сетевых файловых ресурсов (см. раздел "Об области защиты и параметрах безопасности задачи" на стр. 497). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

Чтобы применить к задаче новые параметры области защиты, нужно перезапустить задачу Постоянная защита файлов.

► *Чтобы сформировать область защиты с помощью дерева сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. 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 названием нужного типа дисков. Например, чтобы включить все съемные диски устройства, установите флажок **Съемные диски**.

- Если вы хотите включить в область защиты отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного 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.

4. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

► *Чтобы сформировать область защиты с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В окне **Добавление области защиты** выберите тип объектов, который вы хотите включить в область защиты:
      - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
      - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
      - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

   Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

3. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
4. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.

5. Чтобы скрыть добавленную ранее область защиты или исключения в списке сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

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

6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

Задачу Постоянная защита файлов можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Если указана сложная область защиты, например, заданы разные значения параметров безопасности для отдельных узлов в дереве файловых ресурсов устройства, это может привести к замедлению проверки объектов при доступе к ним.

Включение сетевых объектов в область защиты

Вы можете включать в область защиты сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► *Чтобы включить в область защиты сетевой объект, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, чтобы добавить сетевую папку в область защиты.
   - Выберите пункт **Добавить сетевой файл**, чтобы добавить сетевой файл в область защиты.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention).
5. Нажмите на клавишу **ENTER**.
6. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область защиты.
7. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Формирование виртуальной области защиты

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 590).

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню узла **Виртуальные диски**.
4. Выберите пункт **Добавить виртуальный диск**.
5. В списке доступных имен выберите имя создаваемого виртуального диска.
6. Установите флажок рядом с диском, чтобы включить его в область защиты.
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, чтобы добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, чтобы добавить виртуальный файл в область защиты.
4. В поле ввода задайте имя папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
6. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 499) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

При работе с деревом файловых ресурсов защищаемого 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. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 432).

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 529), создать область защиты (см. раздел "Формирование области защиты" на стр. 529) и создать виртуальную область защиты (см. раздел "Формирование виртуальной области защиты" на стр. 532).
3. В правой части окна выполните одно из следующих действий:
   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. 533).
   - На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
     - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 534)
     - **Действия** (см. раздел "**Настройка действий**" на стр. 537)
     - **Производительность** (см. раздел "**Настройка производительности**" на стр. 539)
4. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Новые параметры области защиты будут сохранены.

В этом разделе

Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранных в дереве или списке файловых ресурсов защищаемого компьютера узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. В дереве или в списке сетевых файловых ресурсов защищаемого компьютера выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область защиты.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

Настройка общих параметров задачи

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите объекты, которые требуется включить в область защиты:
   - **Все объекты**

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

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

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

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

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

     Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

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

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет и защищает файлы, независимо от того, когда они были изменены.

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

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **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 проверяет архивы.

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

     Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

  Проверка самораспаковывающихся архивов.

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

  Параметр доступен, 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 проверяет файлы почтовых баз.

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

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

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

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

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

  Если флажок не установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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 "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.
   - **Блокировать доступ**.

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

     Выберите действие из раскрывающегося списка:
     - **Лечить**
     - **Лечить. Удалять, если не удалось**.**Лечить. Удалять, если не удалось**
     - **Удалять**.

       Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.
     - **Рекомендуемое**.

       Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**.

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

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

     - **Помещать на карантин**
     - **Удалять**.

       Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

     - **Рекомендуемое**.

       Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

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, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Industrial CyberSecurity for Nodes не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

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

   d. Нажмите на кнопку **OK**.

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

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

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

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

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 523).
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 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

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

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

     Исключение из проверки объектов больше указанного размера.

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

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

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

   - **Использовать технологию iSwift**

     iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

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

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

     По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Industrial CyberSecurity for Nodes с момента запуска задачи.

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

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

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

Вы можете просмотреть информацию об объектах, обработанных Kaspersky Industrial CyberSecurity for Nodes с момента запуска задачи (см. таблицу ниже).

Таблица 77. Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes. Например, если программа Kaspersky Industrial CyberSecurity for Nodes обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes признала зараженными, или количество обнаруженных легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes не вылечила по следующим причинам: • Тип обнаруженного объекта не предполагает лечения. • При лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.
Объектов не удалено	Количество объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось удалить, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программе Kaspersky Industrial CyberSecurity for Nodes не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места 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.
Помещено на карантин	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes поместила на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Industrial CyberSecurity for Nodes.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Industrial CyberSecurity for Nodes пропустила, так как эти объекты защищены паролем.

Поле	Описание
Поврежденных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Industrial CyberSecurity for Nodes.

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в разделе **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**.

Управление задачей Постоянная защита файлов с помощью Веб-плагина

В этом разделе описано управление задачей Постоянная защита файлов с помощью интерфейса Веб-плагина.

В этом разделе

Настройка задачи Постоянная защита файлов

С помощью Веб-плагина нельзя изменить стандартный уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. 514) для задачи Постоянная защита файлов.

► *Чтобы настроить задачу Постоянная защита файлов с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.

5. Нажмите на кнопку **Параметры** в подразделе **Постоянная защита файлов**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 78. Параметры задачи Постоянная защита файлов

Параметр	Описание
Интеллектуальный режим	Kaspersky Industrial CyberSecurity for Nodes выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Industrial CyberSecurity for Nodes повторно проверяет объект только после его последнего сохранения этим процессом.
При открытии	Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии на чтение, выполнение и изменение.
При открытии и изменении	Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен. Этот вариант выбран по умолчанию.
При выполнении	Kaspersky Industrial CyberSecurity for Nodes проверяет файл только при открытии на выполнение.
Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)	Kaspersky Industrial CyberSecurity for Nodes выполняет более длительный анализ запускаемых процессов с большей вероятностью обнаружения угрозы. Запуск процесса блокируется до завершения анализа.
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.

Параметр	Описание
Уровень эвристического анализа	Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки. Существуют следующие уровни чувствительности проверки: • **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний. Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
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 для задачи. По умолчанию флажок установлен.

Параметр	Описание
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.
Блокировать доступ к сетевым файловым ресурсам для сетевых сессий, с которых ведется вредоносная активность	Флажок включает или выключает блокировку текущего сеанса и контролирует доступность общих сетевых ресурсов в рамках текущего сеанса. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes блокирует текущий сеанс и в рамках текущего сеанса делает недоступными общие сетевые ресурсы для узлов, для которых обнаружена вредоносная активность в разделе Хранилище заблокированных узлов. Если флажок снят, условия не применяются и Kaspersky Industrial CyberSecurity for Nodes работает в обычном режиме. По умолчанию флажок снят. Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов. Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.
Запустить сканирование важных областей при обнаружении активного заражения	Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Industrial CyberSecurity for Nodes удаляет эту временную задачу. Если флажок не установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes не создает и не запускает задачу Проверка важных областей. По умолчанию флажок установлен.

Параметр	Описание
Использовать Kaspersky Sandbox для защиты	Этот флажок включает или выключает использование Kaspersky Sandbox. Если флажок установлен, Kaspersky Endpoint Agent отправляет объекты в Kaspersky Sandbox. Kaspersky Sandbox анализирует поведение этих объектов, чтобы выявить вредоносную активность и признаки таргетированных атак. Если флажок снят, задача не отправляет объекты в Kaspersky Sandbox. По умолчанию флажок снят.
Область защиты	Можно настроить параметры безопасности для области защиты (см. раздел "Настройка параметров безопасности вручную" на стр. 514).

Настройка области защиты для задачи

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Постоянная защита файлов**.
6. Выберите раздел **Область защиты**.
7. Выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
   - Выберите существующее правило и нажмите на кнопку **Изменить**.

   Откроется окно **Изменить область**.
8. Установите переключатель в положение **Активный** и выберите тип объекта.
9. В разделе **Защита объектов** настройте следующие параметры:
   - **Режим защиты объектов**:
     - **Все объекты**

       Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.

- **Объекты, проверяемые по формату**

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

  Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

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

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

10. В разделе **Защита объектов** установите или снимите флажок **Проверка только новых и измененных файлов**.

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

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

    Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет и защищает файлы, независимо от того, когда они были изменены.

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

11. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Архивы**

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

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

- **SFX-архивы**

  Проверка самораспаковывающихся архивов.

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

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

- **Упакованные объекты**

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

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Почтовые базы**

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

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

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

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Файлы почтовых форматов**

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

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

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

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Вложенные OLE-объекты**

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

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

  Если флажок не установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

- Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой

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

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

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

12. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**.

  Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

  Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

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

- **Выполнять дополнительное действие**

  Выберите действие из раскрывающегося списка:

  - **Лечить**
  - **Лечить. Удалять, если не удалось**.**Лечить. Удалять, если не удалось**

- **Удалять**.

  Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**.

  Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

13. Выберите действие над возможно зараженными объектами:

- **Только сообщать**.

  Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

  Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

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

- **Выполнять дополнительное действие**

  Выберите действие из раскрывающегося списка:

  - **Помещать на карантин**

  - **Удалять**.

    Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

  - **Рекомендуемое**.

    Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

14. 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, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Industrial CyberSecurity for Nodes не позволит открыть или запустить зараженный объект независимо от вашего выбора.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

По умолчанию флажок снят.

b. Нажмите на кнопку **Настройка**.

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

d. Нажмите на кнопку **ОК**.

15. В разделе **Исключения** настройте следующие параметры:

- 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 пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

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

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

  По умолчанию флажок снят.

16. В разделе **Оптимизация** настройте следующие 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, продолжительность проверки не ограничена.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

  Исключение из проверки объектов больше указанного размера.

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

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

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

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

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

17. Нажмите на кнопку **OK**.

kaspersky

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 проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Industrial CyberSecurity for Nodes проверяет файлы и оперативную память защищаемого компьютера, а также объекты автозапуска.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Industrial CyberSecurity for Nodes создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет их резервными копиями.

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

Задача Проверка при старте операционной системы может не выполняться, если защищаемое устройство выходит из спящего режима или режима гибернации. Задача выполняется только при перезагрузке защищаемого устройства или при его запуске после полного выключения.

- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы в системных папках, например, в папке %windir%\system32. Kaspersky Industrial CyberSecurity for Nodes применяет параметры безопасности, соответствующие рекомендуемому уровню (см. раздел "Стандартные уровни безопасности" на стр. 560). Вы можете изменять параметры задачи Проверка важных областей.
- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Industrial CyberSecurity for Nodes на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом компьютере.

Kaspersky Industrial CyberSecurity for Nodes может одновременно выполнять несколько задач проверки по требованию.

kaspersky

Об области проверки и параметрах безопасности задачи

В Консоли программы область проверки выбранной задачи проверки по требованию представляет собой дерево или список файловых ресурсов защищаемого компьютера, которые может контролировать Kaspersky Industrial CyberSecurity for Nodes. По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы включить отображение сетевых файловых ресурсов в виде дерева в Консоли программы,*

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

Элементы и узлы в дереве или списке файловых ресурсов защищаемого 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.

С помощью Консоли программы можно также добавлять виртуальные диски (см. раздел "Создание виртуальной области проверки" на стр. 593) в область проверки. Имена виртуальных узлов отображаются шрифтом синего цвета.

Параметры безопасности

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию параметры безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

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

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

Стандартные области проверки

Дерево или список файловых ресурсов зачищаемого устройства для выбранной задачи проверки по требованию отображается в окне **Настройка области проверки**.

> В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие стандартные области проверки:

- **Мой компьютер**. Kaspersky Industrial CyberSecurity for Nodes проверяет защищаемый компьютер целиком.
- **Локальные жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты на жестких дисках защищаемого 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 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, используемая для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются с правами системной учетной записи.

  > Подключенные сетевые диски также не отображаются в дереве файловых ресурсов защищаемого компьютера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Системная память**. Kaspersky Industrial CyberSecurity for Nodes проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули, которые автоматически запускаются при запуске защищаемого устройства.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом компьютере.

- **Виртуальные диски**. Вы можете включать в область проверки виртуальные папки, файлы и диски, подключенные к защищаемому компьютеру, например, общие диски кластера.

  Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого компьютера в Консоли программы. Чтобы проверить объекты на виртуальном диске, включите в область проверки папку на защищаемом компьютере, с которой связан этот виртуальный диск.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов. Они доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**.
  - **Съемные диски**.
  - **Системная память**.
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows).
  - **Съемные диски**.
  - **Системная память**.
  - **Объекты автозапуска**.
- Прочие задачи:
  - **Локальные жесткие диски** (исключая папки Windows).
  - **Съемные диски**.
  - **Системная память**.
  - **Объекты автозапуска**.
  - **Папки общего доступа**.

Проверка файлов в интернет-хранилище

Об облачных файлах

Kaspersky Industrial CyberSecurity for Nodes может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы из OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Industrial CyberSecurity for Nodes не поддерживает другие интернет-хранилища.

Функция "файлы из OneDrive по запросу" помогает получить доступ к вашим файлам OneDrive без необходимости загружать их и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы из OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

Этот значок показывает, что файл доступен *только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, не удастся открыть файлы, доступные только через интернет.

Этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ( ).

Этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

Проверка облачных файлов

Kaspersky Industrial CyberSecurity for Nodes может выполнять проверку только облачных файлов, сохраненных локально на защищаемом компьютере. Такие файлы OneDrive имеют статус или . Проверка файлов со статусом не выполняется, поскольку физически они не хранятся на защищаемом компьютере.

Во время проверки Kaspersky Industrial CyberSecurity for Nodes не выполняет автоматическую загрузку файлов со статусом из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Industrial CyberSecurity for Nodes в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область задачи Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан задачей Постоянная защита файлов.
- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.

- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами и с помощью задачи Формирование правил контроля запуска программ. Задача Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

  Задача Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

Стандартные уровни безопасности

Параметры безопасности **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** не входят в набор параметров стандартных уровней безопасности. При изменении параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов**, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов узла можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый**, **Максимальная защита** или **Только сообщать**. Каждый из этих уровней имеет свои стандартные параметры безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Industrial CyberSecurity for Nodes на защищаемых компьютерах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

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

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Только сообщать

Уровень безопасности **Только уведомлять** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

Таблица 79. Стандартные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности			
	Максимальное быстродействие	Рекомендуемый	Максимальная защита	Только сообщать
Проверка объектов	По формату	Все объекты	Все объекты	Все объекты
Проверка только новых и измененных файлов	Включено	Выключено	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.	Только сообщать
Действия над возможно зараженными объектами	Карантин	Выполнять рекомендованное действие (Поместить на карантин)	Карантин	Только сообщать

Системно-критические объекты (СКО) нельзя удалить и процессы, относящиеся к таким объектам, не могут быть прекращены. СКО – это файлы, необходимые для работы операционной системы и Kaspersky Industrial CyberSecurity for Nodes.

Параметры	Уровень безопасности			
	Максимальное быстродействие	Рекомендуемый	Максимальная защита	Только сообщать
Исключать файлы	Нет	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	Нет	Нет	Нет
Не проверять составные объекты размером более (МБ)	8 МБ	Нет	Нет	Нет
Альтернативные потоки NTFS	Да	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да	Да
Проверка составных объектов	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • Почтовые базы* • Файлы почтовых форматов* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты

Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключенных к защищаемому компьютеру по USB.

Kaspersky Industrial CyberSecurity for Nodes выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу проверки по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Kaspersky Industrial CyberSecurity for Nodes запускает проверку подключенных съемных дисков при их регистрации в операционной системе в качестве внешних устройств, подключаемых по USB. Программа не выполняет проверку съемного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к съемному диску на время проверки.

Результаты проверки каждого съемного диска доступны в журнале выполнения задачи проверки по требованию, созданной при подключении этого съемного диска.

Вы можете изменять значения параметров компонента Проверка съемных дисков (см. таблицу ниже).

Таблица 80. Параметры проверки съемных дисков

Параметр	Значение по умолчанию	Описание
Проверять съемные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	8192 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на проверяемом диске. Kaspersky Industrial CyberSecurity for Nodes не выполняет проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • **Максимальная защита** • **Рекомендуемый** • **Максимальное быстродействие** Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию.

kaspersky

О задаче Мониторинг целостности файлов на основе эталона

Во время выполнения задачи Мониторинг целостности файлов на основе эталона Kaspersky Industrial CyberSecurity for Nodes не проверяет заблокированные файлы, папки, ярлыки файлов и облачные файлы.

В задаче Мониторинг целостности файлов на основе эталона выполняется контроль целостности файлов в области мониторинга посредством сравнения хеша файлов (MD5 или SHA256) с эталонным значением.

При первом запуске задачи Мониторинг целостности файлов на основе эталона, Kaspersky Industrial CyberSecurity for Nodes создает эталон, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При изменении области задачи Мониторинг целостности файлов на основе эталона, Kaspersky Industrial CyberSecurity for Nodes обновляет эталон при следующем запуске задачи Мониторинг целостности файлов на основе эталона, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При удалении задачи Мониторинг целостности файлов на основе эталона, Kaspersky Industrial CyberSecurity for Nodes удаляет эталон этой задачи.

С помощью командной строки можно удалить эталон (см. раздел "Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE" на стр. 1029), не удаляя задачу Мониторинг целостности файлов на основе эталона.

Задача Мониторинг целостности файлов на основе эталона отслеживает следующие изменения файлов в области мониторинга:

- область мониторинга содержит файл, который отсутствует в эталоне;
- в области мониторинга отсутствует файл, который присутствует в эталоне;
- хеш файла в области мониторинга отличается от хеша этого файла в эталоне.

Задача Мониторинг целостности файлов на основе эталона не отслеживает изменения атрибутов файлов и изменения альтернативных потоков.

Если файл или папка недоступны, Kaspersky Industrial CyberSecurity for Nodes не добавляет этот файл или папку в эталон при создании, а формирует событие о невозможности рассчитать хеш при запуске задачи Мониторинг целостности файлов на основе эталона.

Файл или папка могут быть недоступны по следующим причинам:

- указанный путь не существует;
- тип файлов, указанный в маске, отсутствует по указанному пути;
- указанный файл заблокирован;
- указан пустой файл.

kaspersky

Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать локальные системные и пользовательские задачи проверки по требованию.

Таблица 81. Заданные по умолчанию параметры задач проверки по требованию

Параметр	Значение по умолчанию	Описание
Область проверки	Применяется в следующих локальных системных и пользовательских задачах: • **Проверка при старте операционной системы**: защищаемое устройство целиком, за исключением папок общего доступа и объектов автозапуска. • **Проверка важных областей**: защищаемое устройство целиком, за исключением папок общего доступа и некоторых файлов операционной системы. • **Проверка по требованию** (пользовательские задачи): защищаемое устройство целиком.	Вы можете изменить область проверки. Область проверки нельзя настроить для локальных системных задач **Проверка объектов на карантине** и **Проверка целостности программы**. Задача **Проверка при старте операционной системы** создается автоматически после установки. По умолчанию применяется режим **Только уведомлять**. В этом случае после развертывания Kaspersky Industrial CyberSecurity for Nodes на устройствах можно включить задачу **Проверка при старте операционной системы**, если во время проверки не было обнаружено проблем с сервисами операционной системы. Если программа определяет, что критические сервисы операционной системы являются зараженными или возможно зараженными, режим **Только уведомлять** позволяет выяснить причину и решить проблему. Если программа применяет режим **Выполнять рекомендуемое действие**, выполняется действие **Лечить.** Действие **Удалять, если не удалось вылечить**, лечение или удаление системных файлов могут привести к критическим проблемам при запуске операционной системы.

Параметр	Значение по умолчанию	Описание
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла.
Использовать эвристический анализатор	Применяется с уровнем анализа **Средний** для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач. Применяется с уровнем анализа **Глубокий** для задачи Проверка объектов на карантине.	Вы можете включать и выключать применение эвристического анализатора и регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Эвристический анализатор не используется в задачах Проверка целостности программы и Мониторинг целостности файлов на основе эталона.
Применять доверенную зону	Применяется (не применяется для задачи Проверка объектов на карантине)	Единый список исключений, который можно применять в выбранных задачах.
Использовать KSN для проверки	Применяется.	Вы можете увеличить эффективность защиты устройства с помощью инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с определенными правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска задач с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.
Выполнять задачу в фоновом режиме (низкий приоритет)	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.

Параметр	Значение по умолчанию	Описание
Расписание запуска задачи	Применяется в локальных 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 – **Ежесуточно**. Не применяется во вновь созданных пользовательских задачах.	Можно настроить параметры для запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты устройства	Статус защиты устройства 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; • изменяя область проверки задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

Управление задачами проверки по требованию с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

kaspersky

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к мастеру создания задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Для создания локальной задачи:
   a. Разверните узел **Управляемые устройства** в Консоли администрирования Kaspersky Security Center.
   b. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
   c. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства.
   d. Выберите пункт меню **Свойства**.
   e. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.
2. Для создания групповой задачи:
   a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
   b. Выберите группу администрирования, для которой требуется создать задачу.
   c. Выберите закладку **Задачи**.
   d. Нажмите на кнопку **Создать задачу**.

Откроется окно **Мастер создания задачи**.

3. Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:

   a. В Консоли администрирования Kaspersky Security Center в панели результатов узла **Выборки устройств** нажмите на кнопку **Запустить выборку**, чтобы выбрать устройства.

   b. Выберите закладку **Результаты выборки "имя выборки"**.

   c. В раскрывающемся списке **Сделать выборку** выберите вариант **Создать задачу для результатов выборки**.

   Откроется окно **Мастер создания задачи**.

4. Выберите задачу **Проверка по требованию** в списке доступных задач для Kaspersky Industrial CyberSecurity for Nodes.
5. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

Настройте параметры задачи в соответствии с вашими требованиями.

► *Чтобы настроить задачу проверки по требованию,*

откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач Kaspersky Security Center.

Откроется окно **Свойства: Проверка по требованию**.

Переход к свойствам задачи проверки по требованию

► *Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите закладку **Устройства**.
4. Дважды щелкните мышью по имени защищаемого устройства, для которого вы хотите настроить область проверки.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. Выберите раздел **Задачи**.
6. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
7. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Проверка по требованию**.

Настройте параметры задачи в соответствии с вашими требованиями.

kaspersky

Создание задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка** (см. раздел "**Переход к мастеру создания задачи проверки по требованию**" на стр. 568) в мастере создания задачи.
2. Выберите требуемый **Способ создания задачи**.
3. Нажмите на кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки.

   По умолчанию область проверки включает критические области защищаемого компьютера. Проверяемые области помечены в таблице значком ☑. Области, являющиеся исключениями из проверки, помечены в таблице значком ☐.
   Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

   - Чтобы исключить из проверки все важные области, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
   - Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
     a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить область** или нажмите на кнопку **Добавить**.
     b. В окне **Добавление в область проверки** выберите стандартную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом компьютере в сети и нажмите на кнопку **ОК**.
   - Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:
     a. Откройте контекстное меню и выберите пункт **Настроить**.
     b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
     c. На закладке **Общие** в окне **Настройка проверки по требованию** снимите флажки **Вложенные папки** и **Вложенные файлы**.
   - Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
     a. Откройте контекстное меню области проверки, параметры которой требуется изменить, и выберите пункт **Настроить**.
     b. В окне **Настройка проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

     Параметры безопасности настраиваются таким же образом, как и для задачи Постоянная защита файлов (см. раздел "Настройка параметров безопасности вручную" на стр. 514).

- Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:

  a. Откройте контекстное меню таблицы **Область проверки** и выберите пункт **Добавить исключение**.

  b. Укажите объекты, которые вы хотите исключить: выберите стандартную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на защищаемом компьютере или другом защищаемом устройстве сети.

  c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:

   - Настройте применение эвристического анализатора (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. 509).
   - Установите флажок **Применить Доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в 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 для задачи.

     По умолчанию флажок установлен.

   - Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

     Этот 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 проверки по требованию не использует службы KSN.

     По умолчанию флажок установлен.

   - Чтобы присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*, в окне **Параметры** установите 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 защищаемого компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes и других программ. В результате скорость выполнения задачи уменьшается 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 и другие программы. В этом случае скорость выполнения задачи увеличивается.

По умолчанию флажок снят.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

- Чтобы использовать создаваемую задачу в качестве задачи Проверка важных областей, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых компьютеров по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Industrial CyberSecurity for Nodes. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок снят для пользовательских задач проверки по требованию.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** укажите параметры запуска задачи по расписанию.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
10. Нажмите на кнопку **Далее**.
11. Укажите название задачи.
12. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
13. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
14. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача проверки по требованию для выбранного защищаемого компьютера или группы защищаемых компьютеров.

kaspersky

В этом разделе

Присвоение задаче проверки по требованию статуса Проверка важных областей

По умолчанию Kaspersky Security Center присваивает защищаемому компьютеру статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано параметром для порога формирования события в Kaspersky Industrial CyberSecurity for Nodes – *Проверка важных областей защищаемого устройства давно не выполнялась*.

► *Чтобы настроить проверку всех защищаемых компьютеров, входящих в одну группу администрирования, выполните следующие действия:*

1. Создайте групповую задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 570).
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей**. Указанные параметры задачи (область проверки и параметры безопасности) будут применены ко всем защищаемым компьютерам в группе. Настройте расписание задачи.

   Флажок **Считать выполнение задачи проверкой важных областей** можно установить при создании задачи проверки по требованию для группы защищаемых устройств или позднее в окне **Свойства: <Название задачи>** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
3. С помощью новой или существующей политики выключите запуск по расписанию локальных системных задач проверки по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 373) для группы защищаемых компьютеров.

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого компьютера и уведомлять о нем по результатам последнего выполнения задачи со статусом Проверка важных областей, а не по результатам выполнения локальной системной задачи Проверка важных областей.

Вы можете присваивать статус *Проверка важных областей* как групповым задачам проверки по требованию, так и задачам для групп защищаемых устройств.

В Консоли программы можно также просмотреть, имеет ли задача проверки по требованию статус Проверка важных областей.

В Консоли программы флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задачи, но не доступен для редактирования.

kaspersky

Выполнение задач проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но может положительно повлиять на скорость выполнения процессов других запущенных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Можно указать максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к мастеру создания задачи проверки по требованию**" на стр. 568).
2. 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 защищаемого компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes и других программ. В результате скорость выполнения задачи уменьшается 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 и другие программы. В этом случае скорость выполнения задачи увеличивается.

   По умолчанию флажок снят.
3. 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 задачи Проверка важных областей

По умолчанию статус защиты устройства отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты устройства привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. По умолчанию флажок установлен только для задачи Проверка важных областей и недоступен для редактирования в этой задаче.

Вы можете выбрать задачу проверки по требованию, связанную со статусом защиты устройства, только в Kaspersky Security Center.

kaspersky

Настройка области проверки для задачи

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Industrial CyberSecurity for Nodes (**Пуск** > **Программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Изменение или удаление Kaspersky Industrial CyberSecurity for Nodes**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

► *Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. Чтобы включить элементы в область проверки:
   a. Откройте контекстное меню для списка областей проверки.
   b. В контекстном меню выберите пункт **Добавить область**.
   c. В открывшемся окне **Добавление в область проверки** выберите тип объектов, который вы хотите добавить:
      - **Предопределенная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
      - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
      - **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

   Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.
4. 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 окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
5. Чтобы изменить область проверки или исключение, в контекстном меню требуемой области проверки выберите пункт **Изменить область**.
6. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить область**.

Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

7. Нажмите на кнопку **OK**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узлов, выбранных в списке файловых ресурсов защищаемого компьютера, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. В списке защищаемых компьютеров выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
6. Нажмите на кнопку **OK**.
7. В окне **Свойства: Проверка по требованию** нажмите на кнопку **OK**.

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

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. В списке областей проверки выберите элементы, для которых вы хотите настроить параметры безопасности.

   К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 432). можно применить к выбранному узлу или элементу в области проверки.

4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

5. На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
   - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 577)
   - **Действия** (см. раздел "**Настройка действий**" на стр. 580)
   - **Производительность** (см. раздел "**Настройка производительности**" на стр. 582)
6. Нажмите на кнопку **OK** в окне **Настройка проверки по требованию**.
7. Нажмите на кнопку **OK** в окне **Область проверки**.

Новые параметры области проверки будут сохранены.

В этом разделе

Настройка общих параметров задачи

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

4. Нажмите на кнопку **Настройка**.

5. На закладке **Общие** в блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:

   - **Объекты проверки**:
     - **Все объекты**

       Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.

     - **Объекты, проверяемые по формату**

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

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

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

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по указанному списку расширений**

       Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

   - **Вложенные папки**
   - **Вложенные файлы**
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого компьютера.

     По умолчанию флажок установлен.

   - **Альтернативные потоки NTFS**

     Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

     Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

     Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

     По умолчанию флажок установлен.

6. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

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

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет и защищает файлы, независимо от того, когда они были изменены.

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

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

7. В блоке параметров **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 проверяет архивы.

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

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка самораспаковывающихся архивов.

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

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

     Значение по умолчанию зависит от выбранного уровня защиты.

     Параметр доступен, 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 проверяет файлы почтовых баз.

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

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

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

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

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

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

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

  Если флажок не установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия над зараженными и другими обнаруженными объектами во время выполнения задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Действия**.

6. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.
   - **Лечить**
   - **Лечить. Удалять, если не удалось**.**Лечить. Удалять, если не удалось**
   - **Удалять**.

     Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**
7. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.
   - **Помещать на карантин**
   - **Удалять**.

     Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**.

     Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

8. 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, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Industrial CyberSecurity for Nodes не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

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

   d. Нажмите на кнопку **OK**.

9. 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 принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

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

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

10. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 569).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Производительность**.
6. 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 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

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

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

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
7. 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, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки объектов больше указанного размера.

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

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

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

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

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка проверки съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому компьютеру, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

   В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

6. В блоке **Параметры проверки при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, 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 съемных дисков.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

Настройка задачи Мониторинг целостности файлов на основе эталона

► *Чтобы настроить групповую задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
5. В разделе **Область проверки** выполните следующие действия:
   a. Чтобы добавить папку в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.
      2. Установите или снимите флажок **Проверять эту область**.
      3. Нажмите на кнопку **Обзор**, чтобы указать папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
      4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.

b. Чтобы добавить или исключить добавленную ранее папку из области задачи Мониторинг целостности файлов на основе эталона, снимите или установите флажок слева от пути к папке в таблице **Область проверки**.

c. Чтобы удалить папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите папку в таблице **Область проверки** и нажмите на кнопку **Удалить**.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Управление задачами проверки по требованию с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

В этом разделе

kaspersky

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам задачи проверки по требованию

► *Чтобы перейти к общим параметрам задачи проверки по требованию в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Переход к параметрам области действия задачи проверки по требованию

► *Чтобы перейти к параметрам области проверки в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы 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**.

Создание и настройка задачи проверки по требованию

Вы можете создавать пользовательские задачи для отдельного защищаемого компьютера в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Industrial CyberSecurity for Nodes создание пользовательских задач не предусмотрено.

► *Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.

3. Настройте следующие параметры задачи:

   - **Имя** – название задачи, содержащее не более 100 символов. Допускаются 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 название задачи.

   - **Описание** – дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.

   - **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 защищаемого компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes и других программ. В результате скорость выполнения задачи уменьшается 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 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 для задачи.

     По умолчанию флажок установлен.

- **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых компьютеров по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Industrial CyberSecurity for Nodes. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок снят для пользовательских задач проверки по требованию.

- **Использовать KSN для проверки**.

  Этот 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 проверки по требованию не использует службы KSN.

  По умолчанию флажок установлен.

4. Настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425) на закладках **Расписание** и **Дополнительно**.
5. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
6. В окне **Добавить задачу** нажмите на кнопку **ОК**.

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 953).
7. Если требуется, в панели результатов выбранного узла выберите **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
8. В дереве или в списке файловых ресурсов защищаемого компьютера выберите узлы или элементы, которые вы хотите включить в область проверки.
9. Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 560) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности" на стр. 594).
10. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Настроенные параметры будут применены при последующем запуске задачи.

kaspersky

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

Настройка отображения сетевых файловых ресурсов

► *Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области проверки, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

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

Формирование области проверки

Если вы управляете Kaspersky Industrial CyberSecurity for Nodes на защищаемом компьютере удаленно, с помощью Консоли программы, установленной 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 изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Industrial CyberSecurity for Nodes (**Пуск** > **Программы** > **Kaspersky Industrial CyberSecurity for Nodes** > **Изменение или удаление Kaspersky Industrial CyberSecurity for Nodes**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от выбранного типа отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 590). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

► *Чтобы сформировать область проверки с помощью дерева сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. 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 проверки все диски определенного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски защищаемого компьютера, установите флажок **Съемные диски**).
     - Если вы хотите включить в область проверки отдельный диск определенного типа, разверните узел, который содержит диски этого типа, и установите флажок рядом с именем требуемого 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.
4. Нажмите на кнопку **Сохранить**.

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

► *Чтобы сформировать область проверки с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. Чтобы включить отдельные узлы в область проверки, 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 объектов, который вы хотите добавить:
      - **Предопределенная область**, если вы хотите включить в область проверки одну из предопределнный областей на защищаемом компьютере. Затем в раскрывающемся списке выберите требуемую область проверки.
      - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.

- **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.

3. 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 окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
4. Чтобы изменить добавленную область проверки или исключение, в контекстном меню нужной области проверки выберите пункт **Изменить область**.
5. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

6. 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 можете проверять сетевые папки при работе под системной учетной записью.

► *Чтобы включить в область проверки сетевой объект, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню 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.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.

5. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Можно включать в область проверки виртуальные диски, папки и файлы, таким образом создавая виртуальную область проверки.

Вы можете включить в область проверки отдельные виртуальные диски, папки или файлы, только если область проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 590).

► *Чтобы включить в область проверки виртуальный диск, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого компьютера откройте контекстное меню узла **Виртуальные диски**, выберите пункт **Добавить виртуальный диск** и в списке доступных имен выберите имя виртуального диска.
4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
5. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► *Чтобы включить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого компьютера откройте контекстное меню узла, в который вы хотите добавить папку или файл, и выберите один из следующих вариантов:
   - **Добавить виртуальную папку**, если вы хотите добавить виртуальную папку в область проверки.
   - **Добавить виртуальный файл**, если вы хотите добавить виртуальный файл в область проверки.
4. В поле ввода задайте имя для папки или файла.
5. В строке с именем папки или файла установите флажок, чтобы включить папку или файл в область проверки.
6. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

kaspersky

Настройка параметров безопасности

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого компьютера.

При работе с деревом сетевых файловых ресурсов 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. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В левой части окна выберите узел или элемент, параметры безопасности которого вы хотите настроить.

   Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 432) можно применить к выбранному узлу или элементу в области проверки.

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 590), создать область проверки (см. раздел "Формирование области проверки" на стр. 590) и создать виртуальную область проверки (см. раздел "Создание виртуальной области проверки" на стр. 593).
3. В правой части окна выполните одно из следующих действий:
   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задачах проверки по требованию" на стр. 595).
   - На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
     - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 595)
     - **Действия** (см. раздел "**Настройка действий**" на стр. 598)
     - **Производительность** (см. раздел "**Настройка производительности**" на стр. 600)
4. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Новые параметры области проверки будут сохранены.

В этом разделе

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для выбранных в дереве или списке файловых ресурсов защищаемого компьютера узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. В дереве или в списке сетевых файловых ресурсов защищаемого компьютера выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область проверки.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. Выберите закладку **Общие**.
3. В блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:
   - **Объекты проверки**:
     - **Все объекты**

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

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

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

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

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

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

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет и защищает файлы, независимо от того, когда они были изменены.

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

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

5. В блоке параметров **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 проверяет архивы.

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

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка самораспаковывающихся архивов.

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

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

     Значение по умолчанию зависит от выбранного уровня защиты.

     Параметр доступен, 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 проверяет файлы почтовых баз.

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

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

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

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

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

     Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

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

  Если флажок не установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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 "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.
   - **Лечить**
   - **Лечить. Удалять, если не удалось**.**Лечить. Удалять, если не удалось**
   - **Удалять**.

     Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Industrial CyberSecurity for Nodes автоматически изменит уровень безопасности на **Другой**.

   - **Помещать на карантин**

   - **Удалять**.

     Kaspersky Industrial CyberSecurity for Nodes удаляет объект и помещает его копию в резервное хранилище.

   - **Выполнять рекомендуемое действие**.

     Kaspersky Industrial CyberSecurity for Nodes выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

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, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Industrial CyberSecurity for Nodes не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

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

   d. Нажмите на кнопку **ОК**.

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 принудительное удаление родительского составного файла при обнаружении вредоносного, возможно зараженного или другого вложенного объекта.

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

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

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 "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 587).
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 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

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

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

     Исключение из проверки объектов больше указанного размера.

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

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

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

   - **Использовать технологию iSwift**

     iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

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

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

     По умолчанию флажок установлен.

   - **Использовать технологию iChecker**

     iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет только новые и измененные файлы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы независимо от даты их создания и изменения.

     По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Проверка съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому компьютеру в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

2. В блоке **Параметры проверки при подключении** выполните следующие действия:

   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, 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 съемных дисков.

3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

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 обработала с момента запуска задачи.

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 задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач" на стр. 957).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

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

В таблице ниже приведена информация об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes обработала с момента запуска задачи.

Таблица 82. Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes. Например, если программа Kaspersky Industrial CyberSecurity for Nodes обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes обнаружила и признала зараженными, или количество обнаруженных объектов, которые не были исключены из области проверки и были определены как легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes не вылечила по следующим причинам: • Тип обнаруженного объекта не предполагает лечения. • При лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.
Объектов не удалено	Количество объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось удалить, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программе Kaspersky Industrial CyberSecurity for Nodes не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места 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.
Помещено на карантин	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes поместила на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Industrial CyberSecurity for Nodes.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Industrial CyberSecurity for Nodes пропустила, так как эти объекты защищены паролем.

Поле	Описание
Поврежденных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Industrial CyberSecurity for Nodes.

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в разделе **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Создание и настройка задачи Мониторинг целостности файлов на основе эталона

► *Чтобы создать или настроить задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Диагностика системы**.
2. Выберите пункт **Создать задачу Мониторинг файловых операций**.

   Откроется окно **Добавить задачу**.
3. В раскрывающемся списке **Алгоритм расчета контрольных сумм** выберите один из следующих вариантов:
   - **MD5**
   - **SHA256**
4. В таблице **Области проверки** выполните следующие действия:
   a. Чтобы добавить файл или папку в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.
      2. Установите или снимите флажок **Проверять эту область**.
      3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
      4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.
      5. Нажмите на кнопку **ОК**.

   b. Чтобы поменять файл или папку, добавленную ранее в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Изменить**.

         Откроется окно **Область проверки**.

2. Установите или снимите флажок **Проверять эту область**.
3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
4. Установите или снимите флажок **Также проверять подпапки**, чтобы включить или исключить все вложенные папки из области задачи Мониторинг целостности файлов на основе эталона.
5. Нажмите на кнопку **ОК**.

c. Чтобы удалить файл или папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите этот файл или папку в таблице **Области проверки** и нажмите на кнопку **Удалить**.

5. Настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425) на закладках **Расписание** и **Дополнительно**.
6. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
7. В окне **Добавить задачу** нажмите на кнопку **ОК**.

   Будет создана пользовательская задача Мониторинг целостности файлов на основе эталона. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 953).

► *Чтобы просмотреть параметры задачи Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

kaspersky

Доверенная зона

Этот раздел содержит информацию о доверенной зоне Kaspersky Industrial CyberSecurity for Nodes, а также инструкции по добавлению объектов в доверенную зону при выполнении задач.

В этом разделе

О доверенной зоне

Доверенная зона – это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах Постоянная защита файлов, а также в задачах проверки по требованию.

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

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

- Исключения. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.
- Доверенные процессы. В доверенную зону помещаются объекты, чувствительные к перехватам файловых операций процессами программы.
- Операции резервного копирования. В доверенную зону помещаются объекты, доступ к которым выполняется при операциях резервного копирования жестких дисков на внешние устройства.

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов и в задачах проверки по требованию.

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

kaspersky

Исключения

Применяются в задачах Постоянная защита файлов и в задачах 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 по отдельности.

Вы можете добавлять исключения в доверенную зону по их расположению на защищаемом компьютере, по имени или маске имени обнаруженного объектаили использовать оба параметра.

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

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

Доверенные процессы

Могут применяться в задачах Постоянная защита файлов, Контроль запуска программ, Мониторинг файловых операций и Мониторинг доступа к реестру.

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

Чтобы не нарушать работу таких программ, вы можете выключить защиту файлов, 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. Названия некоторых из них приведены на веб-сайте Microsoft https://www.microsoft.com/ru-ru (код статьи: KB822158).

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

> Если исполняемый файл изменяется, например, в результате обновления, Kaspersky Industrial CyberSecurity for Nodes исключает его из списка доверенных процессов.

Программа не использует путь к файлу на защищаемом 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 можно выключить защиту объектов, доступ к которым осуществляется при операциях резервного копирования. Kaspersky Industrial CyberSecurity for Nodes будет проверять объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

О профилях исключения для промышленных программ

Профили исключения для промышленных программ – это набор правил конфигурации в формате XML, предназначенных для добавления процессов и файлов отдельных промышленных программ в списки доверенной зоны – списки доверенных процессов и исключений, а также для настройки правил и параметров Контроля запуска программ.

В следующей таблице перечислены все доступные профили исключения для промышленных программ.

Таблица 83. Профили исключения для промышленных программ

Название программы	Правила конфигурации доверенной зоны	Правила конфигурации Контроля запуска программ
ABB MicroSCADA	Да	Нет
PCУ ABB 800xA	Да	Нет
Bosch Building Integration System	Да	Нет
Bosch Rexroth MMS 4.0	Да	Нет
Emerson DeltaV	Да	Да
Emerson OpenEnterprise	Да	Да
Emerson Ovation	Да	Нет
Emerson PipelineManager	Да	Нет
GE Cimplicity	Да	Нет
Bently Nevada System 1	Да	Да
Honeywell Experion PKS	Да	Нет
Mitsubishi MAPS	Да	Нет
OMRON CX-Supervisor	Да	Нет
PcVue Solutions 15	Да	Да
Rockwell Automation FactoryTalk View	Да	Нет
Schneider Electric Citect SCADA	Да	Нет
Schneider Electric Clear SCADA	Да	Да

Название программы	Правила конфигурации доверенной зоны	Правила конфигурации Контроля запуска программ
РСУ Schneider Electric EcoStruxure Foxboro	Да	Нет
Schneider Electric EcoStruxture Triconex Safety Systems	Да	Нет
Schneider Electric Unity Pro	Да	Нет
Siemens SIMATIC PCS 7 v8.2	Да	Нет
Siemens SIMATIC PCS 7 v9.0	Да	Нет
Siemens SIMATIC PCS 7 v9.1	Да	Да
Siemens SIMATIC WinCC OA	Да	Да
Siemens SIMATIC WinCC	Да	Нет
Siemens SIMATIC STEP7	Да	Нет
Siemens TIA Portal	Да	Нет
Siemens DIGSI	Да	Нет
Siemens SICAM PAS	Да	Нет
Valmet DNA	Да	Да
Wonderware InTouch	Да	Нет
Wonderware System Platform 2017	Да	Нет
Yokogawa CENTUM VP	Да	Нет
Yokogawa ProSafe-RS	Да	Нет
Yokogawa FAST/TOOLS	Да	Нет
Alpha.Platform	Да	Да
VACS Standart	Да	Да
Tornado-N	Да	Да
РСУ NaftaProcess	Да	Да
Прософт-Системы – комплекс Redkit SCADA	Да	Да
ЭКРА (EKRASMS, EKRASMS-SP)	Да	Да

► *Чтобы применить профиль исключения для промышленных программ во время установки Kaspersky Industrial CyberSecurity for Nodes:*

выберите нужный профиль исключения на соответствующем шаге Мастера установки Kaspersky Industrial CyberSecurity for Nodes.

С помощью Мастера установки можно выбрать только один профиль исключения.

Профиль исключения для промышленных программ будет применен.

При применении профилей исключения во время установки параметры выбранного профиля объединяются с параметрами по умолчанию, заданными для доверенной зоны.

Управление доверенной зоной с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка доверенной зоны для одного или всех защищаемых компьютеров в сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам политики для доверенной зоны

► *Чтобы перейти к доверенной зоне в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.

4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
6. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Если защищаемый компьютер работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к окну параметров доверенной зоны

► *Чтобы настроить доверенную зону в окне свойств программы, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Industrial CyberSecurity for Nodes 3.2**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Industrial CyberSecurity for Nodes 3.2**.
7. Выберите раздел **Дополнительные возможности**.
8. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

kaspersky

Настройка параметров доверенной зоны с помощью Плагина управления

► *Чтобы настроить параметры доверенной зоны, выполните следующие действия:*

1. На закладке **Исключения** укажите объекты, которые Kaspersky Industrial CyberSecurity for Nodes пропускает (см. раздел "Добавление исключений" на стр. 612) при выполнении задачи.
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Industrial CyberSecurity for Nodes пропускает (см. раздел "Добавление доверенных процессов с помощью Плагина управления" на стр. 614) при выполнении задачи.
3. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 617).

В этом разделе

Добавление исключений

► *Чтобы добавить исключение в доверенную зону в политике Kaspersky Security Center:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 610).
2. На закладке **Исключения** укажите объекты, которые Kaspersky Industrial CyberSecurity for Nodes пропускает при проверке и защите:
   - Чтобы создать рекомендуемые исключения, нажмите на кнопку **Добавить рекомендуемые исключения**.

     При нажатии на эту кнопку в список исключений добавляются исключения, рекомендованные корпорацией Microsoft и "Лабораторией Касперского".
   - Чтобы импортировать предварительно настроенные исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Исключения из файла XML будут добавлены в список исключений.
   - Чтобы вручную указать условия, при выполнении которых объект считается доверенным, нажмите на кнопку **Добавить** и перейдите к следующим шагам.

     Откроется окно **Параметры правила исключения**.

3. Если вы нажали на кнопку **Добавить** в разделе **Не проверять объект при выполнении следующих условий**, укажите объекты, которые требуется исключить из области защиты или проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

   - Чтобы исключить объект из области защиты или проверки:

     a. Установите флажок **Объект, исключенный из проверки**.

        Добавляет файл, папку, диск или файл скрипта в исключения.

        Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Industrial CyberSecurity for Nodes, выбранных в разделе **Область применения правила**.

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Объект для исключения из проверки**.

     c. Выберите объект, который вы хотите исключить из области проверки.

        При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Industrial CyberSecurity for Nodes при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Industrial CyberSecurity for Nodes обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

     d. Нажмите на кнопку **ОК**.

     e. Установите флажок **Применять к подпапкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

   - Чтобы указать имя обнаруживаемого объекта:

     a. Установите флажок **Объекты, исключенные из обнаружения**.

        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 пропускает при проверке указанные объекты.

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

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Объекты для исключения из обнаружения**.

     c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

     d. Нажмите на кнопку **Добавить**.

     e. Нажмите на кнопку **ОК**.

4. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.
5. Нажмите на кнопку **ОК**.

Исключение отображается в списке на вкладке **Исключения** окна **Доверенная зона**.

Добавление доверенных процессов с помощью Плагина управления

► *Чтобы добавить один или несколько процессов в список доверенных с помощью Плагина управления:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 610).
2. Выберите вкладку **Доверенные процессы**.
3. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

   Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом компьютере.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом компьютере.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом компьютере.

   По умолчанию флажок установлен.
4. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.
5. Чтобы добавить процесс в список доверенных процессов, выполните одно из следующих действий:
   - Чтобы импортировать предварительно настроенные доверенные процессы, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Процессы из файла XML будут добавлены в список доверенных процессов.
   - Чтобы указать процессы вручную, нажмите на кнопку **Добавить** и перейдите к следующим шагам.
6. Если вы нажали на кнопку **Добавить**, в контекстном меню кнопки выберите один из следующих вариантов:

- **Несколько процессов**.

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

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

     Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

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

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует хеш выбранного файла для определения, является ли процесс доверенным.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  c. Чтобы добавить данные на основе исполняемых процессов, 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. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  h. Нажмите на кнопку **OK**.

     Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Industrial CyberSecurity for Nodes, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом компьютере. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

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

  В открывшемся окне **Добавление процесса** выполните следующие действия:

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

При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Industrial CyberSecurity for Nodes при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Industrial CyberSecurity for Nodes обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

b. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

c. Нажмите на кнопку **ОК**.

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

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

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

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

     Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

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

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует хеш выбранного файла для определения, является ли процесс доверенным.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  e. Нажмите на кнопку **ОК**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

Если вы сделали процесс доверенным для задачи Контроль запуска программ и в параметрах задачи создали разрешающее правило контроля запуска программ для исполняемого файла этого процесса, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes считает процесс доверенным, но запрещает запуск исполняемого файла этого процесса.

7. В окне **Доверенная зона** нажмите на кнопку **ОК**.

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

kaspersky

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Industrial CyberSecurity for Nodes выполнит действия, указанные в параметрах задачи, для программ, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 610).
2. На закладке **Исключения** в графе **Обнаруживаемые объекты** прокрутите список и выберите строку со значением *not-a-virus:**, если флажок снят.
3. Нажмите на кнопку **OK**.

Новые параметры будут применены.

Управление доверенной зоной с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка доверенной зоны для защищаемого компьютера.

В этом разделе

Использование доверенной зоны для задач в Консоли программы

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов, во вновь созданных 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, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить использование доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** выполните одно из следующих действий:
   - Чтобы применить доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Чтобы выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Чтобы настроить параметры доверенной зоны, перейдите по ссылке в названии флажка **Применять доверенную зону**.

   Откроется окно **Доверенная зона**.

   В окне **Доверенная зона** настройте исключения (см. раздел "Добавление исключений в доверенную зону" на стр. 619) и доверенные процессы (см. раздел "Добавление доверенных процессов с помощью Консоли программы" на стр. 620) и нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в окне **Параметры задачи**, чтобы сохранить изменения.

Настройка параметров доверенной зоны в Консоли программы

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Industrial CyberSecurity for Nodes пропускает (см. раздел "Добавление исключений в доверенную зону" на стр. 619) при выполнении задачи.
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Industrial CyberSecurity for Nodes пропускает (см. раздел "Добавление доверенных процессов с помощью Консоли программы" на стр. 620) при выполнении задачи.
3. Примените доверенную зону для задач программы (см. раздел "Использование доверенной зоны для задач в Консоли программы" на стр. 617).
4. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 623).

В этом разделе

Добавление исключений в доверенную зону

► *Чтобы вручную добавить исключение в доверенную зону в Консоли программы, выполните следующие действия:*

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

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Укажите объекты, которые Kaspersky Industrial CyberSecurity for Nodes пропускает при проверке и защите:
   - Чтобы импортировать предварительно настроенные исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Исключения из файла XML будут добавлены в список исключений.
   - Чтобы вручную указать условия, при выполнении которых объект считается доверенным, нажмите на кнопку **Добавить** и перейдите к следующим шагам.

     Откроется окно **Параметры правила исключения**.
5. Если вы нажали на кнопку **Добавить** в разделе **Не проверять объект при выполнении следующих условий**, укажите объекты, которые требуется исключить из области защиты или проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:
   - Чтобы исключить объект из области защиты или проверки:
     a. Установите флажок **Объект, исключенный из проверки**.

        Добавляет файл, папку, диск или файл скрипта в исключения.

        Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Industrial CyberSecurity for Nodes, выбранных в разделе **Область применения правила**.

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Объект для исключения из проверки**.

     c. Выберите объект, который вы хотите исключить из области проверки.

        При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Industrial CyberSecurity for Nodes при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Industrial CyberSecurity for Nodes обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

     d.

e. Нажмите на кнопку **ОК**.

f. Установите флажок **Применять к подпапкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Чтобы указать имя обнаруживаемого объекта:

  a. Установите флажок **Объекты, исключенные из обнаружения**.

     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 пропускает при проверке указанные объекты.

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

     По умолчанию флажок снят.

  b. Нажмите на кнопку **Изменить**.

     Откроется окно **Объекты для исключения из обнаружения**.

  c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

  d. Нажмите на кнопку **Добавить**.

  e. Нажмите на кнопку **ОК**.

6. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.
7. Нажмите на кнопку **ОК**.

Исключение отображается в списке на вкладке **Исключения** окна **Доверенная зона**.

Добавление доверенных процессов с помощью Консоли программы

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 исключит этот процесс из списка доверенных процессов.

► *Чтобы добавить один или несколько процессов в список доверенных с помощью Консоли программы:*

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

   Откроется окно **Доверенная зона**.

3. Выберите вкладку **Доверенные процессы**.
4. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

   Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом компьютере.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом компьютере.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом компьютере.

   По умолчанию флажок установлен.
5. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.
6. Чтобы добавить процесс в список доверенных процессов, выполните одно из следующих действий:
   - Чтобы импортировать предварительно настроенные доверенные процессы, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Процессы из файла XML будут добавлены в список доверенных процессов.
   - Чтобы указать процессы вручную, нажмите на кнопку **Добавить** и перейдите к следующим шагам.
7. Если вы нажали на кнопку **Добавить**, в контекстном меню кнопки выберите один из следующих вариантов:
   - **Несколько процессов**.

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

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

        Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

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

        Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует хеш выбранного файла для определения, является ли процесс доверенным.

        Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

        По умолчанию флажок установлен.

c. Чтобы добавить данные на основе исполняемых процессов, 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. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

h. Нажмите на кнопку **OK**.

> Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Industrial CyberSecurity for Nodes, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом компьютере. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

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

  В открывшемся окне **Добавление процесса** выполните следующие действия:

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

  > При указании объектов можно использовать маски имен (с помощью символов `?` и `*`) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Industrial CyberSecurity for Nodes при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Industrial CyberSecurity for Nodes обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

  b. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  c. Нажмите на кнопку **OK**.

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

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

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

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

     Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

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

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует хеш выбранного файла для определения, является ли процесс доверенным.

Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

По умолчанию флажок установлен.

d. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

e. Нажмите на кнопку **ОК**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

Если вы сделали процесс доверенным для задачи Контроль запуска программ и в параметрах задачи создали разрешающее правило контроля запуска программ для исполняемого файла этого процесса, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes считает процесс доверенным, но запрещает запуск исполняемого файла этого процесса.

8. В окне **Доверенная зона** нажмите на кнопку **ОК**.

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

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Industrial CyberSecurity for Nodes выполнит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

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

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Прокрутите список до элемента *not-a-virus:**.
5. Установите соответствующий флажок, если он снят.

6. Нажмите на кнопку **OK**.

Новые параметры будут применены.

Управление доверенной зоной с помощью Веб-плагина

Чтобы настроить доверенную зону с помощью Веб-плагина, выполните следующие действия:

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Параметры** в подразделе **Доверенная зона**.
6. Настройте доверенную зону (см. раздел "Настройка параметров доверенной зоны с помощью Плагина управления" на стр. 612) в соответствии с вашими требованиями.

kaspersky

Защита от сетевых угроз

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

В этом разделе

О задаче Защита от сетевых угроз

Задача Защита от сетевых угроз выполняет проверку входящего сетевого трафика на наличие действий, характерных для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Industrial CyberSecurity for Nodes блокирует сетевую активность со стороны атакующего компьютера. На экране отображается предупреждение, сообщающее о попытке сетевой атаки и содержащее информацию об атакующем компьютере.

По умолчанию задача Защита от сетевых угроз выполняется в режиме **Блокировать соединения при обнаружении атаки**. В этом режиме Kaspersky Industrial CyberSecurity for Nodes добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

IP-адреса узлов, проявляющих активность, характерную для сетевых атак, удаляются из списка заблокированных узлов в следующих случаях:

- Программа Kaspersky Industrial CyberSecurity for Nodes удалена.
- IP-адрес удален из списка заблокированных узлов вручную.
- Истек срок блокировки узла.
- Завершилось выполнение задачи Защита от сетевых угроз и не установлен флажок **Не останавливать анализ трафика, если задача не исполняется**.
- Выключен режим **Блокировать соединения при обнаружении атаки**.

Параметры по умолчанию для задачи Защита от сетевых угроз

По умолчанию в задаче Защита от сетевых угроз используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 84. Параметры по умолчанию для задачи Защита от сетевых угроз

Параметр	Значение по умолчанию	Описание
Режим работы	**Только уведомлять об обнаруженных атаках**	Задачу Защита от сетевых угроз можно запустить в одном из следующих режимов: **Не осуществлять мониторинг**, **Только уведомлять об обнаруженных атаках** или **Блокировать соединения при обнаружении атаки**.
Исключения	Список исключений не используется.	Укажите области, которые вы хотите исключить из области защиты.
Параметры расписания	По умолчанию, задача Защита от сетевых угроз запускается автоматически при запуске Kaspersky Industrial CyberSecurity for Nodes.	Можно настроить расписание.

Настройка задачи Защита от сетевых угроз с помощью Консоли программы

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Консоли программы.

В этом разделе

Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от сетевых угроз**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Общие**.
5. В разделе **Режим работы** выберите режим работы задачи:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
6. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
7. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
8. Нажмите на кнопку **OK**.

Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от сетевых угроз**.

   Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
5. Укажите IP-адрес и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **OK**.

kaspersky

Настройка задачи Защита от сетевых угроз с помощью Плагина управления

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Плагина управления.

В этом разделе

Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Постоянная защита компьютера** в блоке **Защита от сетевых угроз**нажмите на кнопку **Настройка**.

   Откроется окно **Защита от сетевых угроз**.
5. Выберите закладку **Общие**.
6. В разделе **Режим работы** выберите режим работы задачи:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
7. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
8. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
9. Нажмите на кнопку **OK**.

Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.
5. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
6. Укажите IP-адрес и нажмите на кнопку **Добавить**.
7. Нажмите на кнопку **OK**.

Настройка задачи Защита от сетевых угроз с помощью Веб-плагина

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Веб-плагина.

В этом разделе

kaspersky

Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Веб-консоли:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. В блоке **Защита от сетевых угроз** нажмите на кнопку **Параметры**.

   Откроется окно **Защита от сетевых угроз**.
6. Выберите вкладку **Общие**.
7. В разделе **Режим работы** выберите режим обработки:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
8. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
9. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
10. Нажмите на кнопку **OK**.

Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от сетевых угроз**.
6. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
7. Укажите IP-адрес и нажмите на кнопку **Добавить**.
8. Нажмите на кнопку **OK**.

kaspersky

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 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, 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 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 **Активный** Kaspersky Industrial CyberSecurity for Nodes блокирует все текущие подключения к сетям Wi-Fi, если используемые сети Wi-Fi не добавлены в список доверенных.

- **Только сообщать**. Kaspersky Industrial CyberSecurity for Nodes не блокирует подключения к сетям Wi-Fi. Вместо этого в журнале выполнения задачи фиксируется информация 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.

Задачу Контроль Wi-Fi можно запустить на компьютерах с операционными системами, в которых установлена функция Wireless LAN Service и запущен ее сервис WLAN Autoconfig (wlansvc). Задача Контроль Wi-Fi недоступна без дополнительной настройки параметров в операционных системах, не поддерживающих сервис wlansvc в качестве предустановленного:

- Microsoft Windows XP – должен быть доступен файл wlanapi.dll, а служба wzcsvc должна быть установлена и запущена до запуска задачи Контроль Wi-Fi.
- Microsoft Windows Server 2003 – должен быть доступен файл wlanapi.dll, а служба wzcsvc должна быть установлена и запущена до запуска задачи Контроль Wi-Fi.

- Microsoft Windows Server® 2003R2 – должен быть доступен файл wlanapi.dll, а служба wzcsvc должна быть установлена и запущена до запуска задачи Контроль Wi-Fi.
- 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 защищаемое устройство с операционной системой Microsoft Windows Server 2012 R2 требуется перезагрузка защищаемого устройства.

- Microsoft Windows Server 2016 – сервис wlansvc отсутствует и должен быть установлен до запуска задачи Контроль Wi-Fi.

Kaspersky Industrial CyberSecurity for Nodes 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 можно указать компонент Контроль Wi-Fi в списке выборочной установки, но задача Контроль Wi-Fi будет недоступна для запуска доустановки функции Wireless LAN Service и запуска ее сервиса WLAN Autoconfig (wlansvc).

Параметры задачи Контроль Wi-Fi по умолчанию

Задача Контроль Wi-Fi имеет ряд параметров, настроенных по умолчанию, которые вы можете изменять в соответствии с требованиями безопасности (см. таблицу ниже).

Таблица 85. Параметры задачи Контроль Wi-Fi по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы.	**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.
Разрешать подключения к указанным сетям Wi-Fi	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.
Расписание запуска задачи	**При запуске программы**	Задача Контроль Wi-Fi запускается автоматически при запуске программы. Вы можете настроить расписание запуска задачи.

kaspersky

Список 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 доверенную сеть Wi-Fi вручную (см. раздел "Добавление доверенной сети Wi-Fi вручную" на стр. 640);
- выбрать доверенные сети Wi-Fi из списка доступных сетей Wi-Fi (см. раздел "Добавление доверенной сети Wi-Fi с помощью списка доверенных сетей Wi-Fi" на стр. 641);
- 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 разрешает подключение к доверенным сетям Wi-Fi на основе следующих критериев:

- **Идентификатор беспроводной сети (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.

Настройка задачи Контроль Wi-Fi с помощью Плагина управления

В этом разделе

Настройка параметров задачи Контроль Wi-Fi

► *Чтобы настроить параметры задачи Контроль Wi-Fi, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

   Откроется окно **Свойства: Контроль Wi-Fi**.
4. На закладке **Общие**:
   - В разделе **Режим работы** укажите режим работы задачи Контроль Wi-Fi:
     - **Активный**.

       Kaspersky Industrial CyberSecurity for Nodes 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 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 подключения 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 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, измените список исключений для доверенных сетей Wi-Fi (см. раздел "Список доверенных сетей Wi-Fi" на стр. 633).

5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
6. Нажмите на кнопку **OK**.

Kaspersky Industrial CyberSecurity for Nodes 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.

Удаление исключения для сети Wi-Fi

► *Чтобы удалить сеть Wi-Fi из списка доверенных, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

   Откроется окно **Свойства: Контроль Wi-Fi** 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 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. 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 **OK**.

Выбранные сети Wi-Fi будут удалены из списка доверенных сетей Wi-Fi. Kaspersky Industrial CyberSecurity for Nodes будет блокировать подключение к таким сетям Wi-Fi.

kaspersky

Добавление доверенной сети Wi-Fi вручную

При добавлении доверенной сети Wi-Fi вручную необходимо самостоятельно задать критерии, на основе которых Kaspersky Industrial CyberSecurity for Nodes будет разрешать подключение к доверенной сети Wi-Fi.

► *Чтобы добавить сети Wi-Fi в список доверенных вручную, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

   Откроется окно **Свойства: Контроль Wi-Fi** 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 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 сеть Wi-Fi**.
6. В контекстном меню кнопки выберите вариант **Добавить вручную**.

   Откроется окно **Добавление доверенной сети Wi-Fi**.
7. Укажите параметры сети Wi-Fi, на основе которых Kaspersky Industrial CyberSecurity for Nodes 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 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 **Добавление доверенной 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 будет разрешать подключение к сетям Wi-Fi, которые подпадают под действие заданного исключения.

Добавление доверенной сети Wi-Fi с помощью списка доверенных сетей Wi-Fi

При добавлении исключения для доверенной сети Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 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.

► *Если вы хотите настроить параметры задачи Контроль Wi-Fi для группы компьютеров с помощью политики Kaspersky Security Center, убедитесь, что в политике Kaspersky Industrial CyberSecurity for Nodes включена передача данных о доступных сетях Wi-Fi на Сервер администрирования. Для этого выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики** > **<Имя политики>** > **Журналы и уведомления** > **Взаимодействие с Сервером администрирования**.
2. В окне **Взаимодействие с Сервером администрирования** установите флажок **Доступные устройства**.

   Kaspersky Industrial CyberSecurity for Nodes, установленный на локальных компьютерах, будет передавать информацию о доступных сетях Wi-Fi на Сервер администрирования Kaspersky Security Center.

► *Чтобы добавить доверенную сеть Wi-Fi с помощью списка доступных сетей Wi-Fi, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
- Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

Откроется окно **Свойства: Контроль Wi-Fi** 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 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 сеть Wi-Fi**.
6. В контекстном меню кнопки выберите пункт **Импортировать из списка Сервера Администрирования**.

   Откроется окно **Доступные сети Wi-Fi**.

7. Если требуется, нажмите на 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 **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 будет разрешать подключение к указанным сетям Wi-Fi.

kaspersky

Настройка задачи Контроль Wi-Fi с помощью Консоли программы

В этом разделе

Настройка задачи Контроль Wi-Fi

► *Чтобы настроить параметры задачи Контроль Wi-Fi, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** в панели результатов узла **Контроль Wi-Fi**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие**:
   - В разделе **Режим работы** укажите режим работы задачи Контроль Wi-Fi:
     - **Активный**.

       Kaspersky Industrial CyberSecurity for Nodes 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 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 подключения 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 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, измените список исключений для доверенных сетей Wi-Fi (см. раздел "Список доверенных сетей Wi-Fi" на стр. 633).

5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
6. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 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.

Добавление доверенной сети Wi-Fi вручную

При добавлении доверенной сети Wi-Fi вручную необходимо самостоятельно задать критерии, на основе которых Kaspersky Industrial CyberSecurity for Nodes будет разрешать подключение к доверенной сети Wi-Fi.

► *Чтобы добавить сети Wi-Fi в список доверенных вручную, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** в 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 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 сеть Wi-Fi**.
6. В контекстном меню кнопки выберите вариант **Добавить сеть Wi-Fi вручную**.

   Откроется окно **Добавление доверенной сети Wi-Fi**.
7. Укажите параметры сети Wi-Fi, на основе которых Kaspersky Industrial CyberSecurity for Nodes 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 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 **Добавление доверенной сети Wi-Fi**, нажмите на кнопку **OK**.

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 будет разрешать подключение к сетям Wi-Fi, которые подпадают под действие заданного исключения.

Добавление доверенной сети Wi-Fi с помощью списка доверенных сетей Wi-Fi

При добавлении исключения для доверенной сети Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 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 программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** в 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 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 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 на 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 **OK**.

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 будет разрешать подключение к указанных сетям Wi-Fi.

Удаление исключения для сети Wi-Fi

► *Чтобы удалить сеть Wi-Fi из списка доверенных, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** в 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 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. 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 **OK**.

Выбранные сети Wi-Fi будут удалены из списка доверенных сетей Wi-Fi. Kaspersky Industrial CyberSecurity for Nodes будет блокировать подключение к таким сетям Wi-Fi.

kaspersky

Защита от шифрования

Этот раздел содержит информацию о задаче Защита от шифрования и инструкции по настройке ее параметров.

В этом разделе

О задаче Защита от шифрования

Задача Защита от шифрования позволяет обнаруживать вредоносное шифрование сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств в сети организации.

В ходе выполнения задачи Защита от шифрования, Kaspersky Industrial CyberSecurity for Nodes проверяет обращения удаленных устройств к файлам, расположенным в папках общего доступа на защищаемом устройстве. Если программа расценивает действия удаленного устройства над сетевыми файловыми ресурсами как вредоносное шифрование, Kaspersky Industrial CyberSecurity for Nodes вносит локально уникальный идентификатор (LUID) этого устройства в список заблокированных узлов.

Задача Защита от шифрования может выполняться в синхронном и асинхронном режиме. По умолчанию, задача Защита от шифрования работает в асинхронном режиме. Обработка файловых операций распределяется на несколько параллельных потоков. Дополнительная информация о синхронном и асинхронном режиме обработки файловых операций и об изменении режима обработки файловых операций приведена в базе знаний "Лаборатории Касперского" (см. раздел "Источники для самостоятельного поиска информации" на стр. 1045).

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

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

Задача Защита от шифрования не блокирует доступ со стороны узла к сетевым файловым ресурсам до тех пор, пока активность этого узла 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 только регистрирует попытки вредоносного шифрования со стороны удаленных устройств в журнале выполнения задачи.

kaspersky

Статистика задачи Защита от шифрования

Когда выполняется задача Защита от шифрования, можно просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Industrial CyberSecurity for Nodes с момента запуска задачи, то есть статистику выполнения задачи.

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.

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

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

Таблица 86. Статистика задачи Защита от шифрования

Поле	Описание
Обнаружено попыток шифрования	Количество попыток доступа, в которых программа Kaspersky Industrial CyberSecurity for Nodes обнаружила активность шифрования.
Ошибок обработки	Количество обращений программ к области хранения, вызвавших ошибку задачи.
Обработано объектов	Общее количество обращений, обработанных Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

Параметры по умолчанию для задачи Защита от шифрования

По умолчанию в задаче Защита от шифрования используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 87. Параметры по умолчанию для задачи Защита от шифрования

Параметр	Значение по умолчанию	Описание
Режим работы	**Только статистика**	Задача Защита от шифрования может быть запущена в режиме **Активный** или **Только статистика**.
Область защиты	По умолчанию Kaspersky Industrial CyberSecurity for Nodes применяет задачу Защита от шифрования ко всем папкам общего доступа защищаемого устройства.	Вы можете изменить область защиты, указав папки общего доступа, к которым должна применяться задача.
Исключения	Применяется список исключений, который включает элементы, добавленные специалистами "Лаборатории Касперского" (stt, sig, exe, sldprt).	Укажите области, которые вы хотите исключить из области защиты.
Эвристический анализатор	Эвристический анализатор включен, и в Kaspersky Industrial CyberSecurity for Nodes применяется **Средний** уровень глубины проверки.	Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень глубины проверки.
Параметры расписания	По умолчанию время первого запуска задачи не задано. Задача Защита от шифрования не запускается автоматически при запуске Kaspersky Industrial CyberSecurity for Nodes.	Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень глубины проверки.

Настройка задачи Защита от шифрования с помощью Плагина управления

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.
5. В открывшемся окне настройте следующие параметры:
   - Режим работы задачи и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. 646) на закладке **Общие**.
   - Область защиты (см. раздел "Формирование области защиты" на стр. 648) на закладке **Область защиты**.
   - Исключения (см. раздел "Добавление исключений" на стр. 649) на закладке **Исключения**.
   - Расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404) на закладке **Управление задачей**.
6. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Общие параметры задачи

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
- Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.

5. В разделе **Режим работы** на закладке **Общие** выберите режим **Активный**.

   Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ к папкам общего доступа для скомпрометированных устройств при обнаружении попытки вредоносного шифрования.

6. 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.

7. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

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

kaspersky

Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная**. Можно использовать область защиты, заданную по умолчанию и включающую все папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки защищаемого устройства**.
- **Пользовательская**. Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные общие папки**.

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

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.
5. На закладке **Область защиты** выберите папки, которые Kaspersky Industrial CyberSecurity for Nodes будет проверять в ходе выполнения задачи Защита от шифрования:
   - **Все общие сетевые папки защищаемого устройства**.

     Если выбран этот вариант, в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes проверяет все папки общего доступа на защищаемом компьютере.

     Этот вариант выбран по умолчанию.
   - **Только указанные общие папки**.

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.

6. Чтобы указать папки общего доступа на устройстве, которые вы хотите включить в область защиты от шифрования, выполните следующие действия:
   a. Выберите вариант **Только указанные общие папки** и нажмите на кнопку **Добавить**.

      Откроется окно **Исключение из области контроля**.

   b. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.
   c. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Защита от шифрования**.

Настроенные параметры будут сохранены.

Добавление исключений

► *Чтобы добавить исключения из области защиты от шифрования, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.
5. На закладке **Исключения** установите флажок **Учитывать список исключений**.

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes обнаруживает попытки шифрования во всех папках общего доступа.

   По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

   - *.stt;
   - *.sig;
   - *.exe;
   - *.sldprt.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение из области контроля**.

7. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.
8. Нажмите на кнопку **ОК**.

Исключенная область будет добавлена в список.

Настройка задачи Защита от шифрования с помощью Консоли программы

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от шифрования**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне настройте следующие параметры:
   - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. 651) на закладке **Общие**.
   - Область защиты (см. раздел "Формирование области защиты" на стр. 652) на закладке **Область защиты**.
   - Исключения (см. раздел "Добавление исключений" на стр. 653) на закладке **Исключения**.
   - Расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404) на закладках **Расписание** и **Дополнительно**.
5. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

kaspersky

Общие параметры задачи

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от шифрования**.

   Откроется окно **Параметры задачи**.
4. В разделе **Режим работы** на закладке **Общие** выберите режим **Активный**.

   Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ к папкам общего доступа для скомпрометированных устройств 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.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
7. Нажмите на кнопку **OK**, чтобы применить новые параметры.

kaspersky

Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная**. Можно использовать область защиты, заданную по умолчанию и включающую в проверку все сетевые папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки защищаемого устройства**.
- **Пользовательская**. Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные общие папки**.

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

При использовании стандартной или пользовательской области защиты можно 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 программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от шифрования**.

   Откроется окно **Параметры задачи**.
4. На закладке **Область защиты** выберите папки, которые Kaspersky Industrial CyberSecurity for Nodes будет проверять в ходе выполнения задачи Защита от шифрования:
   - **Все общие сетевые папки защищаемого устройства**.

     Если выбран этот вариант, в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes проверяет все папки общего доступа на защищаемом компьютере.

     Этот вариант выбран по умолчанию.
   - **Только указанные общие папки**.

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.
5. Чтобы указать папки общего доступа на защищаемом устройстве, которые вы хотите включить в область защиты от шифрования, используйте один из следующих способов:
   - Вручную:
     a. Введите имя папки общего доступа на защищаемом устройстве.
     b. Нажмите на кнопку **Добавить**.

        Папка будет добавлена в список.

- Выбор папки:
  a. Нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows.

  b. Выберите папку, которую вы хотите добавить в область защиты задачи.

  c. Нажмите на кнопку **OK**.

6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Добавление исключений

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от шифрования**.

   Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Учитывать список исключений**.

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes обнаруживает попытки шифрования во всех папках общего доступа.

   По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

   - *.stt;
   - *.sig;
   - *.exe;
   - *.sldprt.
5. Укажите название или маску названия папки.
6. Нажмите на кнопку **Добавить**.
7. При необходимости повторите шаги 5 и 6 для добавления исключений.
8. В окне **Параметры задачи** нажмите на кнопку **OK**.

Исключения из области защиты будут добавлены и применены.

kaspersky

Настройка задачи Защита от шифрования с помощью Веб-плагина

В этом разделе описано управление задачей Защита от шифрования с помощью интерфейса Веб-плагина.

В этом разделе

Общие параметры задачи

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от шифрования**.
6. На закладке **Общие** выберите режим **Активный**.

   Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ к папкам общего доступа для скомпрометированных устройств при обнаружении попытки вредоносного шифрования.
7. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - 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.
   - Если требуется, отрегулируйте уровень эвристического анализа.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни чувствительности проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

8. Нажмите на кнопку **OK**, чтобы применить новые параметры.

Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

- **Стандартная**. Можно использовать область защиты, заданную по умолчанию и включающую в проверку все сетевые папки общего доступа на устройстве. Применяется, если выбран вариант **Все общие сетевые папки защищаемого устройства**.
- **Пользовательская**. Вы можете настроить область защиты вручную, выбрав папки, которые требуется включить в область защиты для задачи Защита от шифрования. Применяется, если выбран вариант **Только указанные общие папки**.

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

При использовании стандартной или пользовательской области защиты можно 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 главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от шифрования**.

6. На закладке **Область защиты** выберите папки, которые Kaspersky Industrial CyberSecurity for Nodes будет проверять в ходе выполнения задачи Защита от шифрования:

   - **Все общие сетевые папки защищаемого устройства**

     Если выбран этот вариант, в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes проверяет все папки общего доступа на защищаемом компьютере.

     Этот вариант выбран по умолчанию.

   - **Только указанные общие папки**

     Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes обеспечивает защиту только тех папок общего доступа на устройстве, которые вы указали вручную.

7. Чтобы указать папки общего доступа на устройстве, которые вы хотите включить в область защиты от шифрования, выполните следующие действия:

   a. Выберите вариант **Только указанные общие папки** и нажмите на кнопку **Добавить**.

   b. На панели справа укажите путь к папке.

   c. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **OK**, чтобы применить новые параметры.

Настроенные параметры будут сохранены.

Добавление исключений

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от шифрования**.
6. На закладке **Список исключений** установите флажок **Учитывать список исключений**.

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

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes обнаруживает попытки шифрования во всех папках общего доступа.

По умолчанию флажок установлен, а список исключений включает следующие элементы, добавленные специалистами "Лаборатории Касперского":

- *.stt;
- *.sig;
- *.exe;
- *.sldprt.

7. Нажмите на кнопку **Добавить**.
8. На панели справа укажите путь к папке или маску.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

Исключения из области защиты будут добавлены и применены.

kaspersky

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

Во время выполнения задачи Контроль запуска программ Kaspersky Industrial CyberSecurity for Nodes проверяет попытки пользователей запускать различные программы и разрешает или запрещает запуск этих программ. Задача Контроль запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются.

Вы можете разрешить запуск программ одним из следующих способов:

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

Запрет запуска программы имеет в задаче более высокий приоритет. Например, если запуск программы запрещен одним из правил, программа не будет запущена, независимо от заключения KSN о доверенности программы. При этом если программа признана недоверенной службами KSN, но подпадает под действие разрешающего правила, запуск такой программы будет запрещен.

Все попытки запуска программ фиксируются в журнале выполнения задач (см. раздел "О журналах выполнения задач" на стр. 956).

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

- **Активный**. Kaspersky Industrial CyberSecurity for Nodes с помощью набора правил контролирует запуск программ, которые попадают под действия правил контроля запуска программ. Область применения правил контроля запуска программ указывается в параметрах этой задачи. Если программа удовлетворяет правилам контроля запуска программ, а параметры задачи не удовлетворяют ни одному из указанных правил, то запуск такой программы будет запрещен.

  Запуск программ, которые не подпадают под действие правил, указанных в параметрах задачи Контроль запуска программ, не разрешается, независимо от параметров задачи Контроль запуска программ.

  Задачу **Контроль запуска программ** нельзя запустить в активном режиме, если не создано ни одного правила или если для одного защищаемого компьютера создано более 65535 правил.

- **Только статистика**. В Kaspersky Industrial CyberSecurity for Nodes не используются правила контроля запуска программ для запрета или разрешения запуска программ. Выполняется только запись информации обо всех запусках программ, правилах, выполненных при запуске программ, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Активный**. Разрешен запуск всех программ. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования правил контроля запуска программ (см. раздел "Формирование разрешающих правил по событиям задачи Контроль запуска программ" на стр. 708) на основе информации, зафиксированной в журнале выполнения задачи.

Вы можете настроить задачу Контроль запуска программ по одному из следующих сценариев:

- Дополнительная настройка (см. раздел "О правилах контроля запуска программ" на стр. 660) и применение правил контроля запуска программ.
- Базовая настройка правил и использование KSN (см. раздел "Настройка использования KSN" на стр. 700) для контроля запуска программ.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Kaspersky Industrial CyberSecurity for Nodes также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ фиксирует запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

kaspersky

О правилах контроля запуска программ

Как работают правила контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешить или запретить запуск программы. Соответственно, они называются *разрешающими* или *запрещающими*. Для создания списка разрешающих правил контроля запуска программ можно использовать задачу формирования разрешающих правил или задачу Контроль запуска программ в режиме **Только статистика**. Можно также добавлять разрешающие правила вручную.

- Пользователь или группа пользователей.

  Правила контроля запуска программ контролируют запуск указанных программ пользователем или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут применяться к *исполняемым файлам*, *скриптам* и *пакетам MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих хотя бы одному из критериев, указанных в параметрах правила: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256*, расположены по указанному *пути*, соответствуют указанным аргументам *командной строки*. Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

  Если в качестве критерия срабатывания правила выбран **Цифровой сертификат**, созданное правило контролирует запуск всех доверенных программ в операционной системе. Вы можете задать более строгие условия для этого критерия, установив следующие флажки:

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, заголовок указанного 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, можно указать только в свойствах 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, отпечаток указанного 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**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах 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 срабатывание правил запуска программ на основе цифрового сертификата, поскольку 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 определенных разрешающих правил: например, если требуется разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. 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.

kaspersky

О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программного обеспечения на защищаемых компьютерах, например, на защищаемых компьютерах, где происходит регулярное автоматическое обновление установленного программного обеспечения. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения можно использовать подсистему Контроль пакетов установки.

Пакет установки (далее также "пакет") представляет собой программу, устанавливаемую на защищаемый компьютер. В каждом пакете содержится как минимум одна программа, а также могут содержаться отдельные файлы, обновления и отдельные команды, в частности, когда выполняется установка программы или обновления.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. При добавлении пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Industrial CyberSecurity for Nodes контролирует только полный цикл распространения программного обеспечения. Программа не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен компонент Контроль пакетов установки или не был установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в параметрах задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш распространения программного обеспечения

Kaspersky Industrial CyberSecurity for Nodes использует динамически формируемый кеш распространения программного обеспечения (далее "кеш распространения") для связи между доверенными пакетами и файлами, созданными во время распространения программного обеспечения. При первом запуске пакета Kaspersky Industrial CyberSecurity for Nodes обнаруживает все файлы, созданные этим пакетом во время распространения программного обеспечения, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем, по умолчанию, разрешается запуск всех файлов в кеше распространения.

Кеш распространения нельзя просматривать, очищать и изменять вручную через пользовательский интерфейс. Kaspersky Industrial CyberSecurity for Nodes самостоятельно наполняет его, а также контролирует его актуальность.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и очищать 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 обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла программа удаляет запись для этого файла из кеша распространения. При активном режиме работы задачи Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

Обработка извлеченных файлов

Все извлеченные из доверенного пакета файлы наследуют атрибут доверенности при первом запуске пакета. При снятии флажка после первого запуска все извлеченные из пакета файлы сохраняют атрибут наследования. Чтобы отменить признак наследования для всех извлеченных файлов, необходимо очистить кеш распространения и снять флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** перед следующим запуском доверенного пакета установки.

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки, наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными. По умолчанию количество уровней наследования признака доверенности не ограничено.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 676) с помощью флажка **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и установлен флажок, то все пакеты и программы, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** не установлен, программа присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (только первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

Работа со 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 к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

Использование заключений KSN

Заключения KSN о том, что файл является недоверенным, имеют более высокий приоритет, чем исключения Контроля пакетов установки. Распаковка доверенных пакетов и запуск файлов, созданных или измененных доверенными пакетами, будет заблокирован, если для таких файлов получено заключение KSN о том, что файл является недоверенным.

При распаковке из доверенного пакета, запуск всех вложенных файлов будет разрешен, независимо от использования KSN в задаче Контроль запуска программ. При этом значение флажков **Запрещать запуск программ, недоверенных в KSN** и **Разрешать запуск программ, доверенных в KSN** не влияет на флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

Об использовании KSN в задаче Контроль запуска программ

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

Если данные KSN о репутации программы используются в задаче Контроль запуска программ, репутация программы по данным KSN считается основным критерием для разрешения или запрета запуска этой программы. Если KSN передает Kaspersky Industrial CyberSecurity for Nodes данные о том, что программа не является доверенной, то попытка пользователя запустить программу блокируется. Если KSN передает Kaspersky Industrial CyberSecurity for Nodes данные о том, что программа является доверенной, то разрешается запуск программы пользователем. KSN можно применять 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 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 запрета по умолчанию. Применение KSN при отсутствии правил позволяет защитить устройство от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании заключений KSN совместно с правилами контроля запуска программ применяются следующие условия:

- Kaspersky Industrial CyberSecurity for Nodes всегда блокирует запуск программы, если она 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 позволит расширить список заблокированных программ.
- Kaspersky Industrial CyberSecurity for Nodes всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для этой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить устройство от программ, которые по данным KSN представляют угрозу, но не были учтены при первоначальной настройке правил.

О формировании правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых компьютеров и групп защищаемых компьютеров в сети организации. Рекомендуется использовать перечисленные сценарии, если в сети организации нет эталонной машины и вы не можете сформировать список разрешающих правил на основе программ, установленным на такой эталонной машине.

Можно запустить задачу Формирование правил контроля запуска программ локально с помощью Консоли программы для создания списка правил на основе программ, запущенных на отдельном защищаемом компьютере.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающее правило для скриптов и пакетов установщика Windows с сертификатом, доверенным в операционной системе.
- Разрешающее правило для исполняемых файлов с сертификатом, доверенным в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи Формирование правил контроля запуска программ.

  В рамках этого сценария групповая задача формирует собственный список правил контроля запуска программ для каждого защищаемого компьютера в сети и сохраняет эти списки в XML-файл в указанной папке общего доступа. XML-файл, созданный задачей Формирование правил контроля запуска программ, содержит разрешающие правила, указанные при настройке параметров задачи, до ее запуска.Для программ, запуск которых не разрешен в параметрах указанной задачи, не будет создано ни одного правила. Запуск таких программ будет заблокирован по умолчанию. Затем вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ для политики Kaspersky Security Center.

  Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Рекомендуется использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом компьютере в тестовой группе защищаемых компьютеров или на эталонной машине.

- На основе отчета о событиях в работе задачи Контроль запуска программ в режиме **Только статистика**, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Industrial CyberSecurity for Nodes не блокирует запуск программ. Когда задача Контроль запуска программ работает в режиме **Только статистика**, все разрешенные и запрещенные запуски программ на всех защищаемых компьютерах сети регистрируются на закладке **События** в рабочей области узла Сервера администрирования в Kaspersky Security Center. С помощью отчетов в Kaspersky Security Center формируется единый список событий о заблокированных запусках программ.

  Вам нужно настроить период выполнения задачи так, чтобы за указанный промежуток времени выполнились все возможные сценарии работы защищаемых компьютеров и групп защищаемых компьютеров и хотя бы одна перезагрузка. После завершения выполнения задачи можно импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

  Рекомендуется использовать этот сценарий, если в сети организации имеется большое количество защищаемых компьютеров разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на защищаемом устройстве должна находиться под управлением активной политики Kaspersky Security Center. При этом все события на защищаемом устройстве передаются на Сервер администрирования.

Рекомендуется обновить список правил при изменении состава программ, установленных на управляемых компьютерах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется сформировать обновленный список правил, запустив задачу Формирование правил контроля запуска программ или задачу Контроль запуска программ в режиме **Только статистика** на защищаемых компьютерах тестовой группы администрирования. Тестовая группа администрирования включает защищаемые компьютеры, необходимые для тестового запуска новых программ перед их установкой на остальные защищаемые компьютеры сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом компьютере. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуется запускать задачи Формирование правил контроля запуска программ и Контроль запуска программ в режиме **Только статистика** на эталонной машине.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.

Параметры по умолчанию для задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 88. Параметры по умолчанию для задачи Контроль запуска программ

Параметр	Значение по умолчанию	Описание
Режим работы.	**Только статистика**. Задача регистрирует события, соответствующие попыткам запуска программ, запрещенным или разрешенным на основе набора правил. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Активный** после того, как будет сформирован окончательный список правил.
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	Не применяется	Можно повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках.
Запрещать запуск командных интерпретаторов без команды к исполнению	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.

Параметр	Значение по умолчанию	Описание
Правила	**Добавить правила политики к локальным правилам**	Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на защищаемом устройстве.
Область применения правил	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов. Кроме того, задача контролирует загрузку DLL-модулей.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.
Использование KSN	Данные KSN о репутации программы не используются.	Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.
Автоматически разрешать распространение с помощью указанных программ и пакетов установки	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию распространение программ разрешено только с помощью служб установщика Windows.
Всегда разрешать распространение программ с помощью установщика Windows	Применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются с помощью установщика Windows.
Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи	Не применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Можно включить или выключить автоматическое распространение программного обеспечения с помощью решения System Center Configuration Manager.
Параметры запуска задачи	Время первого запуска не задано.	Задача Контроль запуска программ не запускается автоматически сразу после Kaspersky Industrial CyberSecurity for Nodes. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Таблица 89. Заданные по умолчанию параметры задачи Формирование правил контроля запуска программ

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем защищаемого компьютера, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes.	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 будет 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 контроля запуска программ; новые правила объединяются с существующими правилами; дублирующиеся правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующихся правил или заменять существующие правила новыми разрешающими правилами, а также настраивать параметры экспорта разрешающих правил в файл.

Параметр	Значение по умолчанию	Описание
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи Формирование правил контроля запуска программ с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Время первого запуска не задано.	Задача Формирование правил контроля запуска программ не запускается автоматически при запуске Kaspersky Industrial CyberSecurity for Nodes. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем запуска программ с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам политики для задачи Контроль запуска программ

► *Чтобы перейти к параметрам задачи Контроль запуска программ в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.

Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

Настройте список правил в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам

► *Чтобы создать задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
5. Выберите задачу **Формирование правил контроля запуска программ**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля запуска программ**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля запуска программ.

Настройка параметров задачи Контроль запуска программ

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

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 671).

2. На закладке **Общие** в разделе **Режим работы** настройте следующие параметры:

   - В раскрывающемся списке **Режим работы** выберите режим работы задачи.

     В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:

     - **Активный**. Kaspersky Industrial CyberSecurity for Nodes использует определенные правила контроля запуска всех программ.
     - **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.

     По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

   - Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

     Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет программу при каждой попытке ее запуска.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

     - Запуск командного интерпретатора разрешен.
     - Исполняемая команда разрешена.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Industrial CyberSecurity for Nodes работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

3. В блоке **Правила** настройте параметры применения правил:

   a. Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила в задачу Контроль запуска программ.

   > Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

   b. Выберите режим применения правил:

   - **Заменить правилами политики локальные правила**

     Программа применяет список правил, заданных в политике, для централизованного контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.

   - **Добавить правила политики к локальным правилам**

     Программа применяет список правил, заданный в политике, совместно с локальными списками правил. Вы можете редактировать локальные списки правил с помощью задач автоматического формирования правил контроля запуска программ.

4. В разделе **Область применения правил** укажите следующие параметры:

   - **Использовать правила для исполняемых файлов**.

     Флажок включает или выключает контроль запуска исполняемых файлов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

     По умолчанию флажок установлен.

   - **Контролировать загрузку DLL-модулей**.

     Флажок включает или выключает контроль загрузки DLL-модулей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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 установлен.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**.

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

5. В блоке параметров **Использование KSN** настройте следующие параметры запуска программ:

   - **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

   - **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает запуск программ, доверенных в KSN. 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 не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

- Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ:
  a. В контекстном меню кнопки **Изменить** выберите способ добавления пользователей.

     Откроется окно **Выбор пользователя или группы пользователей**.
  b. Выберите пользователя или группу пользователей.
  c. Нажмите на кнопку **OK**.

6. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 676).
7. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания задач" на стр. 404).
8. В окне **Контроль запуска программ** нажмите на кнопку **OK**.

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

Настройка Контроля пакетов установки

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 671).
2. На закладке **Контроль пакетов установки** 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 с помощью доверенных пакетов установки. Список программ и пакетов 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 на закладке **Использовать правила для исполняемых файлов** в параметрах задачи **Общие** установлен флажок **Контроль запуска программ**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, добавленных в список разрешенных и запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

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 установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. 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 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).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

   Программа контролирует цикл распространения программного обеспечения на защищаемом компьютере: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемый компьютер.

5. Чтобы создать список разрешенных или изменить существующий список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

        Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

- **Использовать цифровой сертификат**
- **Использовать хеш SHA256**

- **Добавить несколько по хешу**

  Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Industrial CyberSecurity for Nodes учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

  Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**.

  Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Industrial CyberSecurity for Nodes такой файл должен удовлетворять следующим условиям:

  - иметь расширение TXT;
  - 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.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

kaspersky

Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 672).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:
   - Укажите префикс для названий правил.
   - Выберите способ создания разрешающих правил:
     - **Создавать разрешающие правила на основе запущенных программ**

       Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

       Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

       Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

       По умолчанию флажок снят.

       Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

     - **Создавать разрешающие правила для программ из папок**

       В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
4. В разделе **Параметры** можно указать действия при формировании разрешающих правил контроля запуска программ:
   - **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. 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.

Этот вариант выбран по умолчанию.

- **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. Kaspersky Industrial CyberSecurity for Nodes разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

  Использование этого флажка 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, использовать**

  Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма 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 срабатывания 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** в разделе **Настройка**.

- **Использовать хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задач.

1. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
2. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
3. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

4. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка правил контроля запуска программ в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

В этом разделе

Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ с помощью Плагина управления:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 671).
2. Нажмите на кнопку **Добавить**.

3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.

4. 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 блокировало 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.

        Если вы создаете разрешающее правило для исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для задачи Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

      - **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:

      i. В контекстном меню кнопки **Выбрать** выберите способ добавления доверенных пользователей.

         Откроется окно **Выбор пользователя или группы пользователей**.

      ii. Выберите пользователя или группу пользователей.

      iii. Нажмите на кнопку **ОК**.

   e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:

      i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.

      ii. Выберите файл.

      iii. Нажмите на кнопку **Открыть**.

         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 параметров **Критерий срабатывания правила** выберите как минимум один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.
  - **Командная строка**, чтобы правило контролировало запуск программ, осуществляемый с помощью аргументов, указанных в поле командной строки. Поле доступно при выборе варианта **Путь к файлу**. При указании аргументов командной строки для запущенных процессов в качестве критерия можно использовать маску, включающую символы ? и *.

Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь. При указании объектов можно использовать символы ? и * в качестве маски файлов.

Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

i. В разделе **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения.

iii. Укажите параметры исключения файлов 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.

Этот вариант выбран по умолчанию.

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, заголовок указанного 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, можно указать только в свойствах 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, отпечаток указанного 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**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах 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 контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

  Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

i. Нажмите на кнопку **OK**.

ii. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 671).
2. Нажмите на кнопку **Добавить** и в открывшемся контекстном меню выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
3. В поле **Название** введите название правила.
4. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
5. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
6. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
7. Введите следующую маску: `?:\`
8. В окне **ОК** нажмите на кнопку **Параметры правила**.

Kaspersky Industrial CyberSecurity for Nodes применяет режим разрешения по умолчанию.

Формирование разрешающих правил контроля запуска программ на основе событий Kaspersky Security Center

► Чтобы сформировать разрешающие правила контроля запуска программ на основе событий Kaspersky Security Center:

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 671).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
4. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

Откроется окно **Создать правила контроля запуска программ**.

5. Выберите типы событий, на основе которых программа будет создавать правила контроля запуска программ:
   - **Только статистика: запуск программы запрещен**.
   - **Запуск программы запрещен**.
6. Выберите период из раскрывающегося списка **Учитывать события, сформированные в течение периода**.
7. Если необходимо, в поле **Использовать события, сформированные для группы управляемых устройств** введите имя или фрагмент имени группы управляемых с помощью Kaspersky Security Center устройств, события для которых будут основой для формирования правил контроля запуска программ.
8. Снимите или установите флажок **Приоритизировать использование контрольной суммы при создании правил**.
9. Нажмите на кнопку **Создать правила**.
10. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

    Список правил в задаче Контроль запуска программ будет дополнен новыми правилами, сформированными на основе системных данных защищаемого компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

    Правила с повторяющимся хешем не добавляются, поскольку все правила в списке должны быть уникальными.

Импорт правил из отчета Kaspersky Security Center о заблокированных программах

Вы можете импортировать данные о заблокированных запусках программ из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль запуска программ в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил запуска программ в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль запуска программ, вы можете отслеживать программы, запуск которых был заблокирован.

При импорте из отчета данных о заблокированных программах в свойства политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

► *Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых компьютеров на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 671).

2. В блоке **Режим работы** выберите режим **Только статистика**.
3. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что:
   - Для событий с уровнем важности **Критический** срок хранения событий **Запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).
   - Для событий с уровнем важности **Предупреждение** срок хранения событий **Только статистика: запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

   По истечении срока хранения событий информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль запуска программ в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленный срок хранения указанных событий.
4. По завершении задачи выполните экспорт зарегистрированных событий в файл формата TXT:
   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.
   b. Нажмите на кнопку **Создать выборку**, чтобы создать выборку событий по критерию Заблокировано и просмотреть, запуск каких программ будет заблокирован задачей Контроль запуска программ.
   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых требуется разрешить.
5. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:
   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля запуска программ**.
   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.
   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку настроенных ранее правил контроля запуска программ:
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

a. **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.В открывшемся стандартном окне Microsoft Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

d. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

Импорт правил контроля запуска программ из XML-файла

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Формирование правил контроля запуска программ, и применить их в качестве списка разрешающих правил в настраиваемой политике.

По завершении групповой задачи формирования правил контроля запуска программ выполняется экспорт созданных разрешающих правил в XML-файлы в указанную папку общего доступа. Каждый файл со списком правил создается на основе анализа исполняемых файлов и запущенных программ на каждом отдельном защищаемом компьютере в сети организации. Списки содержат разрешающие правила для файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче формирования правил контроля запуска программ.

► *Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых компьютеров на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** в панели результатов настраиваемой группы защищаемых устройств создайте групповую задачу Формирование правил контроля запуска программ или выберите уже созданную задачу (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 672).
2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
   - В разделе **Уведомление** настройте параметры сохранения отчета выполнения задачи.

     Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

   - В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Можно изменить набор папок, содержащих разрешенные для запуска программы: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
   - В разделе **Параметры** укажите действия, выполняемые задачей во время работы и после завершения. Укажите критерий формирования правил и имя файла, в который будут экспортированы эти правила.
   - В разделе **Расписание** настройте параметры запуска задачи по расписанию.
   - В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
   - В разделе **Исключения из области действия задачи** задайте группы защищаемых компьютеров, которые вы хотите исключить из области действия задачи.

> Kaspersky Industrial CyberSecurity for Nodes не будет создавать разрешающие правила по программам, запускаемым на исключенных защищаемых компьютерах.

3. На закладке **Задачи** в панели результатов настраиваемой группы защищаемых компьютеров в списке групповых задач выберите созданную задачу Формирование правил контроля запуска программ и нажмите на кнопку **Запустить** для запуска задачи.

   После завершения задачи, автоматически сформированные списки разрешающих правил будут сохранены в XML-файлы в папке общего доступа.

   > Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом компьютере в тестовой группе защищаемых компьютеров или на эталонной машине.

4. Чтобы добавить сформированные списки разрешающих правил в задачу Контроль запуска программ, выполните следующие действия:

   a. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 671).

   b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

   c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

   a. В открывшемся стандартном окне Microsoft Windows выберите XML-файлы, созданные по завершении групповой задачи Формирование правил контроля запуска программ.

   b. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

5. Если вы хотите применять созданные правила для контроля запуска программ, в политике в свойствах задачи Контроль запуска программ выберите режим **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном защищаемом компьютере, будут применены на всех защищаемых компьютерах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых компьютеров программа разрешит запуск только тех программ, для которых созданы разрешающие правила.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу, чтобы определить, какие правила контроля запуска программ срабатывают для выбранной программы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes блокирует программы, запуск которых не разрешен хотя бы одним правилом. Чтобы избежать блокировки запуска важных программ, необходимо создать для них разрешающие правила.

Если запуск программы контролируется несколькими правилами разных типов, запрещающие правила имеют больший приоритет: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы проверить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 671).
2. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
3. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все правила, которые сработают при запуске указанного файла.

Создание задачи Формирование правил контроля запуска программ

► *Чтобы создать задачу Формирование правил контроля запуска программ и настроить ее параметры, выполните следующие действия:*

1. Откройте окно **Настройка** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 672).
2. Настройте следующие параметры:
   - Укажите **Префикс для названий правил**.

     Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

     По умолчанию в качестве префикса указано имя защищаемого компьютера, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes. Вы можете изменить префикс для названий разрешающих правил.
   - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 711).
3. Нажмите на кнопку **Далее**.
4. Укажите действия, которые должна выполнять программа Kaspersky Industrial CyberSecurity for Nodes:
   - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. 712);
   - по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. 714).
5. В окне **Расписание** укажите параметры запуска задачи по расписанию.
6. Нажмите на кнопку **Далее**.

7. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
8. Нажмите на кнопку **Далее**.
9. Укажите название задачи.
10. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
11. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
12. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

► *Чтобы настроить существующее правило в Kaspersky Security Center,*

откройте окно **Свойства: Формирование правил контроля запуска программ** и настройте параметры, как описано выше.

Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 672)
2. Выберите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных программ**

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

По умолчанию флажок снят.

Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

- **Создавать разрешающие правила для программ из папок**

  В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

► *Чтобы настроить действия Kaspersky Industrial CyberSecurity for Nodes во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 672).
2. Выберите закладку **Параметры**.
3. 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.

     Этот вариант выбран по умолчанию.

   - **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. Kaspersky Industrial CyberSecurity for Nodes разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

     Использование этого флажка 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, использовать**

  Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма 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 срабатывания 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** в разделе **Настройка**.

- **Использовать хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

4. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Industrial CyberSecurity for Nodes по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 672).
2. Выберите закладку **Параметры**.
3. 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 при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.
   - **Принцип добавления**.

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
     - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

     По умолчанию выбран способ **Объединять с существующими правилами**.
   - **Экспортировать разрешающие правила в файл**.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  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.

  По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Управление контролем запуска программ с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам задачи Контроль запуска программ

► *Чтобы перейти к общим параметрам задачи Контроль запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы 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**.

Переход к окну с правилами контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы 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. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
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. Настройте задачу в соответствии с вашими требованиями.

kaspersky

Настройка параметров задачи Контроль запуска программ

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 696).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 698).
     - Область применения правил в задаче (см. раздел "Настройка области действия задачи Контроль запуска программ" на стр. 699).
     - Использование KSN (см. раздел "Настройка использования KSN" на стр. 700).
   - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. 701) на закладке **Контроль пакетов установки**.
   - Расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425) на закладках **Расписание** и **Дополнительно**.
3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.

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

В этом разделе

Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 696).
2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим работы задачи.

   В раскрывающемся списке вы можете выбрать режим работы задачи Контроль запуска программ:

   - **Активный**. Kaspersky Industrial CyberSecurity for Nodes контролирует все запускаемые программы с помощью заданных правил.
   - **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о блокировках, зарегистрированной в журнале выполнения задачи.

   По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.
3. Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

   Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет программу при каждой попытке ее запуска.

   По умолчанию флажок снят.

   Kaspersky Industrial CyberSecurity for Nodes заводит новый список событий в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом, контроль запуска программ осуществляется в соответствии с актуальными параметрами безопасности.
4. Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

   - Запуск командного интерпретатора разрешен.
   - Исполняемая команда разрешена.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Industrial CyberSecurity for Nodes работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

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

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Настройка области действия задачи Контроль запуска программ

► *Чтобы задать область действия задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 696).
2. На закладке **Общие** в блоке **Область применения правил** задайте следующие параметры:
   - **Использовать правила для исполняемых файлов**

     Флажок включает или выключает контроль запуска исполняемых файлов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

     По умолчанию флажок установлен.

   - **Контролировать загрузку DLL-модулей**

     Флажок включает или выключает контроль загрузки DLL-модулей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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 установлен.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Настройка использования KSN

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 696).
2. На закладке **Общие** в блоке **Использование KSN** укажите параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

- Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

  Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает запуск программ, доверенных в KSN. 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 не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

  По умолчанию флажок снят.

- Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, укажите пользователей и 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**.

     По умолчанию доступ к доверенным в KSN программам разрешен всем пользователям.

  b. Задайте список пользователей и / или групп пользователей.

  c. Нажмите на кнопку **OK**.

3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Контроль пакетов установки

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 696).
2. На закладке **Контроль пакетов установки** 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 с помощью доверенных пакетов установки. Список программ и пакетов 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 на закладке **Использовать правила для исполняемых файлов** в параметрах задачи **Общие** установлен флажок **Контроль запуска программ**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, добавленных в список разрешенных и запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

   Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

   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 установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. 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 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).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения на защищаемом компьютере: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемый компьютер.

5. Чтобы создать список разрешенных или изменить существующий список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

        Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

     d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

        - **Использовать цифровой сертификат**
        - **Использовать хеш SHA256**

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Industrial CyberSecurity for Nodes учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

   - **Изменить выбранный**

     Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

   - **Импортировать из текстового файла**.

     Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Industrial CyberSecurity for Nodes такой файл должен удовлетворять следующим условиям:

     - иметь расширение TXT;
     - 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.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

kaspersky

Настройка правил контроля запуска программ

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

В этом разделе

Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ с помощью Консоли программы:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к окну с правилами контроля запуска программ**" на стр. 696).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. 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 блокировало 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.

        Если вы создаете разрешающее правило для исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для задачи Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

- **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:

   i. В контекстном меню кнопки **Выбрать** выберите способ добавления доверенных пользователей.

      Откроется окно **Выбор пользователя или группы пользователей**.

   ii. Выберите пользователя или группу пользователей.

   iii. Нажмите на кнопку **OK**.

e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:

   i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

      Откроется стандартное окно Microsoft Windows **Открыть**.

   ii. Выберите файл.

   iii. Нажмите на кнопку **Открыть**.

      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 параметров **Критерий срабатывания правила** выберите как минимум один из следующих вариантов:

   - **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
     - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
     - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
   - **хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
   - **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.
     - **Командная строка**, чтобы правило контролировало запуск программ, осуществляемый с помощью аргументов, указанных в поле командной строки. Поле доступно при выборе варианта **Путь к файлу**. При указании аргументов командной строки для запущенных процессов в качестве критерия можно использовать маску, включающую символы ? и *.

     Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь. При указании объектов можно использовать символы ? и * в качестве маски файлов.

   Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

i. В разделе **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения.

iii. Укажите параметры исключения файлов 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.

  Этот вариант выбран по умолчанию.

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, заголовок указанного 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, можно указать только в свойствах 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, отпечаток указанного 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**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах 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 контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

  Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.

i. Нажмите на кнопку **OK**.

ii. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

1. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. В поле **Название** введите название правила.
5. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.

6. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
7. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
8. Введите следующую маску: `?:\`
9. В окне **ОК** нажмите на кнопку **Параметры правила**.

Kaspersky Industrial CyberSecurity for Nodes применяет режим разрешения по умолчанию.

Формирование разрешающих правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл с разрешающими правилами, сформированный 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. 698), чтобы регистрировать в журнале выполнения задачи информацию обо всех запусках 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 создаст конфигурационный файл в формате XML со списком правил, сформированных на основе событий задачи Контроль запуска программ, отработавшей в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. 709) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть и обработать вручную список правил, чтобы убедиться, что запуск важных файлов (например, файлов операционной системы) разрешен заданными правилами.

Все события задачи фиксируются в журнале выполнения задачи, независимо от режима работы задачи. Вы можете создать конфигурационный файл со списком правил на основе журнала, сформированного во время выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, поскольку финальный список правил должен быть сформирован перед запуском задачи в режиме **Активный**, чтобы правила работали эффективно.

Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. 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, при экспорте правил его содержимое будет перезаписано.
4. Нажмите на кнопку **Сохранить**.

Параметры правил будут экспортированы в указанный файл.

Импорт правил контроля запуска программ из XML-файла

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
4. 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 требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, содержащий правила контроля запуска программ.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. В списке выберите правила, которые требуется удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 696) для задачи **Формирование правил контроля запуска программ**.
2. Настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите **Префикс для названий правил**.

       Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя защищаемого компьютера, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes. Вы можете изменить префикс для названий разрешающих правил.
     - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 711).
   - На закладке **Действия** укажите действия, которые должна выполнять программа Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Действия при автоматическом формировании правил" на стр. 712).
   - На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
   - На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

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

kaspersky

В этом разделе

Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 696) для задачи **Формирование правил контроля запуска программ**.
2. Выберите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных программ**.

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок снят.

     Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.
   - **Создавать разрешающие правила для программ из папок**.

     В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

► *Чтобы настроить действия, которые программа Kaspersky Industrial CyberSecurity for Nodes должна выполнять во время работы и по завершении задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 696) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. 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.

     Этот вариант выбран по умолчанию.

   - **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. Kaspersky Industrial CyberSecurity for Nodes разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

     Использование этого флажка 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, использовать**

     Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма 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 срабатывания 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** в разделе **Настройка**.

- **Использовать хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

4. 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 при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

   - **Принцип добавления**.

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменять существующие правила**. Правила добавляются вместо существующих правил.

- **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.
- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  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.

  По умолчанию флажок установлен.

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

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Industrial CyberSecurity for Nodes по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 696) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. 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 при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

- **Принцип добавления**.

  Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.
- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  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.

  По умолчанию флажок установлен.

4. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Управление контролем запуска программ с помощью веб-плагина

► *Чтобы настроить задачи контроля запуска программ с помощью веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Параметры** в подразделе **Контроль запуска программ**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 90. Параметры задачи Контроль запуска программ

Параметр	Описание
Режим работы задачи.	В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ: • **Активный**. Kaspersky Industrial CyberSecurity for Nodes использует определенные правила контроля запуска всех программ. • **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи. По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет программу при каждой попытке ее запуска. По умолчанию флажок снят.

Параметр	Описание
Запрещать запуск командных интерпретаторов без команды к исполнению	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий: • Запуск командного интерпретатора разрешен. • Исполняемая команда разрешена. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее. Kaspersky Industrial CyberSecurity for Nodes работает со следующими командными интерпретаторами: • cmd.exe; • powershell.exe; • python.exe; • perl.exe. По умолчанию флажок снят.
Использовать правила для исполняемых файлов	Флажок включает или выключает контроль запуска исполняемых файлов. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен. По умолчанию флажок установлен.

Параметр	Описание
Контролировать загрузку DLL-модулей	Флажок включает или выключает контроль загрузки DLL-модулей. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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 установлен.
Использовать правила для скриптов и пакетов MSI	Флажок включает или выключает запуск скриптов и пакетов MSI. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен. По умолчанию флажок установлен.

Параметр	Описание
Запрещать запуск программ, недоверенных в KSN	Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам. По умолчанию флажок снят.
Разрешать запуск программ, доверенных в KSN	Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает запуск программ, доверенных в KSN. 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 не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам. По умолчанию флажок снят.

Параметр	Описание
Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ	Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, в этом поле можно указать пользователей и группы пользователей, которым разрешен запуск программ, доверенных в KSN. По умолчанию указаны следующие пользователи: **Все** и **NT AUTHORITY\SYSTEM**.
Правила	Настройте разрешающие и запрещающие правила (см. раздел "Настройка правил контроля запуска программ в Kaspersky Security Center" на стр. 681) для задачи контроля запуска программ.
Контроль пакетов установки	Можно добавлять доверенные пакеты установки (см. раздел "Настройка Контроля пакетов установки" на стр. 676).
Управление задачей	Вы можете настроить расписание запуска задачи.

kaspersky

Контроль устройств

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

В этом разделе

О задаче Контроль устройств

Kaspersky Industrial CyberSecurity for Nodes контролирует регистрацию и использование внешних устройств и CD/DVD-дисководов в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемыми флеш-накопителями или внешними устройствами другого типа.

Kaspersky Industrial CyberSecurity for Nodes контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители, в том числе поддерживающие технологию UAS;
- устройства чтения CD/DVD-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые сетевые адаптеры;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Industrial CyberSecurity for Nodes 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 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 следующих статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. При формировании списка правил значение *Путь к экземпляру устройства* подпадает под область применения хотя бы одного правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область применения 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 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 в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Industrial CyberSecurity for Nodes контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета 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 до запуска задачи Контроль устройств в режиме **Активный**, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемый компьютер. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes 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.

  Этот режим можно использовать для формирования правил на основе информации о блокировании устройств, зарегистрированной во время выполнения задачи (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 744).

О правилах контроля устройств

Kaspersky Industrial CyberSecurity for Nodes не использует разрешающие правила для MTP-подключаемых мобильных 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 формирования разрешающих правил контроля устройств можно:

- Использовать задачу Формирование правил контроля устройств (см. раздел "О задаче Формирование правил контроля устройств" на стр. 726).
- Запустить задачу Контроль устройств в режиме Только статистика (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 744).
- Использовать данные системы о подключавшихся устройствах (см. раздел "Добавление разрешающего правила для одного или нескольких внешних устройств" на стр. 745).
- Расширить область применения уже созданных правил (см. раздел "Расширение области применения правил контроля устройств" на стр. 747).

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Industrial CyberSecurity for Nodes, составляет 3072.

Правила контроля устройств описаны ниже.

Тип правила

Тип правила – всегда *разрешающее*. Задача Контроль 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 параметра *Путь к экземпляру устройства*. Путь к экземпляру устройства является уникальным идентификатором, который система присваивает устройству в момент его подключения и регистрации в качестве внешнего устройства или устройства чтения CD/DVD-дисков (например, IDE или SCSI).

Kaspersky Industrial CyberSecurity for Nodes 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 внешнего устройства и для устройства чтения CD/DVD-дисков (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 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 сформировал разрешающее правило. Вы можете настраивать значения параметров созданного правила с помощью маски, чтобы расширить область применения правила (см. раздел "Расширение области применения правил контроля устройств" на стр. 747).

Данные исходного устройства

Данные устройства, на основе которых программа Kaspersky Industrial CyberSecurity for Nodes сформировала разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Путь к экземпляру устройства**. На основании этого свойства Kaspersky Industrial CyberSecurity for Nodes 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 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 правила контроля устройств в поле **Описание**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующем поле 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.

О формировании правил контроля устройств

Вы можете импортировать списки разрешающих правил 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 запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие заданных правил контроля устройств.

Таблица 91. Цели и сценарии формирования правил контроля устройств

Сценарий формирования списка правил	Решаемая задача
Задача Формирование правил контроля устройств	• 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.
Создание правил на основе данных системы	Создать разрешающие правила для внешних устройств, данные о которых хранятся в системе.
Формирование правил по данным о подключенных в текущий момент устройствах	Обновление списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств.
Режим **Только статистика** задачи Контроль устройств	Добавить разрешающие правила для большого количества 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.

Используйте этот способ, чтобы учесть при формировании правил данные обо всех когда-либо подключавшихся внешних устройствах, сохранившиеся в системах на всех защищаемых устройствах сети, или данные только об устройствах, подключенных в настоящее время. Задача также учитывает все внешние устройства, подключенные в момент выполнения задачи. По завершении выполнения групповой задачи, Kaspersky Industrial CyberSecurity for Nodes формирует списки разрешающих правил для всех зарегистрированных в сети внешних устройств и сохраняет эти списки в XML-файл в указанной папке. Далее вы можете вручную импортировать сформированные правила в свойства задачи Контроль устройств. В отличие от задачи на защищаемом устройстве, в политике невозможно настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи Формирование правил контроля 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 получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому компьютеру в данный момент, и отображает обнаруженные устройства в списке в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Industrial CyberSecurity for Nodes определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Можно сформировать разрешающие правила для любого внешнего устройства, данные о котором хранятся в системе, и сразу добавить новые правила в список правил контроля устройств.

При использовании этого сценария Kaspersky Industrial CyberSecurity for Nodes формирует разрешающие правила для внешних устройств, подключавшихся ранее или подключенных в текущий момент к защищаемому устройству, на котором установлена программа Kaspersky Security Center.

Рекомендуется использовать этот сценарий для обновления списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств.

Использование данных о подключенных в текущий момент устройствах

При использовании этого сценария Kaspersky Industrial CyberSecurity for Nodes формирует разрешающие правила только для внешних устройств, подключенных в текущий момент. Вы можете выбрать одно или несколько внешних устройств, для которых вы хотите сформировать разрешающие правила.

Использование 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 фиксирует информацию обо всех подключениях флеш-накопителей и других внешних 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 задачи Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на защищаемых устройствах.

О задаче Формирование правил контроля устройств

Задача Формирование правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других внешних устройств на основе данных системы обо всех внешних устройствах, которые ранее подключались к защищаемому компьютеру.

По завершении выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 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 параметров задачи Формирование правил контроля устройств. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются в окне **Правила контроля устройств**.

Параметры по умолчанию для задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 92. Параметры по умолчанию для задачи Контроль устройств

Параметр	Значение по умолчанию	Описание
Режим работы.	**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 устройства, чтобы применять фактическую блокировку использования внешних устройств.
Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется	Не применяется	Kaspersky Industrial CyberSecurity for Nodes 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 программа Kaspersky Industrial CyberSecurity for Nodes разрешала использование всех внешних устройств, если задача Контроль устройств не выполняется.
Расписание запуска задачи	Время первого запуска не задано.	Задача Контроль устройств не запускается автоматически при запуске программы Kaspersky Industrial CyberSecurity for Nodes. Вы можете настроить запуск задачи по расписанию.

Таблица 93. Параметры задачи Формирование правил контроля устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Режим генерации.	**Учитывать данные системы обо всех когда-либо подключавшихся устройствах**	Режим работы задачи. Можно выбрать режим **Учитывать данные только об устройствах, подключенных в текущий момент**.
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	Время первого запуска не задано.	Задача Формирование правил контроля устройств не запускается автоматически сразу при запуске программы Kaspersky Industrial CyberSecurity for Nodes. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем устройств с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и управление подключением внешних устройств ко всем защищаемым компьютерам в сети с помощью списков правил в Kaspersky Security Center для групп защищаемых компьютеров.

В этом разделе

kaspersky

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам политики для задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.
7. Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.

7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.

8. Настройте политику в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам

► *Чтобы создать задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.

5. Выберите задачу **Формирование правил контроля устройств**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля устройств**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля устройств.

Настройка задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Контроль устройств** (см. раздел "**Переход к параметрам политики для задачи Контроль устройств**" на стр. 729).
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Industrial CyberSecurity for Nodes контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета 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 до запуска задачи Контроль устройств в режиме Активный, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**.

       Kaspersky Industrial CyberSecurity for Nodes не контролирует подключение съемных дисков 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 запоминающих устройств, если задача Контроль устройств не выполняется**.

     Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется.

     Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Industrial CyberSecurity for Nodes разрешает использовать любые внешние устройства на защищаемом компьютере.

     Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом компьютере в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

     По умолчанию флажок снят.
3. Нажмите на кнопку **Список правил**, чтобы изменить список правил контроля устройств (см. раздел "Настройка правил контроля устройств в Kaspersky Security Center" на стр. 733).

4. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**.
5. Нажмите на кнопку **ОК** в окне **Контроль устройств**.

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

Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля устройств** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам**" на стр. 730).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:
   - Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.
   - Настройте параметры для конфигурационных файлов со списком разрешающих правил, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задачи.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
6. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

   Настроенные параметры групповых задач будут сохранены.

kaspersky

Настройка правил контроля устройств в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

В этом разделе

Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила на основе данных системы** задачи Контроль устройств, выполните следующие действия:*

1. Если требуется, подключите к защищаемому устройству с установленной Консолью администрирования Kaspersky Security Center новое внешнее устройство, использование которого вы хотите разрешить.
2. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 729).
3. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.
4. Выберите устройство в списке устройств в окне **Сформировать правила на основе данных системы**.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.
6. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

Формирование правил для подключенных устройств

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 729).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.
3. В списке обнаруженных устройств, которые подключены к защищаемому компьютеру, выберите устройства, для которых вы хотите сформировать разрешающие правила.
4. Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

Формирование правил на основе реестра Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 729).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.
3. Нажмите на кнопку **Обновить список**, чтобы отобразился список доступных устройств, и выберите устройства, для которых требуется сформировать разрешающие правила. В поле **Поиск** можно также указать **Адаптированное имя**, чтобы отфильтровать устройства и упростить их выбор.
4. Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе реестра Kaspersky Security Center.

Просмотр свойств правил Контроля устройств

Чтобы просмотреть свойства правил задачи **Контроль устройств**, выполните следующие действия:

1. Откройте окно **Контроль устройств**.
2. На закладке **Общие** нажмите на кнопку **Список правил** и дважды щелкните выбранное правило.

   Откроется окно **Свойства правила**.

Таблица 94. Свойства правил Контроля устройств

Свойство	Описание
Применять правило	Этот параметр используется, чтобы включать и выключать применение правила.
Производитель (VID)	Вы можете указать полный VID производителя устройства или использовать символ * в качестве маски. Символ * используется для указания любого производителя. Если в поле Производитель (VID) установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила.
Тип контроллера (PID)	Вы можете указать полный PID контроллера или использовать символ * в качестве маски. Символ * используется для указания любого типа контроллера. Если в поле Тип контроллера (PID) установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила.
Серийный номер	Вы можете указать полный серийный номер устройства или использовать символы * или ? в качестве маски. Символ * обозначает любую последовательность символов, включая пустую последовательность. Символ ? обозначает один символ в последовательности. Если в поле Серийный номер установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила. Если вы выбрали вариант **Использовать маску**, но не ввели никаких символов в поле **Серийный номер**, после чего сохранили параметры и закрыли окно, программа применит * в качестве маски для поля **Серийный номер** и не будет учитывать его при применении правила.
Путь к экземпляру устройства	Идентификатор подключенного устройства. Это свойство нельзя изменить. Поле предназначено только для справки. Это поле не используется программой для управления устройством.

Свойство	Описание
Адаптированное имя	Название устройства, заданное производителем. Это свойство нельзя изменить. Поле предназначено только для справки. Это поле не используется программой для управления устройством.
Пользователь или группа пользователей	Вы можете указать учетную запись пользователя или группу пользователей, у которых есть доступ к выбранным USB-устройствам, несколькими способами: с помощью доменной службы Active Directory; с помощью списка пользователей и групп пользователей Сервера администрирования; добавлением вручную. Операционная система отображает все подключенные USB-устройства. Вы можете получить доступ только к USB-устройствам, для которых у вас есть соответствующие права доступа.
Описание	Описание устройства, заданное по умолчанию. При необходимости укажите в поле Описание дополнительную информацию о правиле. Например, уточните, на какие устройства должно распространяться правило.

Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах

Можно импортировать данные о заблокированных попытках подключения устройств из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика** (см. раздел "**Настройка задачи Контроль устройств**" на стр. 731), и применить эти данные для формирования списка разрешающих правил контроля устройств в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль устройств, вы можете отследить, подключение каких устройств будет блокироваться.

► *Чтобы задать разрешающие правила подключения устройств для группы защищаемых компьютеров на основе отчета Kaspersky Security Center о заблокированных устройствах, выполните следующие действия:*

1. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что выполняются следующие условия:
   - Для событий с уровнем важности **Критическое событие** срок хранения событий *Обнаружено и запрещено недоверенное устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

- Для событий с уровнем важности **Предупреждение** срок хранения событий *Только статистика: обнаружено недоверенное устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

> По завершении периода хранения событий, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль устройств в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленное время хранения указанных событий.

2. Запустите задачу Контроль устройств в режиме **Только статистика**.
   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.
   b. Нажмите на кнопку **Создать выборку** и создайте выборку событий по критерию *Обнаружено и запрещено недоверенное устройство*. Просмотрите, подключения каких устройств заблокированы задачей Контроль устройств.
   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных подключениях в файл формата TXT.

> Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех устройствах, подключение которых вы хотите разрешить.

3. Импортируйте данные о заблокированных попытках подключения устройств в задачу Контроль устройств.
   a. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 729).
   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать правила из файла отчета KSC о заблокированных устройствах**.
   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля устройств:

- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
- **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

   a. **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.
   b. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

4. Нажмите на кнопку **ОК** в окне **Контроль устройств**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

Создание правил с помощью задачи Формирование правил контроля устройств

► *Чтобы задать разрешающие правила контроля устройств для группы защищаемых компьютеров с помощью задачи Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Настройка** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам" на стр. 730).
2. Настройте следующие параметры:
   - В блоке **Режим**:
     - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
     - **Учитывать данные только об устройствах, подключенных в текущий момент**
   - В блоке **После завершения задачи**:
     - **Добавлять разрешающие правила в список правил контроля устройств**.

       Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

       По умолчанию флажок снят.

     - **Принцип добавления**.

       Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

       - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
       - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
       - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

       По умолчанию выбран способ **Объединять с существующими правилами**.

     - **Экспортировать разрешающие правила в файл**.

       Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Industrial CyberSecurity for Nodes экспортирует разрешающие правила в файл, указанный в поле ниже.

Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

По умолчанию флажок снят.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  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.

  По умолчанию флажок установлен.

3. Нажмите на кнопку **Далее**.
4. В окне **Расписание** укажите параметры запуска задачи по расписанию.
5. Нажмите на кнопку **Далее**.
6. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
7. Нажмите на кнопку **Далее**.
8. Укажите название задачи.
9. Нажмите на кнопку **Далее**.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

   Откроется окно **Завершение создания задачи**.
10. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
11. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.
12. На закладке **Задачи** в рабочей области настраиваемой группы защищаемых компьютеров в списке групповых задач выберите созданную задачу Формирование правил контроля устройств.
13. Нажмите на кнопку **Запустить** для запуска задачи.

    По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в папке общего доступа в файлах формата XML.

    При применении политики контроля устройств в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. Если применение сетевой папки общего доступа не предусмотрено политикой организации, рекомендуется запускать задачу Формирование правил контроля устройств в тестовой группе защищаемых компьютеров или на эталонной машине организации.

Добавление сформированных правил в список правил контроля устройств

► *Чтобы добавить сформированные списки разрешающих правил в задачу Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 729).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки **Добавить** выберите пункт **Импортировать правила из файла XML**.
4. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля устройств:
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
5. **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

   Все сформированные правила из XML-файла добавляются в список в соответствии с выбранным принципом.
7. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.
8. Если вы хотите применять созданные правила контроля устройств, в свойствах политики **Активный** выберите режим выполнения задачи **Контроль устройств**.

Разрешающие правила, автоматически сформированные на основе данных системы на каждом отдельном защищаемом компьютере, будут применены на всех защищаемых компьютерах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых компьютеров программа будет разрешать подключение только тех устройств, для которых созданы разрешающие правила.

Управление Контролем устройств с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

kaspersky

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы 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. Настройте задачу в соответствии с вашими требованиями.

Переход к окну с правилами контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
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. Настройте задачу в соответствии с вашими требованиями.

Настройка параметров задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль устройств**" на стр. 741).
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Industrial CyberSecurity for Nodes контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета 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 до запуска задачи Контроль устройств в режиме Активный, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**.

       Kaspersky Industrial CyberSecurity for Nodes не контролирует подключение съемных дисков 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 запоминающих устройств, если задача Контроль устройств не выполняется**.

Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется.

Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Industrial CyberSecurity for Nodes разрешает использовать любые внешние устройства на защищаемом компьютере.

Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом компьютере в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

По умолчанию флажок снят.

3. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания задач" на стр. 425).
4. Чтобы изменить список правил контроля устройств (см. раздел "О формировании правил контроля устройств" на стр. 724), перейдите по ссылке **Правила контроля устройств** в нижней части панели результатов узла **Контроль устройств**.

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

Настройка правил контроля устройств

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

В этом разделе

Импорт правил контроля устройств из файла формата XML

► *Чтобы импортировать правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. Нажмите на кнопку **Добавить**.

3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла 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**.
5. В окне **Открыть** выберите XML-файл, который содержит параметры правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила 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. 742), чтобы зафиксировать в журнале выполнения задачи все события подключения 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 разделе **Управление** в панели результатов узла **Контроль устройств**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Industrial CyberSecurity for Nodes создаст конфигурационный файл в формате XML со списком правил на основе событий, зарегистрированных при работе задачи Контроль устройств в режиме **Только статистика**. Можно применить этот список в задаче Контроль устройств (см. раздел "Импорт правил контроля устройств из файла формата XML" на стр. 743).

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, возникшие в ходе выполнения задачи, фиксируются в журнале выполнения задачи, независимо от режима. Вы можете создать конфигурационный файл со списком правил по результатам выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется сформировать финальную версию списка правил до запуска задачи в активном режиме.

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 правила для новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка разрешающих правил программа использует данные Windows обо всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает подключенные в текущий момент устройства.

► *Чтобы добавить разрешающее правило для внешних устройств, подключенных в данный момент, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню выберите пункт **Сформировать правила на основе данных системы**.
4. В открывшемся окне в списке обнаруженных устройств выберите устройство или несколько устройств, использование которых вы хотите разрешить на защищаемом компьютере.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

Удаление правил контроля устройств

► *Чтобы удалить правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. 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. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. 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.
4. 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 включить или выключить созданное правило контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
3. 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.
4. Нажмите на кнопку **ОК**.

Статус применения правила будет сохранен и отобразится для указанного правила.

kaspersky

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 внешних устройств.

► *Чтобы применить маску пути к экземпляру устройства в свойствах правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 741).
2. В открывшемся окне выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
3. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.
4. В открывшемся окне выполните следующие действия:
   - Установите флажок **Использовать маску** рядом с полем **Производитель (VID)**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанным производителем устройства.
   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанным типом контроллера.
   - Установите флажок **Использовать маску** рядом с полем **Серийный номер**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанными данными о серийном номере устройства.

   Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых установлен этот флажок, заменяются символом * и не учитываются при применении правила.
5. Укажите учетную запись пользователя или группу пользователей, у которых есть доступ к выбранным USB-устройствам. Операционная система отображает все подключенные USB-устройства. Вы можете получить доступ только к USB-устройствам, к которым у вас есть соответствующие права доступа.
6. Если требуется, введите дополнительную информацию о правиле в поле **Пользователь или группа пользователей**. Например, уточните, на какие устройства должно распространяться правило.
7. Нажмите на кнопку **ОК**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

kaspersky

Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Формирование правил контроля устройств**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Режим генерации** выберите режим работы задачи:
   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
   - **Учитывать данные только об устройствах, подключенных в текущий момент**
5. В разделе **По завершении задачи** укажите действия, которые программа Kaspersky Industrial CyberSecurity for Nodes должна выполнять по завершении задачи:
   - **Добавлять разрешающие правила в список правил контроля устройств**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

     По умолчанию флажок снят.
   - **Принцип добавления**.

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля устройств.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируются.
     - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
     - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

     По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

  Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Industrial CyberSecurity for Nodes экспортирует разрешающие правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

  По умолчанию флажок снят.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  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.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

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

Управление Контролем устройств с помощью Веб-плагина Консоли программы

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров задачи на защищаемом устройстве.

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Параметры** в подразделе **Контроль устройств**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 95. Параметры задачи Контроль устройств

Параметр	Описание
Активный	Kaspersky Industrial CyberSecurity for Nodes контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.
Только статистика	Kaspersky Industrial CyberSecurity for Nodes не контролирует подключение съемных дисков 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.
Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется	Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется. Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Industrial CyberSecurity for Nodes разрешает использовать любые внешние устройства на защищаемом компьютере. Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом компьютере в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. По умолчанию флажок снят.
Правила контроля устройств	Можно настраивать список правил контроля устройств (см. раздел "Настройка правил контроля устройств в Kaspersky Security Center" на стр. 733).
Управление задачами	Вы можете настроить расписание запуска задачи.

kaspersky

Управление сетевым экраном

Задача Управление сетевым экраном предоставляет графическую оболочку для управления брандмауэром Windows.

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

Если при установке Kaspersky Industrial CyberSecurity for Nodes брандмауэр Windows выключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы брандмауэр Windows включен, задача Управление сетевым экраном выполняется по завершении установки.

Запуск задачи Управление сетевым экраном невозможен, если брандмауэр Windows находится под управлением групповой политики Kaspersky Security Center.

Задача Управление сетевым экраном не фильтрует сетевой трафик самостоятельно, но предоставляет возможность управления брандмауэром Windows с помощью графического интерфейса Kaspersky Industrial CyberSecurity for Nodes.

Задача регулярно опрашивает брандмауэр Windows. По умолчанию интервал опроса составляет одну минуту и не может быть изменен.

В ходе выполнения задачи Управление сетевым экраном Kaspersky Industrial CyberSecurity for Nodes выполняет действия, определенные режимом взаимодействия с брандмауэром Windows:

- **Отслеживать статус работы брандмауэра Windows**. Программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.
- **Контролировать работу брандмауэра Windows**. Программа контролирует работу брандмауэра Windows в объеме, определенном следующими функциями:
    - **Поддерживать статус работы брандмауэра Windows**;

Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью ракрывающегося списка **Включен/Выключен** состоянии.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает состояние брандмауэра Windows.
- Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
- Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

По умолчанию функция включена и выбрано состояние **Включено**.

- **Управлять параметрами и правилами брандмауэра Windows**.

Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
- Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
- Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

  Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
- Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

kaspersky

О правилах сетевого экрана

Задача Управление сетевым экраном через брандмауэр Windows фильтрует сетевой трафик с помощью правил сетевого экрана, если установлен режим взаимодействия с брандмауэром Windows **Контролировать работу брандмауэра Windows**.

Правила сетевого экрана для приложений контролируют сетевые соединения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу приложения.

Правила сетевого экрана для портов контролируют сетевые соедниения для указанных портов и протоколов (TCP/UDP). Критериями срабатывания таких правил являются порт или диапазон портов и тип протокола.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая сетевые соединения с помощью правил для портов, вы снижаете уровень безопасности защищаемого компьютера.

Вы можете управлять правилами сетевого экрана:

- создавать и удалять правила сетевого экрана;
- изменять параметры правил сетевого экрана;
- включать и выключать правила сетевого экрана.

Создаваемые по умолчанию правила сетевого экрана

При установке Kaspersky Industrial CyberSecurity for Nodes создает набор разрешающих правил, предотвращающих блокировку программ, устанавливаемых вместе с Kaspersky Industrial CyberSecurity for Nodes. Ниже приведена подробная информация и описаны ограничения.

При установке на устройство с любой поддерживаемой версией Windows Kaspersky Industrial CyberSecurity for Nodes создает набор правил для входящих сетевых соединений:

- Разрешающие правила для Консоли Kaspersky Industrial CyberSecurity for Nodes (kavfsgt.exe), расположенной в папке установки программы. Статус: включено. Область применения правил: все адреса. Протоколы: TCP и UPD, по одному правилу на протокол.
- Два разрешающих правила для локального порта 15000, если на устройстве установлен Агент администрирования Kaspersky Security Center. Состояние: включено. Область применения правил: все адреса.. Протоколы: TCP и UPD, по одному правилу на протокол.

При установке на устройство с Windows 7 и выше Kaspersky Industrial CyberSecurity for Nodes создает набор правил для исходящих сетевых соединений:

- Разрешающие правила для Консоли Kaspersky Industrial CyberSecurity for Nodes (kavfsgt.exe), расположенной в папке установки программы. Статус: включено. Область применения правил: все адреса. Протоколы: TCP и UPD, по одному правилу на протокол.
- Разрешающие правила для Kaspersky Industrial CyberSecurity for Nodes (kavfswp.exe), расположенной в папке установки программы. Состояние: включено. Область применения правил: все адреса. Протоколы: TCP и UPD, по одному правилу на протокол.
- Два разрешающих правила для локального порта 13000, если на устройстве установлен Агент администрирования Kaspersky Security Center. Состояние: включено. Область применения правил: все адреса. Протоколы: TCP и UPD, по одному правилу на протокол.

kaspersky

Параметры по умолчанию для задачи Управление сетевым экраном

По умолчанию в задаче Управление сетевым экраном используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 96. Параметры по умолчанию для задачи Управление сетевым экраном

Параметр	Значение по умолчанию	Описание
Режим взаимодействия Kaspersky Industrial CyberSecurity for Nodes с брандмауэром Windows	**Отслеживать статус работы брандмауэра Windows**	Программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center уведомление, если брандмауэр Windows выключен.
Входящие соединения	**Блокировать**	Вы можете создавать и настраивать правила сетевого экрана для входящих соединений, чтобы блокировать или разрешать входящие соединения.
Исходящие соединения	**Разрешать**	Вы можете создавать и настраивать правила сетевого экрана для исходящих соединений, чтобы блокировать или разрешать исходящие соединения.
Разрешить ICMP-соединения	**Выключено**	Параметр разрешает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.
Расписание запуска задачи	Недоступно	Задача Управление сетевым экраном не запускается автоматически при запуске Kaspersky Industrial CyberSecurity for Nodes. Вы можете настроить запуск задачи по расписанию.

Настройка задачи Управление сетевым экраном с помощью Плагина управления

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью Плагина управления.

kaspersky

В этом разделе

Настройка общих параметров задачи Управление сетевым экраном

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** в блоке **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
5. На вкладке **Общие** в блоке **Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже** выберите режим взаимодействия Kaspersky Industrial CyberSecurity for Nodes с брандмауэром Windows:
   - **Отслеживать статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого компьютера.

- **Контролировать работу брандмауэра Windows**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:
  - **Поддерживать статус работы брандмауэра Windows**;

    Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью ракрывающегося списка **Включен/Выключен** состоянии.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает состояние брандмауэра Windows.
    - Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
    - Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

    Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

    По умолчанию функция включена и выбрано состояние **Включено**.
  - **Управлять параметрами и правилами брандмауэра Windows**.

    Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
    - Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
    - Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

      Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
    - Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

      Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

6. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 757).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
7. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.
   - При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 757).

     Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.
8. В блоке **Дополнительно** установите флажок **Разрешить ICMP-соединения**, если хотите, чтобы брандмауэр Windows разрешал входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.
9. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** в блоке **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
5. На вкладке **Общие** в блоке **Входящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. Создайте и настройте правила сетевого экрана для входящих соединений.
7. На вкладке **Приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для приложения**.
8. Настройте параметры правила:
   a. В поле **Имя правила** введите название правила.
   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
      - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для приложения.
   c. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.
   d. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

      Для IP-адресов поддерживается только формат IPv4.

   e. Нажмите на кнопку **ОК**, чтобы сохранить правило.
9. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для портов**.
10. Настройте параметры правила:
    a. В поле **Имя правила** введите название правила.
    b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
       - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для портов.
       - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для портов.

c. В блоке **Локальные порты** укажите порт или диапазон портов.

Для входящих сетевых соединений укажите порт или диапазон портов для локального устройства.

Для исходящих сетевых соединений укажите порт или диапазон портов для удаленных устройств.

Для номера порта доступны значения 1–65535.

Для диапазона номеров портов доступны значения 1–10, 20–30000 и 1–65535.

Windows XP не поддерживает диапазон портов. Поэтому для устройств из области применения правила, работающих по управлением Windows XP, программа применяет правило только к первому порту указанного диапазона.

d. Выберите тип протокола (TCP/UDP), для которого программа контролирует входящие сетевые соединения.

e. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

Для IP-адресов поддерживается только формат IPv4.

f. Нажмите на кнопку **ОК**, чтобы сохранить правило.

11. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **ОК**.
12. На вкладке **Общие** в блоке **Исходящие соединения** нажмите на кнопку **Список правил**.

    Откроется окно **Правила сетевого экрана для исходящих соединений**.
13. Создайте и настройте правила сетевого экрана для исходящих соединений.
14. В окне **Управление сетевым экраном** нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. В зависимости от типа правила, статус которого вы хотите изменить, перейдите по ссылке **Входящее** или **Исходящее**, а затем выберите закладку **Приложения** или **Порты**.
7. 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.
8. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.
9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
10. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

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. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
7. В списке правил выберите правило, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
9. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.
10. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
11. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Настройка задачи Управление сетевым экраном с помощью Консоли программы

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью интерфейса Консоли программы.

В этом разделе

kaspersky

Настройка общих параметров задачи Управление сетевым экраном

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Параметры**.

   Откроется окно **Параметры задачи**.
4. На вкладке **Общие** в блоке **Фильтрация сетевого трафика** выберите вариант взаимодействия Kaspersky Industrial CyberSecurity for Nodes с брандмауэром Windows:
   - **Отслеживать статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого компьютера.
   - **Контролировать работу брандмауэра Windows**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:
     - **Поддерживать статус работы брандмауэра**;

       Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью ракрывающегося списка **Включен/Выключен** состоянии.

       Если функция включена, программа выполняет следующие действия:

       - Опрашивает брандмауэр Windows с интервалом в одну минуту.
       - Считывает состояние брандмауэра Windows.
       - Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
       - Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

       Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

       По умолчанию функция включена и выбрано состояние **Включено**.
     - **Управлять параметрами и правилами брандмауэра Windows**.

       Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

       Если функция включена, программа выполняет следующие действия:

       - Опрашивает брандмауэр Windows с интервалом в одну минуту.
       - Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.

- Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
- Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

  Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
- Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

5. В блоке **Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже** настройте следующие параметры:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 764).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.

- При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 764).

  Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.

  Если Консоль программы подключена к локальному хосту под управлением Windows XP/Windows 2003/Windows Vista, параметр **Действие для исходящих соединений** и правила сетевого экрана для исходящих соединений недоступны для настройки.

6. В блоке **Дополнительно** установите флажок **Разрешать ICMP-соединения**, если хотите, чтобы брандмауэр Windows разрешал входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров фильтрации сетевого трафика.
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Входящие**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
4. Создайте и настройте правила сетевого экрана для входящих соединений.
5. На вкладке **Приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для приложения**.
6. Настройте параметры правила:
   a. В поле **Имя правила** введите название правила.
   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
      - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для приложения.
   c. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

d. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

e. Нажмите на кнопку **ОК**, чтобы сохранить правило.

7. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для портов**.

8. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:

   - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для портов.
   - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для портов.

   c. В блоке **Локальные порты** укажите порт или диапазон портов.

      Для входящих сетевых соединений укажите порт или диапазон портов для локального устройства.

      Для исходящих сетевых соединений укажите порт или диапазон портов для удаленных устройств.

      Для номера порта доступны значения 1–65535.

      Для диапазона номеров портов доступны значения 1–10, 20–30000 и 1–65535.

> Windows XP не поддерживает диапазон портов. Поэтому для устройств из области применения правила, работающих по управлением Windows XP, программа применяет правило только к первому порту указанного диапазона.

   d. Выберите тип протокола (TCP/UDP), для которого программа контролирует входящие сетевые соединения.

   e. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

   f. Нажмите на кнопку **ОК**, чтобы сохранить правило.

9. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **ОК**.

10. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Исходящие соединения**.

    Откроется окно **Правила сетевого экрана для исходящих соединений**.

11. Создайте и настройте правила сетевого экрана для исходящих соединений.

12. На вкладке **Приложения** нажмите на кнопку **Добавить**.

    Откроется окно **Правило сетевого экрана для приложения**.

13. Настройте параметры правила:

    a. В поле **Имя правила** введите название правила.

    b. В раскрывающемся списке **Действие правила** выберите один из вариантов:

    - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для приложения.
    - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для приложения.

    c. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

    d. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

    > Для IP-адресов поддерживается только формат IPv4.

    e. Нажмите на кнопку **ОК**, чтобы сохранить правило.

14. На вкладке **Порты** нажмите на кнопку **Добавить**.

    Откроется окно **Правило сетевого экрана для портов**.

15. Настройте параметры правила:

    a. В поле **Имя правила** введите название правила.

    b. В раскрывающемся списке **Действие правила** выберите один из вариантов:

    - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для портов.
    - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для портов.

    c. В блоке **Локальные порты** укажите порт или диапазон портов.

    Для входящих сетевых соединений укажите порт или диапазон портов для локального устройства.

    Для исходящих сетевых соединений укажите порт или диапазон портов для удаленных устройств.

    Для номера порта доступны значения 1–65535.

    Для диапазона номеров портов доступны значения 1–10, 20–30000 и 1–65535.

> Windows XP не поддерживает диапазон портов. Поэтому для устройств из области применения правила, работающих по управлением Windows XP, программа применяет правило только к первому порту указанного диапазона.

    d. Выберите тип протокола (TCP/UDP), для которого программа контролирует входящие сетевые соединения.

e. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

f. Нажмите на кнопку **ОК**, чтобы сохранить правило.

16. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров задачи сохранится в журнале системного аудита.

Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, статус которого вы хотите изменить, перейдите по ссылке **Входящее** или **Исходящее**, а затем выберите закладку **Приложения** или **Порты**.
5. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.
6. В окне **Сохранить** нажмите на кнопку **Правила сетевого экрана**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

kaspersky

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 программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
5. В списке правил выберите правило, которое вы хотите удалить.
6. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
7. В окне **Сохранить** нажмите на кнопку **Правила сетевого экрана**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Настройка задачи Управление сетевым экраном с помощью Веб-плагина

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью Веб-плагина.

В этом разделе

kaspersky

Настройка общих параметров задачи Управление сетевым экраном

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. В разделе **Управление сетевым экраном** нажмите на кнопку **Параметры**.

   Откроется окно **Управление сетевым экраном**.
6. На вкладке **Общие** в блоке **Интеграция с брандмауэром Windows** выберите вариант взаимодействия Kaspersky Industrial CyberSecurity for Nodes с брандмауэром Windows:

   - **Отслеживать статус работы брандмауэра Windows Программа только отслеживает статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого компьютера.
   - **Контролировать работу брандмауэра Windows Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:

     - **Поддерживать статус работы брандмауэра Windows**;

Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью ракрывающегося списка **Включен/Выключен** состоянии.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает состояние брандмауэра Windows.
- Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
- Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

По умолчанию функция включена и выбрано состояние **Включено**.

- **Управлять параметрами и правилами брандмауэра Windows**.

Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
- Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
- Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

  Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
- Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

1. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 771).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
2. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.
   - При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 771).

     Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.

3. В блоке **Дополнительно** установите флажок **Разрешить ICMP-соединения**, если хотите, чтобы брандмауэр Windows разрешал входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Таблица 97.

Параметр	Описание
Правила сетевого экрана для приложений	Вы можете управлять правилами для программ. Правила этого типа выборочно разрешают сетевые подключения для указанных программ. Критерием срабатывания таких правил является путь к исполняемому файлу.
Правила сетевого экрана для портов	Вы можете управлять правилами 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.
Управление задачей	Вы можете настроить расписание запуска задачи.

Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. В блоке **Управление сетевым экраном** нажмите на кнопку **Параметры**.

   Откроется окно **Управление сетевым экраном**.
6. Создайте и настройте правило сетевого экрана для входящих соединений для приложения.
7. Создайте и настройте правило сетевого экрана для входящих соединений для портов.
8. Создайте и настройте правило сетевого экрана для исходящих соединений для приложения.

9. Создайте и настройте правило сетевого экрана для исходящих соединений для портов.
10. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Правила сетевого экрана для приложений** или **Правила сетевого экрана для портов**.
7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, включите переключатель слева от имени правила.
   - Если вы хотите, чтобы активное правило не применялось, выключите переключатель слева от имени правила.
8. Нажмите на кнопку **OK**.

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 главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Правила сетевого экрана для приложений** или **Правила сетевого экрана для портов**.
7. В списке правил выберите правило, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
9. Нажмите на кнопку **ОК**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

kaspersky

Использование KSN

В сертифицированной версии программы используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

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

В этом разделе

О задаче Использование KSN

Kaspersky Security Network (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Industrial CyberSecurity for Nodes 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 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 подробная информация о передаче, обработке, хранении и уничтожении информации об использовании программы приведена в окне **Обработка данных** задачи Использование KSN и в Политике 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. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network можно использовать в следующих задачах Kaspersky Industrial CyberSecurity for Nodes:

- Постоянная защита файлов.
- Проверка по требованию.
- Правила контроля запуска программ.

Kaspersky Private Security Network

Подробная информация о настройке Kaspersky Private Security Network (далее также "Локальный KSN") приведена в *Справке Kaspersky Security Center*.

Если вы используете Локальный KSN на устройстве, в окне **Обработка данных** (см. раздел "**Настройка обработки данных**" на стр. 779) задачи Использование KSN можно ознакомиться с Положением о KSN и включить использование компонента, установив флажок **Я принимаю условия использования Kaspersky Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KSN (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 выполнения задачи Использование KSN, происходит ошибка *Нарушение лицензии* и выполнение задачи прекращается. Чтобы продолжить защищать устройство, вам нужно принять Положение о KSN в окне **Обработка данных** 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 службу 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 использования 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: обработка всех связанных с KSN данных останавливается.
- Вы удалили лицензионный ключ Kaspersky Industrial CyberSecurity for Nodes или приостановили использование лицензии: обработка всех связанных с KSN данных останавливается.

Параметры по умолчанию для задачи Использование KSN

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

Таблица 98. Параметры по умолчанию для задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Industrial CyberSecurity for Nodes 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 рассчитывает MD5-хеш для файлов любого размера.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.
Использовать Kaspersky Security Center в качестве прокси-сервера KSN	Выбрано.	По умолчанию все данные отправляются в KSN через Kaspersky Security Center. Этот параметр можно изменять только с помощью Плагина управления.
Я принимаю условия использования Kaspersky Security Network	Флажок снят	Если флажок установлен, от вас получено согласие на участие в KSN после установки программы. Вы можете изменить 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.

Параметр	Значение по умолчанию	Описание
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.

Управление использованием KSN с помощью Плагина управления

В этом разделе описана настройка использования KSN и обработки данных с помощью Плагина управления.

В этом разделе

Настройка параметров задачи Использование KSN

Вы можете изменять параметры обработки данных, заданные по умолчанию (см. таблицу ниже).

Таблица 99. Параметры обработки данных, заданные по умолчанию

Параметр	Значение по умолчанию	Описание
Я принимаю условия использования Kaspersky Security Network	Флажок снят	Если флажок установлен, от вас получено согласие на участие в KSN после установки программы. Вы можете изменить 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.

► *Чтобы настроить задачу Использование KSN, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Использование KSN**.

   Откроется окно **Использование KSN**.
5. На закладке **Общие** настройте следующие параметры задачи:
   - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Industrial CyberSecurity for Nodes при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалять**

       Kaspersky Industrial CyberSecurity for Nodes 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 фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Industrial CyberSecurity for Nodes не удаляет недоверенный объект.
   - В разделе **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 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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 будет рассчитывать контрольную сумму.

- В разделе **Прокси-сервер KSN** снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

  Флажок позволяет управлять передачей данных от защищаемых компьютеров в KSN.

  Если флажок снят, данные с Сервера администрирования и защищаемых компьютеров отправляются в KSN напрямую (минуя Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую.

  Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center.

  По умолчанию флажок установлен.

Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Справке Kaspersky Security Center*.

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

   Программа будет запускать задачу Использование KSN по расписанию.

7. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных" на стр. 779).
8. 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. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Обработка данных** в подразделе **Использование KSN**.

   Откроется окно **Обработка данных в KSN**.

5. Прочитайте Положение о KSN (или Положение о KPSN, если вы используете Локальный KSN).

6. Если вы принимаете условия Положения 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 Локального KSN;
   - при переключении с Локального KSN на Глобальный KSN.

   Чтобы включить службы KSN, примите Положение о KSN снова.

7. Для повышения уровня защиты следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**

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

     Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом компьютере. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *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 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 не отправляет дополнительную статистику.

  По умолчанию флажок установлен.

Если вы приняли Положение KSN, флажки **Разрешить отправку данных о проверяемых файлах** и **Разрешить отправку статистики Kaspersky Security Network** будут недоступны.

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

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

Нажмите на кнопку **OK**.

Управление использованием KSN с помощью Консоли программы

В этом разделе описана настройка использования KSN и обработки данных с помощью Консоли программы.

В этом разделе

Настройка задачи Использование KSN с помощью Консоли программы

► *Чтобы настроить задачу Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы 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 разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Industrial CyberSecurity for Nodes при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалять**

       Kaspersky Industrial CyberSecurity for Nodes 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 фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Industrial CyberSecurity for Nodes не удаляет недоверенный объект.
   - В разделе **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 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 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 будет рассчитывать контрольную сумму.
5. Если требуется, настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

   Программа будет запускать задачу Использование KSN по расписанию.
6. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. 783).
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 системного аудита.

kaspersky

Настройка обработки данных с помощью Консоли программы

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

1. В дереве Консоли программы 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. На закладке **Службы и статистика KSN** прочитайте текст Положения и установите флажок **Я принимаю условия использования Kaspersky Security Network**.
5. Для повышения уровня защиты, флажок **Разрешить отправку данных о проверяемых файлах** устанавливается автоматически.

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

   Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом компьютере. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

   По умолчанию флажок установлен.

   Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.
6. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes отправляла дополнительную статистику в "Лабораторию Касперского".

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

   По умолчанию флажок установлен.
7. Нажмите на кнопку **OK**.

Конфигурация обработки данных будет сохранена.

Управление использованием KSN с помощью Веб-плагина

► *Чтобы настроить использование KSN и обработку данных с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Использование KSN**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 100. Настройка параметров задачи Использования KSN и обработки данных с помощью Плагина управления

Параметр	Описание
Удалять	Kaspersky Industrial CyberSecurity for Nodes 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 фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Industrial CyberSecurity for Nodes не удаляет недоверенный объект.
Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает	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 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ). Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму для файлов любого размера. По умолчанию флажок установлен.

Параметр	Описание
Использовать Kaspersky Security Center в качестве прокси-сервера KSN	Флажок позволяет управлять передачей данных от защищаемых компьютеров в KSN. Если флажок снят, данные с Сервера администрирования и защищаемых компьютеров отправляются в KSN напрямую (минуя Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую. Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center. По умолчанию флажок установлен.
Принять условия Положения о Kaspersky Security Network	Устанавливая этот флажок, вы подтверждаете, что прочитали и принимаете условия Положения о Kaspersky Security Network.
Разрешить отправку данных о проверяемых файлах	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 не отправляет контрольные суммы файлов в KSN. Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом компьютере.

Параметр	Описание
	Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*. По умолчанию флажок установлен.
Разрешить отправку данных о запрашиваемых веб-адресах	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отправляет данные о запрашиваемых веб-ресурсах, включая веб-адреса, в "Лабораторию Касперского". Заключение о безопасности запрашиваемых веб-ресурсов основано на репутации, полученной от KSN. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не проверяет репутацию веб-адресов в KSN. По умолчанию флажок установлен. Флажок влияет на настройку задачи Защита трафика.
Разрешить отправку статистики Kaspersky Security Network	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 не отправляет дополнительную статистику. По умолчанию флажок установлен.

Параметр	Описание
Принять условия Положения о Kaspersky Managed Protection	Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого компьютера специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности. По умолчанию флажок снят.
Управление задачей	Вы можете настроить расписание запуска задачи.

Настройка передачи дополнительных данных

В Kaspersky Industrial CyberSecurity for Nodes 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 с помощью Консоли программы" на стр. 783), только если установлен флажок **Я принимаю условия использования Kaspersky Security Network**.

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

Таблица 101. 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	**Условия для состояния флажка** Я принимаю условия использования Kaspersky Security Network
☑	• отправляются запросы репутации • действия с флажком доступны	• отправляется дополнительная статистика • действия с флажком доступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны
☑	• отправляются запросы репутации • действия с флажком недоступны	• отправляется дополнительная статистика • действия с флажком недоступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком недоступны
☐	• не отправляются запросы репутации • действия с флажком доступны	• не отправляется дополнительная статистика • действия с флажком доступны	• не принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны
☐	• не отправляются запросы репутации • действия с флажком недоступны	• не отправляется дополнительная статистика • действия с флажком недоступны	• не принимаются условия Положения о Kaspersky Security Network • 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 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. 956).

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

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 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 обработала за время выполнения задачи (см. таблицу ниже).

Таблица 102. Статистика задачи Использование KSN

Поле	Описание
Отправлено файловых запросов	Количество запросов о репутации файла, отправленных Kaspersky Industrial CyberSecurity for Nodes в KSN.
Недоверенных заключений по файлам	Количество объектов, признанных недоверенными в KSN.
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Пакетов статистик сформировано	Количество пакетов с данными, которые были отправлены на обработку в KSN.
Удалено объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes удалила в результате выполнения задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes сохранила в резервном хранилище.
Объектов не удалено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 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 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. В ограниченном режиме Kaspersky Industrial CyberSecurity for Nodes отправляет только часть запросов о репутации файлов, в соответствии с рекомендациями специалистов "Лаборатории Касперского".

kaspersky

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Мониторинг файловых операций.

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 из-за физического отсутствия внешнего устройства на защищаемом компьютере. Kaspersky Industrial CyberSecurity for Nodes сообщит об обнаружении файловых операций в области мониторинга, как только внешнее 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 должна использоваться файловая система ReFS или 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 Мониторинг файловых операций, вам нужно перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 828). 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 правила и регулировать уровень важности событий для обнаруженных файловых операций, регистрируемых 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.

Статус *Недоверенный пользователь* присваивается всем пользователям, не указанным в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи.

Статус *Доверенный пользователь* присваивается пользователю или группе пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes 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 не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Статус *Неизвестный пользователь* присваивается пользователю в случае, когда Kaspersky Industrial CyberSecurity for Nodes не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Industrial CyberSecurity for Nodes 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 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 зарегистрирует 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 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см. таблицу ниже).

Таблица 103. 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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Параметры по умолчанию для задачи Мониторинг файловых операций

По умолчанию в задаче Мониторинг файловых операций используются параметры, описанные в таблице ниже. Вы можете изменять значения параметров с помощью:

- Плагина управления (см. раздел "Управление мониторингом файловых операций с помощью Плагина управления" на стр. 795)
- Консоли программы
- Веб-плагина (см. раздел "Управление мониторингом файловых операций с помощью Веб-плагина" на стр. 805)

Таблица 104. Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Этот параметр используется, чтобы задавать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список **Доверенные пользователи**	Не задано	Этот параметр используется, чтобы задавать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.
Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга	Применяется	Этот параметр используется для включения или выключения записи в журнал файловых операций, выполненных в указанных областях мониторинга в периоды простоя задачи. По умолчанию собирается статистика для недоверенных и неизвестных пользователей и объектов.

Параметр	Значение по умолчанию	Описание
Блокировать попытки компрометации журнала USN	Применяется	Этот параметр используется, чтобы включать и выключать защиту USN-журнала.
Обнаруживать и блокировать все файловые операции в выбранной области	Выключено	Установите или снимите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**, чтобы блокировать все изменения для выбранной области мониторинга.
Исключить следующие папки из области контроля	Не применяется	Этот параметр используется, чтобы контролировать применение исключений для папок, в которых не требуется контролировать за файловые операции. При выполнении задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes пропускает области мониторинга, заданные в качестве исключений.
Контрольная сумма	Не применяется	Этот параметр используется, чтобы настроить расчет контрольной суммы файла после внесения изменений.
Маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Этот параметр используется, чтобы указать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Industrial CyberSecurity for Nodes формирует событие аудита.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настроить расписание запуска задачи.

Управление мониторингом файловых операций с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Плагина управления.

В этом разделе

kaspersky

Настройка парметров задачи Мониторинг файловых операций

► *Чтобы настроить параметры задачи Мониторинг файловых операций с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.
5. На вкладке **Параметры мониторинга файловых операций** настройте следующие параметры:
   - 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 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.
   - Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

     Этот флажок включает или выключает защиту USN-журнала.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

     Если флажок снят, программа не контролирует изменения в USN-журнале.

     По умолчанию флажок установлен.
6. Добавьте правила мониторинга файловых операций (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 828), в соответствии с которыми работает задача.
7. На вкладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. 404).

8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. Выполните одно из следующих действий:
   - Если вы создаете правило мониторинга файловых операций в политике, в разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
   - Если вы создаете правило мониторинга файловых операций для локальной задачи, в окне **Свойства: Мониторинг файловых операций** перейдите в раздел **Настройка**.
5. В блоке **Область мониторинга** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга файловых операций**.
6. Добавьте область мониторинга файловых операций одним из следующих способов:
   - Если вы хотите выбрать папку или диск через стандартный диалог Microsoft Windows:
     a. Нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Выбрать папку**.
     b. Выберите папку, файловые операции в которой вы хотите контролировать.
     c. Нажмите на кнопку **ОК**.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.

- <\dir*> – все файлы в папке <\dir>.
- <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Industrial CyberSecurity for Nodes не добавит указанную область мониторинга.

7. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** в контекстном меню кнопки **Добавить** выберите способ добавления доверенных пользователей.

      Откроется окно **Выбор пользователя или группы пользователей**.

   b. Выберите пользователя или группу пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга.
   c. Нажмите на кнопку **ОК**.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 791), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

8. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:
   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 791) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

9. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.
10. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:
    a. Установите флажок **Рассчитывать контрольную сумму файла после файловой операции, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

- **Хеш MD5**;
- **Хеш SHA256**.

11. Если необходимо, добавьте папки или диски для исключения из выбранной области контроля файловых операций:

a. На вкладке **Исключения** установите флажок **Исключить следующие папки из области контроля**.

Флажок 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 пропускает области мониторинга, указанные в списке исключений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes фиксирует события для всех указанных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

b. Нажмите на кнопку **Добавить**.

Откроется окно **Исключение из области контроля**.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Выбрать папку**.

d. Выберите папку или диск.

e. Нажмите на кнопку **ОК**.

Указанная папка или диск отобразится в списке исключений на вкладке **Исключения**.

> Вы можете добавить исключения для области мониторинга файловых операций вручную, используя те же маски, что и для задания областей мониторинга файловых операций.

12. В окне **ОК** нажмите на кнопку **Правило мониторинга файловых операций**.

Настроенное правило мониторинга файловых операций отобразится в окне **Мониторинг файловых операций** / **Свойства: Монторинг файловых операций** в блоке **Область мониторинга**.

Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. Выполните одно из следующих действий:
   - Если вы хотите импортировать или экспортировать правила мониторинга файловых операций в политике, в разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
   - Если вы хотите импортировать или экспортировать правила мониторинга файловых операций для локальной задачи, в окне **Свойства: Мониторинг файловых операций** перейдите в раздел **Настройка**.
5. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление мониторингом файловых операций с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Консоли программы.

kaspersky

В этом разделе

Настройка параметров задачи Мониторинг файловых операций

► *Чтобы настроить общие параметры задачи Мониторинг файловых операций с помощью Консоли программы*

1. В дереве Консоли программы 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. На вкладке **Общие** настройте следующие параметры:
   a. 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 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.

   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

      Этот флажок включает или выключает защиту USN-журнала.

      Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

      Если флажок снят, программа не контролирует изменения в USN-журнале.

      По умолчанию флажок установлен.
5. На владках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404).
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

kaspersky

Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Правила мониторинга файловых операций** перейдите по ссылке **Мониторинг файловых операций**.

   Откроется окно **Правила мониторинга файловых операций**.
4. Укажите путь для области мониторинга файловых операций одним из следующих способов:
   - Если вы хотите выбрать папку или диск через стандартный диалог Microsoft Windows:
     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Выбрать папку**.
     b. Выберите папку, файловые операции в которой вы хотите контролировать.
     c. Нажмите на кнопку **ОК**.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.
     - <\dir*> – все файлы в папке <\dir>.
     - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Industrial CyberSecurity for Nodes не добавит указанную область мониторинга.
5. Нажмите на кнопку **Добавить**.

   Область мониторинга отобразится в списке в левой части окна **Правила мониторинга файловых операций**.
6. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

      Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
   b. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами из выбранной области мониторинга.

c. Нажмите на кнопку **OK**.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 791), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

7. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:

   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.

   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 791) установите флажки напротив тех операций, которые вы хотите контролировать.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

8. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области мониторинга, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.

9. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:

   a. В блоке **Контрольная сумма** выберите **Рассчитывать контрольную сумму измененного файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.**Рассчитывать контрольную сумму измененного файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

      Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

      Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не рассчитывает контрольную сумму измененных файлов.

      Расчет контрольной суммы не выполняется в следующих случаях:

      - если файл стал недоступен (например, в результате изменения прав доступа к файлу);
      - если файловая операция обнаружена в файле, который впоследствии был удален.

      По умолчанию флажок снят.

      Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

      Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех

изменений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих вариантов:

- **Хеш MD5**;
- **Хеш SHA256**.

10. Если необходимо, добавьте папки или диски для исключения из мониторинга файловых операций:

a. На вкладке **Исключения** установите флажок **Учитывать исключенные области мониторинга**.

Флажок 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 пропускает области мониторинга, указанные в списке исключений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes фиксирует события для всех указанных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

b. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Выбрать папку**.

c. Выберите папку или диск.

d. Нажмите на кнопку **ОК**.

e. Нажмите на кнопку **Добавить**.

Указанная папка или диск отобразится в списке исключений.

> Вы можете добавить исключения для области мониторинга файловых операций вручную, используя те же маски, что и для задания областей мониторинга файловых операций.

11. Нажмите на кнопку **Сохранить**.

Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Правила мониторинга файловых операций** перейдите по ссылке **Мониторинг файловых операций**.

   Откроется окно **Правила мониторинга файловых операций**.
4. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление мониторингом файловых операций с помощью Веб-плагина

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Веб-плагина.

В этом разделе

Настройка параметров задачи Мониторинг файловых операций

► *Чтобы настроить параметры задачи Мониторинг файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг файловых операций**.

6. На вкладке **Параметры мониторинга файловых операций** настройте следующие параметры:
   a. 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 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.

   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

      Этот флажок включает или выключает защиту USN-журнала.

      Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

      Если флажок снят, программа не контролирует изменения в USN-журнале.

      По умолчанию флажок установлен.
7. На вкладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404).
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
6. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга файловых операций**.

7. В поле **Выполнять мониторинг файловых операций для области** укажите путь с помощью одной из поддерживаемых масок:

   - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
   - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.
   - <\dir*> – все файлы в папке <\dir>.
   - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Industrial CyberSecurity for Nodes не добавит указанную область мониторинга.

8. На вкладке **Доверенные пользователи**, если необходимо, задайте доверенных пользователей одним из следующих способов:

   - С помощью кнопки **Добавить**:
     a. Нажмите на кнопку **Добавить**.
     b. В открывшемся окне в поле **Имя пользователя** укажите пользователя или группу пользователей в формате SID.
     c. Нажмите на кнопку **ОК**.
   - С помощью кнопки **Добавить из списка Сервера администрирования**:
     a. Нажмите на кнопку **Добавить из списка Сервера администрирования**.
     b. В открывшемся окне выберите пользователя или группу пользователей из списка.
     c. Нажмите на кнопку **ОК**.

   Доверенным пользователям разрешены операции с файлами из выбранной области мониторинга.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 791), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

9. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:

   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 791) установите флажки напротив тех операций, которые вы хотите контролировать.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области мониторинга, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.
11. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:
    a. Установите флажок **Рассчитывать контрольную сумму файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не рассчитывает контрольную сумму измененных файлов.

       Расчет контрольной суммы не выполняется в следующих случаях:

       - если файл стал недоступен (например, в результате изменения прав доступа к файлу);
       - если файловая операция обнаружена в файле, который впоследствии был удален.

       По умолчанию флажок снят.

    b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

       - **Хеш SHA256**;
       - **Хеш MD5**.

12. Если необходимо, добавьте папки или диски для исключения из мониторинга файловых операций:
    a. На вкладке **Исключения** установите флажок **Исключить следующие папки из области контроля**.

       Флажок 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 пропускает области мониторинга, указанные в списке исключений.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes фиксирует события для всех указанных областей мониторинга.

       По умолчанию флажок снят, список исключений пуст.

    b. Нажмите на кнопку **Добавить**.

    c. В открывшемся справа окне в поле **Имя папки** введите путь к папке или диску, который вы хотите исключить из области мониторинга файловых операций.

    d. Нажмите на кнопку **OK**.

    Путь к указанной папке или диску отобразится в списке.

13. В окне **Правило мониторинга файловых операций** нажмите на кнопку **OK**.

Настроенное правило мониторинга файловых операций отобразится в окне **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.

Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
6. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
7. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Портативный сканер

Портативный сканер выполняет проверку изолированных устройств на присутствие вирусов и других программ, представляющих угрозу.

С помощью портативного сканера вы можете выполнять проверку нескольких устройств подряд – компонент формирует отдельный отчет для каждого проверяемого устройства. Портативный сканер применяет установленный по умолчанию уровень безопасности – *Лечить. Удалять, если не удалось*.

В этом разделе

Требования для создания портативного сканера

Ниже приведены требования для создания Портативный сканер:

- Подключаемый по USB съемный диск с 2 ГБ свободного места.
- Установленная программа Kaspersky Industrial CyberSecurity for Nodes с компонентом Портативный сканер.
- Действительная лицензия на Kaspersky Industrial CyberSecurity for Nodes.
- Действительная лицензия на Kaspersky Industrial CyberSecurity for Nodes Portable Scanner.

Создание Портативного сканера

Перед созданием Портативного сканера убедитесь, что задача обновления баз программы не выполняется или завершена.

► *Чтобы создать Портативный сканер:*

1. В области уведомлений в контекстном меню значка программы выберите **Открыть Диагностическое окно**.
2. В открышемся диагностическом окне нажмите на ссылку **Создать Портативный сканер**.

   Откроется окно **Параметры Портативного сканера** с предложением выбрать файл лицензии.

3. Нажмите **Файлы лицензионного ключа (*.key)**, чтобы в открывшемся окне добавить файл лицензии портативного сканера Kaspersky Industrial CyberSecurity for Nodes.

   После добавления файла лицензии отображается информация о лицензировании.

4. Нажмите на кнопку **Далее**.
5. В окне **Параметры Портативного сканера** задайте область проверки. По умолчанию в область проверки добавляется **Мой компьютер**. Если вы хотите добавить другие области проверки, нажмите на кнопку **Добавить**. В открывшемся окне Область проверки выберите необходимые элементы и нажмите на кнопку **ОК**, чтобы сохранить изменения.
6. В окне **Параметры Портативного сканера** нажмите на кнопку **Параметры сканирования**.

   Откроется окно **Параметры сканирования**.

   a. На вкладке **Общие** выберите подходящие варианты:

      - **Сканировать объекты**.
      - **Проверка составных объектов**.

   b. На вкладке **Дополнительно** выберите подходящие варианты:

      - **Общие параметры**.
      - **Папка для временных файлов, создаваемых при сканировании**.
      - **Действия над обнаруженными объектами**.
      - **Действия над составными файлами, недоступными для изменения**.

   c. На вкладке **Производительность** выберите подходящие варианты:

      - **Исключения**.
      - **Дополнительные параметры**.

7. Нажмите на кнопку **Далее**.
8. В раскрывающемся списке выберите съемный диск, чтобы создать Портативный сканер. Система автоматически обновит список доступных съемных дисков и проверит, доступно ли на выбранном диске 2 ГБ свободного места. Подключаемый по USB съемный диск должен быть доступен для записи.
9. Если применимо, выберите **Верифицировать данные сканера после записи**.

   Используйте этот параметр для проверки данных сканера. Например, если вы планируете создать несколько портативных сканеров с одинаковыми параметрами подряд, проверка данных для первого портативного сканера и обнаружение расхождений на ранней стадии позволят сэкономить время. По умолчанию этот параметр выключен.

10. Нажмите на кнопку **Создать**, чтобы завершить работу мастера.

Мастер проверяет, доступно ли 2 ГБ свободного места на выбранном диске, и записывает Портативный сканер. Если на диске уже есть Портативный сканер и требуется установить новый Портативный сканер с другими параметрами, мастер установки перезаписывает файлы существующего портативного сканера, за исключением файлов отчетов и журналов. Если на диске менее 2 ГБ свободного места, вы можете удалить с диска отдельные файлы или существующий Портативный сканер, чтобы освободить необходимое пространство и создать новый Портативный сканер.

Если вы решите прервать запись, мастер установки прекратит запись без отката изменений.

После завершения установки мастер прдложит создать следующий Портативный сканер. Чтобы создать следующий Портативный сканер, повторите процедуру установки, начиная с шага 3. В противном случае мастер установки закроется.

После установки портативного сканера на подключаемом по USB съемном диске появятся следующие файлы:

- **Kavscan** – папка, содержащая утилиту проверки, файлы программы, файлы настроек, антивирусные базы и отчеты.
- **kavscan.exe** – утилита проверки.
- **startscan.cmd** – командный файл для запуска утилиты проверки без открытия терминального окна.
- **Bases** – папка с антивирусными базами Kaspersky Industrial CyberSecurity for Nodes, актуальными на дату записи портативного сканера на подключаемый по USB съемный диск.

Запуск портативного сканера из командной строки

Вы можете запустить только Портативный сканер, записанный на исходный съемный диск, подключаемый по USB. Если вы скопируете портативный сканер на другой подключаемый по USB съемный диск, запустить его не получится.

► *Чтобы запустить портативный сканер, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, с помощью команды `cmd.exe`) с правами локального администратора.
2. С помощью команды `cd` перейдите в папку, в которой находится файл kavscan.exe.

   Например, вы можете ввести команду `cd "[drive]:\Kavscan"` и нажать **ENTER**.
3. Выполните одну из следующих команд и нажмите **ENTER**:

   `kavscan.exe` **help**

   `kavscan.exe` **scan** `[/mycomputer] [/fixed] [/removable] [/remote] [/shared] [/memory] [/startup] [/drive=<диск>] [/folder=<проверяемая папка>] [/file=<имя файла>] [/trace] [/dump] [/report=<тип>] [/cure={yes|no}] [/settings=< полный путь к файлу с пользовательскими настройками>]`

   `kavscan.exe` **update** `[/source=<имя_папки_с_обновлениями_баз>]`

Параметр	Описание
<режим>	Режим Портативный сканер. Доступные значения: **help** – вызов справки и получение дополнительной информации о доступных параметрах. **scan** – проверка выбранной области на устройстве. **update** – обновление антивирусных баз. Если значение не задано, Портативный сканер не запускается и возвращает следующее уведомление: "*Режим не задан. Для вызова справки запустите команду kavscan.exe help*".
/mycomputer	Проверка всего компьютера.
/fixed	Проверка всех жестких дисков.
/removable	Проверка всех съемных дисков.
/remote	Проверка всех удаленных дисков.
/shared	Проверка общих папок.
/memory	Проверка всех процессов памяти.
/startup	Проверка объектов автозапуска.
/drive=<диск>	Проверка всех загрузочных секторов и файлов на указанном диске.
/folder=<имя_папки_для_проверки>	Проверка указанной папки. В качестве значения этого параметра нельзя использовать шаблон метки папки.
/file=<имя_файла>	Проверка указанного файла.
/trace	Включает трассировку.
/dump	Включает запись дампа.
/report=<тип>	Определяет тип возвращаемого отчета. Доступны следующие значения: **full** – полный отчет о проверке со всеми типами событий. **critical** – отчет о проверке содержит только критические события. **short** – отчет о проверке содержит общую статистику и не содержит данных о событиях. По умолчанию применяется тип short.

/cure={yes|no}	Определяет режим проверки. Доступны следующие значения: **yes** – проверка с последующим лечением. Если параметр не задан, применяется режим, заданный в настройках. **no** – проверка в режиме обнаружения. Если параметр не задан, применяется режим, заданный в настройках.
/settings=<полный путь к файлу пользовательских настроек>	Применяет пользовательские настройки из файла <полный_путь_к_файлу_пользовательских_настроек>. Если значение не задано, сканер применяет настройки по умолчанию из файла <путь_к_программе>\Settings.dat.
/source=<имя_папки_с_обновлениями_баз>	Определяет источник, из которого Портативный сканер получает обновления в режиме обновления. Если значение не задано, обновление не выполняется.

Коды возврата команды kavscan.exe scan:

- 0 – команда успешно выполнена.
- 1 – общая ошибка.

Если выполнение команды завершено успешно (код 0), в папке **Kavscan** будет доступен отчет в формате kics_report_<имя_проверяемого_устройства>_<дата_время>.txt.

Изменение настроек портативного сканера

► *Чтобы изменить настройки портативного сканера:*

1. Сохраните существующий файл settings.dat под другим именем, например custom_settings.dat.
2. Создайте новый портативный сканер (см. раздел "Создание Портативного сканера" на стр. 810) с требуемыми настройками.

   После создания нового Портативный сканер создается новый файл settings.dat с необходимыми настройками. Он расположен в папке **Kavscan** нового Портативный сканер.
3. Скопируйте сформированный файл settings.dat в удобную вам папку.

   В результате у вас будет существующий Портативный сканер с двумя файлами настроек.
4. Запустите **Портативный сканер** из командной строки и укажите путь к требуемому файлу с настройками.

kaspersky

Обновление антивирусных баз данных для портативного сканера

Обновление антивирусных баз **Портативный сканер** из командной строки возможно только при наличии действующей лицензии Kaspersky Industrial CyberSecurity for Nodes.

► *Чтобы обновить антивирусные базы портативного сканера:*

1. Выберите один из следующих вариантов:

   - Обновление баз с помощью хранилищ точек распространения.

     В этом случае создайте или настройте задачу "Обновление баз" для устройства или группы устройств, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes, и запустите задачу.

   - Обновление баз с помощью Kaspersky Updater Utility (KUU).

     В этом случае используйте KUU для загрузки обновлений в папку на устройстве.

2. После загрузки обновлений выполните команду `kavscan.exe update /source=<имя папки с обновлениями баз>`, где <имя папки с обновлениями баз> – это хранилище точек распространения или локальная папка с загруженными обновлениями, в зависимости от варианта, выбранного на предыдущем шаге.

   Портативный сканер обновляет базы в папке **Bases** и выполняет проверку баз. В результате сканер отправляет уведомление об успешном обновлении или о проблемах при проверке.

Просмотр результатов работы портативного сканера

После завершения проверки создается папка **Results**. Она имеет следующую структуру:

- <имя проверяемого устройства> – папка, названная именем проверяемого устройства и содержащая следующие вложенные папки:
  - <дата_время> – подпапка, название которой – это дата и время проверки устройства в формате ГГГГ-ММ-ДД_ЧЧ-ММ-СС, содержащая следующие вложенные папки:
    - **Backup** – папка, содержащая резервные копии исходных файлов, которые система пыталась вылечить. В имени каждого файла содержится путь, по которому файл находился на проверяемом устройстве. Каждый файл упакован в защищенный паролем ZIP-архив. Пароль для доступа к этим файлам: `infected`.
    - **Dump** – папка, содержащая дампы памяти. Папка создается, если проверка была запущена в режиме записи дампа и во время проверки произошла критическая ошибка.
    - **Report** – папка, содержащая файлы отчетов о проверке.
    - **Temp** – папка, содержащая временные данные, создаваемые при проверке.
    - **Trace** – папка, содержащая файлы журнала трассировки. Папка создается, если сканер был запущен в режиме трассировки.

Просмотр отчетов

После завершения проверки создается папка **Reports**. Вы можете просмотреть файлы отчетов для каждого проверяемого устройства в следующем формате: kics_report_<имя_проверяемого_устройства>_<ГГГГ-ММ-ДД_ЧЧ-ММ-СС>.txt.

Отчет состоит из следующих разделов:

- Заголовок
- Список событий
- Статистика

kaspersky

AMSI-защита

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

В этом разделе

О задаче AMSI-защита

В ходе выполнения задачи AMSI-защита Kaspersky Industrial CyberSecurity for Nodes контролирует выполнение скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript®. Программа может также обрабатывать скрипты PowerShell™ и скрипты, работающие в программах Microsoft Office в операционных системах с установленным компонентом Antimalware Scan Interface (далее "AMSI"). Можно разрешить или запретить исполнение опасных или предположительно опасных скриптов. Если программа Kaspersky Industrial CyberSecurity for Nodes признала скрипт предположительно опасным, она выполняет выбранное вами действие: запрещает или разрешает выполнение скрипта. Если выбрано действие **Блокировать выполнение**, программа разрешает выполнение скрипта, только если этот скрипт считается безопасным.

Начиная с операционных систем Microsoft Windows 10 и Microsoft Windows Server 2016, Kaspersky Industrial CyberSecurity for Nodes поддерживает технологию AMSI. Технология AMSI позволяет интегрировать программы и службы с любым установленным на устройстве антивирусным программным обеспечением, чтобы это программное обеспечение могло перехватывать и проверять все исполняемые скрипты.

Более подробная информация о технологии AMSI приведена на сайте Microsoft Windows https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal.

Вы можете настраивать параметры задачи AMSI-защита (см. раздел "Настройка параметров задачи AMSI-защита с помощью Консоли программы" на стр. 819).

kaspersky

Параметры задачи AMSI-защита, установленные по умолчанию

По умолчанию локальная системная задача AMSI-защита имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 105. Параметры задачи AMSI-защита, установленные по умолчанию

Параметр	Значение по умолчанию	Описание
Действия над опасными скриптами	**Блокировать выполнение**	Вы можете указывать действия, выполняемые при обнаружении предположительно опасных скриптов: запрещать или разрешать их выполнение.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Можно включать и выключать эвристический анализатор. Можно настраивать уровень анализа.
Доверенная зона	Применяется	Единый список исключений, который можно применять в выбранных задачах.

Настройка параметров задачи AMSI-защита с помощью Плагина управления

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Постоянная защита сервера** окна **Свойства: <Имя политики>** нажмите на кнопку **Настройка** в подразделе **AMSI-защита**.

5. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
6. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

     - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
7. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
8. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Настройка параметров задачи AMSI-защита с помощью Консоли программы

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **AMSI-защита**.
3. В панели результатов узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В разделе **Действия над опасными скриптами** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
5. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

     - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
6. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
7. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Настройка параметров задачи AMSI-защита с помощью Веб-плагина

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **AMSI-защита**.

6. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
7. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень эвристического анализа.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

     - **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. 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 инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
8. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
9. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Статистика задачи AMSI-защита

В ходе выполнения задачи **AMSI-защита** вы можете просматривать информацию о количестве скриптов, обработанных программой Kaspersky Industrial CyberSecurity for Nodes с момента запуска задачи.

► *Чтобы просмотреть статистику задачи AMSI-защита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **AMSI-защита**.

Текущая статистика задачи отобразится в панели результатов узла, в разделах **Управление** и **Статистика**.

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

Таблица 106. Статистика задачи AMSI-защита

Поле	Описание
Заблокировано скриптов	Количество скриптов, заблокированных Kaspersky Industrial CyberSecurity for Nodes.
Обнаружено опасных скриптов	Количество обнаруженных опасных скриптов.
Обнаружено предположительно опасных скриптов	Количество обнаруженных предположительно опасных скриптов.
Обработано скриптов	Общее количество обработанных скриптов.

kaspersky

Мониторинг доступа к реестру

В этом разделе описано, как запустить и настроить задачу Мониторинг доступа к реестру.

В этом разделе

О задаче Мониторинг доступа к реестру

Задача Мониторинг доступа к реестру предназначена для отслеживания действий, выполненных с указанными ветвями и разделами реестра, в областях мониторинга, заданных в параметрах задачи. Задача отслеживает действия в операционной системе, установленной на устройстве, или в контейнерах Windows Server 2016 и более поздних версий, указанных в области мониторинга. Вы можете использовать задачу, чтобы обнаруживать изменения, указывающие на нарушение безопасности на защищаемом устройстве.

Чтобы запустить задачу Мониторинг доступа к реестру, необходимо настроить хотя бы одно правило мониторинга.

О правилах мониторинга доступа к реестру

Задача **Мониторинг доступа к реестру** запускается в соответствии с правилами мониторинга доступа к реестру. Вы можете использовать критерии срабатывания правила, чтобы настроить условия запуска задачи, и установить уровень важности обнаруженных событий, записываемых в журнал задачи.

Правило мониторинга доступа к реестру задается для каждой области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- **Действия**
- **Контролируемые значения**
- **Доверенные пользователи**

Действия

При запуске задачи Мониторинг доступа к реестру Kaspersky Industrial CyberSecurity for Nodes использует список действий для мониторинга реестра (см. таблицу ниже).

При обнаружении действия, указанного в качестве критерия срабатывания правила, программа регистрирует соответствующее событие.

Уровень важности фиксируемых событий не зависит от выбранных действий и количества событий.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes учитывает все действия. Вы можете настроить список действий вручную в параметрах правила задачи.

Таблица 107. Действия

Действие	Ограничения	Операционная система
Создать раздел	• Для Windows XP и Windows Server 2003, если вы добавляете в список **Создать раздел** действие **Действия**, а затем выбираете режим **Блокировать операции согласно правилам**, в указанных операционных системах создание раздела не блокируется из-за их системных ограничений. Раздел создается с соответствующим уведомлением, отправляемым в журнал событий. • Если вы хотите запретить создание определенного раздела с помощью редактора реестра, создайте правило для родительского раздела реестра и добавьте в список **Создание вложенных разделов** действие **Действия**, а затем выберите режим **Блокировать операции согласно правилам**.	Windows XP и выше
Удалить раздел	Если вы хотите удалить родительский раздел, убедитесь, что в списке **Удалить раздел** для настраиваемого раздела реестра сняты оба флажка: **Удаление вложенных разделов** и **Действия**, поскольку родительский раздел можно удалить, только включая подразделы.	Windows XP и выше
Переименование ключа	Недоступно	Windows XP и выше
Изменение параметров безопасности раздела	Недоступно	Windows Vista и выше
Удаление значений	Недоступно	Windows XP и выше

Действие	Ограничения	Операционная система
Задать значения	Если вы добавляете в список **Задать значения** действие **Действия**, в правиле для раздела указываете **Значение или маска значения** по умолчанию, а затем выбираете режим **Блокировать операции согласно правилам**, раздел не будет создан, поскольку новый раздел может быть создан только со значением по умолчанию.	Windows XP и выше
Создать вложенные разделы	Недоступно	Windows XP и выше
Удалить вложенные разделы	Недоступно	Windows XP и выше
Переименовать вложенные разделы	Недоступно	Windows XP и выше
Изменить параметры безопасности вложенных разделов	Недоступно	Windows Vista и выше

Значения реестра

В дополнение к мониторингу разделов реестра можно блокировать или контролировать изменения существующих значений реестра. Доступны следующие варианты:

- **Изменение значения** – создать новые или изменить существующие значения реестра.
- **Удалить значение** – удалить существующие значения реестра.

Переименование и изменение параметров безопасности не применимо к значениям реестра.

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности событий, формируя список доверенных пользователей в параметрах правила мониторинга системного реестра.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes обнаруживает действие, выполненное недоверенным пользователем, задача Мониторинг доступа к реестру фиксирует критическое событие в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение действий в указанной области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes обнаруживает действие, выполненное доверенным пользователем, задача Мониторинг доступа к реестру фиксирует информационное событие в журнале выполнения задачи.

kaspersky

Параметры по умолчанию для задачи Мониторинг доступа к реестру

В следующей таблице приведены параметры по умолчанию для задачи Мониторинг доступа к реестру. Вы можете изменять значения параметров с помощью:

- Плагина управления (см. раздел "Управление мониторингом доступа к реестру с помощью Плагина управления" на стр. 827)
- Консоли программы (см. раздел "Управление мониторингом доступа к реестру с помощью Консоли программы" на стр. 830)
- Веб-плагина (см. раздел "Управление мониторингом доступа к реестру с помощью Веб-плагина" на стр. 833)

Таблица 108. Параметры по умолчанию для задачи Мониторинг доступа к реестру

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Этот параметр используется, чтобы задать родительские и вложенные разделы реестра для мониторинга. Обязательный параметр. Если параметр не задан, задача не запустится. События мониторинга создаются для родительских и вложенных разделов реестра в указанной области мониторинга.
Действия	Выбраны все пункты списка действий	Этот параметр используется, чтобы настроить список требуемых действий посредством установки или снятия соответствующих флажков.
Контролируемые значения	Не задано	Этот параметр используется, чтобы добавлять, изменять и удалять значения реестра, которые требуется отслеживать для определенной области мониторинга.
Доверенные пользователи	Не задано	Вы можете указать пользователей и группы пользователей, которым разрешено выполнять определенные действия для указанных разделов реестра.
Режим работы задачи.	Только статистика	Вы можете выбрать режим работы задачи **Блокировать операции согласно правилам** или, для получения уведомлений, режим **Только статистика**.
Расписание запуска задачи	Не задано	Вы можете настроить параметры запуска задачи по расписанию.

kaspersky

Управление мониторингом доступа к реестру с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Плагина управления.

В этом разделе

Настройка параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить параметры задачи Мониторинг доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг доступа к реестру**.
5. На вкладке **Параметры мониторинга доступа к реестру** в блоке **Режим работы задачи** выберите требуемый вариант из списка:
   - **Блокировать операции согласно правилам**;
   - **Только статистика**.
6. Добавьте правила мониторинга доступа к реестру (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 828), в соответствии с которыми работает задача.

7. На вкладке **Управление задачей** настройте параметры расписания запуска (см. раздел "Работа с расписанием задач" на стр. 404) задачи.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. Выполните одно из следующих действий:
   - Если вы создаете правило мониторинга доступа к реестру в политике, в разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
   - Если вы создаете правило мониторинга доступа к реестру для локальной задачи, в окне **Свойства: Мониторинг доступа к реестру** перейдите в раздел **Настройка**.
5. В блоке **Правила мониторинга доступа к реестру** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга доступа к реестру**.

6. В поле **Выполнять мониторинг доступа к реестру для области** введите путь с помощью поддерживаемой маски.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы. Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.

7. На вкладке **Добавить** настройте список действий в соответствии с вашими требованиями.
8. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для значения реестра**.

   b. В одноименном поле введите маску значения реестра.
   c. В блоке **Значение или маска значения** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
9. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** в контекстном меню кнопки **Добавить** выберите способ добавления доверенных пользователей.

      Откроется окно **Выбор пользователя или группы пользователей**.

   b. Выберите пользователя или группу пользователей, которым разрешено выполнять выбранные действия.
   c. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 823), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

10. В окне **Правило мониторинга доступа к реестру** нажмите на кнопку **ОК**.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** / **Свойства: Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

kaspersky

Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать или импортировать правила мониторинга доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. Выполните одно из следующих действий:
   - Если вы хотите импортировать или экспортировать правила мониторинга доступа к реестру в политике, в разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
   - Если вы хотите импортировать или экспортировать правила мониторинга доступа к реестру для локальной задачи, в окне **Свойства: Мониторинг доступа к реестру** перейдите в раздел **Настройка**.
5. Экспортируйте или импортируйте правила мониторинга доступа к реестру:
   - Как экспортировать правила мониторинга доступа к реестру.
   - Как импортировать правила мониторинга доступа к реестру.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление мониторингом доступа к реестру с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Консоли программы.

kaspersky

В этом разделе

Настройка общих параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить общие параметры задачи Мониторинг доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Мониторинг доступа к реестру** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на вкладке **Общие**.
4. В блоке **Режим работы** выберите требуемый вариант из списка:
   - **Блокировать операции согласно правилам**;
   - **Только статистика**.
5. На вкладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Правила мониторинга реестра** перейдите по ссылке **Мониторинг доступа к реестру**.

   Откроется окно **Мониторинг доступа к реестру**.

4. В поле **Добавьте раздел системного реестра для мониторинга** введите путь к разделу реестра с помощью поддерживаемой маски.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы.
   Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.

5. Нажмите на кнопку **Добавить**.
6. На вкладке **Действия** для выбранной области мониторинга настройте список действий в соответствии с вашими требованиями.
7. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило обработки значений реестра**.

   b. В одноименном поле введите значение реестра или маску значения реестра.
   c. В блоке **Контролируемые операции** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **OK**, чтобы сохранить изменения.
8. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.
   b. В окне **Выбор пользователей или групп** выберите пользователей или группы пользователей, которым разрешено выполнять выбранные действия.
   c. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 823), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

9. В окне **Мониторинг доступа к реестру** нажмите на кнопку **Сохранить**.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать и импортировать правила мониторинга доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Правила мониторинга реестра** перейдите по ссылке **Мониторинг доступа к реестру**.

   Откроется окно **Мониторинг доступа к реестру**.
4. Как экспортировать правила мониторинга доступа к реестру.
5. Как импортировать правила мониторинга доступа к реестру.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление мониторингом доступа к реестру с помощью Веб-плагина

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Веб-плагина.

В этом разделе

Настройка параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить задачу Мониторинг доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.

5. В подразделе **Мониторинг доступа к реестру** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.

6. В блоке **Режим работы** выберите требуемый вариант из списка:

   - **Блокировать операции согласно правилам;**
   - **Только статистика.**

7. Добавьте правила мониторинга доступа к реестру (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 834), в соответствии с которыми работает задача.

8. На вкладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 404).

9. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг доступа к реестру** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.

6. В блоке **Правила мониторинга доступа к реестру** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга доступа к реестру**.

7. В поле **Выполнять мониторинг доступа к реестру для области** введите путь, используя поддерживаемую маску.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы.
   Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.

8. На вкладке **Действия** для выбранной области мониторинга настройте список действий в соответствии с вашими требованиями.
9. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило обработки значений реестра**.

   b. В одноименном поле введите маску значения реестра.
   c. В блоке **Контролируемые действия** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **OK**, чтобы сохранить изменения.
10. Если необходимо, задайте доверенных пользователей:
    a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.
    b. Введите **Имя пользователя** или нажмите на кнопку **Установить SID для группы Все**, чтобы задать пользователей, которым разрешено выполнять выбранные действия.
    c. Нажмите на кнопку **OK**, чтобы сохранить изменения.

    По умолчанию Kaspersky Industrial CyberSecurity for Nodes считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 823), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

11. В окне **Правило мониторинга доступа к реестру** нажмите на кнопку **OK**, чтобы сохранить изменения.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать или импортировать правила мониторинга доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В блоке **Мониторинг доступа к реестру** нажмите на кнопку **Параметры**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
6. Экспортируйте или импортируйте правила мониторинга доступа к реестру:
   - Как экспортировать правила мониторинга доступа к реестру.
   - Как импортировать правила мониторинга доступа к реестру.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

kaspersky

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 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 кибератак.

Kaspersky Industrial CyberSecurity for Nodes анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами, заданными пользователем, или с параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Стандартные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью стандартных правил, осуществляющих 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 стандартных правил. Вы можете включать и выключать любые правила. Нельзя удалять существующие правила и создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих 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 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 вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил анализа журналов содержит четыре правила. Вы можете включать и выключать эти правила, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при создании новой записи в журнале событий Windows, если в свойствах 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 журнал в журнале событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом журнале. Вы можете выбрать один из стандартных журналов (Программа, Безопасность или Система) или указать пользовательский журнал, введя его имя в поле выбора источника.

  > Программа не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows.

При срабатывании правила Kaspersky Industrial CyberSecurity for Nodes фиксирует событие с уровнем важности Критический в журнале выполнения задачи Анализ журналов.

По умолчанию в задаче Анализ журналов применяются пользовательские правила.

> Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробная информация приведена в статье Microsoft https://technet.microsoft.com/ru-ru/library/cc952128.aspx.

kaspersky

Параметры по умолчанию для задачи Анализ журналов

По умолчанию в задаче Анализ журналов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 109. Параметры по умолчанию для задачи Анализ журналов

Параметр	Значение по умолчанию	Описание
Применять пользовательские правила для анализа журналов	Не применяется.	Пользовательские правила можно включать, отключать, добавлять или изменять.
Использовать предзаданные правила для анализа журналов	Применяется.	Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве.
Обработка перебора пароля	10 неудачных попыток входа в течение 300 секунд.	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
Обработка сетевого входа	00:00:00	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Industrial CyberSecurity for Nodes расценивает данное действие как аномальную активность.
Исключения	Не применяется.	Можно указать пользователей и IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настроить расписание запуска задачи.

Управление правилами анализа журналов с помощью Плагина управления

В этом разделе описано добавление и настройка правил анализа журналов с помощью Плагина управления.

В этом разделе

kaspersky

Управление стандартными правилами задачи с помощью Плагина управления

► *Чтобы настроить параметры стандартных правил для задачи Анализ журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Диагностика системы** в подразделе **Настройка** нажмите на кнопку **Анализ журналов**.

   Откроется окно **Анализ журналов**.
5. Выберите закладку **Предзаданные правила**.
6. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Industrial CyberSecurity for Nodes применяет стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок снят.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
7. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - 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.
8. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Анализ журналов**.

9. В разделе **Обработка подбора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
10. В разделе **Обработка атипичной аутентификации** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Industrial CyberSecurity for Nodes как аномальная активность.
11. Выберите закладку **Исключения**.
12. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

    Указанный пользователь будет добавлен в список доверенных.
13. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.
14. Указанный IP-адрес будет добавлен в список доверенных.
15. На закладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Настройка расписания задач" на стр. 404).
16. В окне **Анализ журналов** нажмите на кнопку **OK**.

Параметры задачи Анализ журналов будут сохранены.

Добавление правил анализа журналов с помощью Плагина управления

► *Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
    - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
    - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Диагностика системы** в подразделе **Настройка** нажмите на кнопку **Анализ журналов**.

   Откроется окно **Анализ журналов**.

5. На закладке **Пользовательские правила** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Industrial CyberSecurity for Nodes применяет параметры правил по умолчанию.

   По умолчанию флажок снят. Активно только правило обнаружения всплывающих окон программ.

   Вы можете контролировать применение стандартных правил для анализа журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

   Откроется окно **Пользовательское правило**.

7. В разделе **Общие** укажите следующие данные нового правила:

   - **Имя правила**
   - **Источник**

     Выберите журнал, события которого будут использоваться для анализа. Доступны следующие журналы событий Windows: Программа, Безопасность, Система.

     Вы можете добавить новый пользовательский журнал, указав название журнала в поле **Источник**.

8. В разделе **Критерии срабатывания** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.

   a. Укажите идентификатор.

   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

9. Нажмите на кнопку **ОК**.

   Правило анализа журналов добавится в список правил.

kaspersky

Управление правилами анализа журналов с помощью Консоли программы

В этом разделе описано добавление и настройка правил анализа журналов с помощью Консоли программы.

В этом разделе

Управление стандартными правилами задачи с помощью Консоли программы

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Анализ журналов**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Industrial CyberSecurity for Nodes применяет стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок снят.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
6. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - 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, выберите закладку **Расширенные**.
8. В разделе **Обработка перебора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
9. В разделе **Обработка сетевого входа** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Industrial CyberSecurity for Nodes как аномальная активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

    Указанный пользователь будет добавлен 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 будет добавлен в список доверенных.
13. Выберите закладки **Расписание** и **Дополнительно**, чтобы настроить расписание запуска задачи.
14. В окне **Параметры задачи** нажмите на кнопку **OK**.

    Параметры задачи Анализ журналов будут сохранены.

Добавление правил анализа журналов с помощью Консоли программы

► *Чтобы добавить и настроить пользовательское правило анализа журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.
4. Откроется окно **Правила анализа журналов**.
5. Снимите или установите флажок **Применять пользовательские правила для анализа журналов. Настроенные параметры правил не применяются, если флажок снят**.

   Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.

Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Industrial CyberSecurity for Nodes применяет параметры правил по умолчанию.

По умолчанию флажок снят. Активно только правило обнаружения всплывающих окон программ.

Вы можете контролировать применение стандартных правил в задаче Анализ журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы создать пользовательское правило, выполните следующие действия:
   a. Введите имя нового правила.
   b. Нажмите на кнопку **Добавить**.

      Созданное правило добавится в общий список правил.
7. Чтобы настроить правило, выполните следующие действия:
   a. Выберите правило в списке.

      В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

      Комментарии для нового правила пусты.

   b. Выберите закладку **Параметры правила**.
8. В разделе **Общие** укажите следующие данные нового правила:
   - **Имя правила**
   - **Имя журнала**

     Выберите журнал, события которого будут использоваться для анализа. Доступны следующие журналы событий Windows: Программа, Безопасность, Система.

     Вы можете добавить новый пользовательский журнал, указав название журнала в поле **Источник**.

   - **Источник**

Укажите программу, события которой будут использоваться для анализа.

1. В разделе **Идентификаторы событий** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
   a. Укажите идентификатор события.
   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
2. Нажмите на кнопку **Сохранить**.

   Настроенные параметры правил анализа журналов будут применены.

kaspersky

Управление правилами анализа журналов с помощью Веб-плагина

► *Чтобы добавить и настроить правила анализа журналов с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Параметры** в подразделе **Анализ журналов**.
6. Настройте параметры, приведены в следующей таблице.

Таблица 110. Параметры задачи Анализ журналов

Параметр	Описание
Применять пользовательские правила для анализа журналов	Пользовательские правила можно включать, отключать, добавлять или изменять. Этот параметр доступен в таблице со списком пользовательских правил.
Использовать предзаданные правила для анализа журналов	Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве. Этот параметр доступен в таблице со списком пользовательских правил.
Считать попытки неудачного ввода пароля потенциальной атакой, если они выполняются с указанной частотой	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
Обнаруживать сетевую сессию, если вход выполнен в указанный интервал	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Industrial CyberSecurity for Nodes расценивает данное действие как аномальную активность.
Исключения	Можно указать пользователей, которые не будут являться критериями срабатывания эвристического анализатора.
Исключения IP-адресов	Можно указать IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.
Управление задачей	Вы можете настроить расписание запуска задачи.

kaspersky

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 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.

Агент защиты процессов – это динамически загружаемый модуль Kaspersky Industrial CyberSecurity for Nodes, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, вам нужно завершить данный процесс. Может потребоваться перезагрузка защищаемого компьютера (например, при защите системного процесса).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Industrial CyberSecurity for Nodes выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;
- удалить процесс из списка защищаемых и перезапустить его.

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.

Если на устройстве установлена операционная система Windows 10 или более поздних версий, программа не будет продолжать защищать процессы и память процессов после остановки службы Kaspersky Security Exploit Prevention.

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 следующих 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 не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

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

  В этом режиме Kaspersky Industrial CyberSecurity for Nodes регистрирует все попытки эксплуатации уязвимостей посредством создания событий. Выбран по умолчанию.

Управление защитой от эксплойтов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров компонента для защищаемых компьютеров в сети.

kaspersky

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к параметрам политики для защиты от эксплойтов

► *Чтобы перейти к параметрам защиты от эксплойтов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Переход к окну параметров защиты от эксплойтов

► *Чтобы перейти к окну свойства для защиты от эксплойтов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.

3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Industrial CyberSecurity for Nodes 3.2**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Industrial CyberSecurity for Nodes 3.2**.
7. Перейдите в раздел **Постоянная защита компьютера**.
8. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 849).
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

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

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

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**.

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

   - **Только сообщать**.

     Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 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 обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.

3. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

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

     По умолчанию флажок снят.
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security Service**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Industrial CyberSecurity for Nodes не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

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

     По умолчанию флажок снят.
4. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

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

Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Можно исключить процессы из области защиты, сняв соответствующие флажки в списке процессов.

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

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 849).
2. На закладке **Защищаемые процессы** нажмите на кнопку **Обзор**.

   Откроется окно проводника Windows.
3. Выберите процесс, который вы хотите добавить в список.
4. Нажмите на кнопку **Открыть**.

   Имя процесса будет отображено в строке.
5. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.
6. Выберите добавленный процесс.

7. Нажмите на кнопку **Указать техники защиты от эксплойта**.

   Откроется окно **Техники защиты от эксплойта**.

8. Выберите один из следующих вариантов применения техник снижения рисков:

   - **Применять все доступные техники защиты от эксплойта**.

     Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

   - **Применять указанные техники защиты от эксплойта**

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

9. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

10. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

    - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
    - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
      - **Интернет**
      - **Интранет**
      - **Доверенные сайты**
      - **Сайты с ограниченным доступом**
      - **Компьютер**

      Данные параметры применимы только для Internet Explorer®.

11. Нажмите на кнопку **ОК**.

Процесс будет добавлен в область защиты задачи.

kaspersky

Управление защитой от эксплойтов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров компонента на защищаемом устройстве.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

В этом разделе

Переход к основным параметрам защиты от эксплойтов

► *Чтобы перейти к окну **Параметры защиты от эксплуатации уязвимостей**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита файлов**.
2. Выберите узел **Защита от эксплойтов**.
3. В разделе **Параметры защиты процессов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.

Настройте общие параметры защиты от эксплойтов в соответствии с вашими требованиями.

Переход к параметрам защиты процессов при защите от эксплойтов

► *Чтобы перейти к окну **Параметры защиты процессов** , выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита файлов**.
2. Выберите узел **Защита от эксплойтов**.
3. В разделе **Параметры защиты процессов** перейдите по ссылке **Параметры защиты процессов** .

   Откроется окно **Параметры защиты процессов** .

Настройте параметры защиты процессов для защиты от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

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

1. Откройте окно **Параметры защиты от эксплуатации уязвимостей**.
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

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

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

     По умолчанию флажок снят.

     - **Завершать скомпрометированные процессы**.

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

     - **Только сообщать**.

       Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 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 обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.
3. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

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

По умолчанию флажок снят.

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

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Industrial CyberSecurity for Nodes не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

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

  По умолчанию флажок снят.

4. В окне **Параметры защиты от эксплуатации уязвимостей** нажмите на кнопку **OK**.

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

Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. 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. Откройте окно **Параметры защиты процессов** .
2. Чтобы защитить процесс от компрометации и снизить возможное влияние эксплуатации уязвимостей, выполните 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.
3. Выберите добавленный процесс в списке.

4. Текущая конфигурация отображается на **Параметры защиты процессов** закладке:
   - **Имя процесса**.
   - **Выполняется сейчас**.
   - **Применяемые техники защиты**.
   - **Снижение области действия процесса (параметры техники Attack Surface Reduction)**.
5. Чтобы изменить применяемые к процессу техники защиты от эксплойтов, выберите закладку **Техники защиты от эксплойта** .
6. Выберите один из следующих вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**.

     Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
   - **Применять указанные техники защиты от эксплойта**.

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
7. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
   - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей** .
   - В разделе **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
     - **Интернет**
     - **Интранет**
     - **Доверенные сайты**
     - **Сайты с ограниченным доступом**
     - **Компьютер**

     > Данные параметры применимы только для Internet Explorer®.
8. Нажмите на кнопку **Сохранение**.

Процесс будет добавлен в область защиты задачи.

Управление защитой от эксплойтов с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров компонента на защищаемом устройстве.

kaspersky

В этом разделе

Настройка защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от эксплойтов**.
6. Откройте закладку **Параметры защиты от эксплойтов**.
7. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

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

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

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**.

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

   - **Только статистика**.

     Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 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 обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.

8. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

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

     По умолчанию флажок снят.
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security Service**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Industrial CyberSecurity for Nodes не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

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

     По умолчанию флажок снят.
9. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

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

Добавление процесса в область защиты

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от эксплойтов**.
6. Перейдите на закладку **Защищаемые процессы**.
7. Нажмите на кнопку **Добавить**.
8. Откроется окно **Техники защиты от эксплойтов**.
9. Укажите название процесса.

10. Выберите один из следующих вариантов применения техник снижения рисков:
    - **Применять все доступные техники защиты от эксплойтов**.

      Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
    - **Применять указанные техники защиты от эксплойтов**

      Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

      a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
11. Установите или снимите флажок **Применять технику Attack Surface Reduction**.
12. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
    - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
    - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
      - **Интернет**
      - **Интранет**
      - **Доверенные сайты**
      - **Сайты с ограниченным доступом**
      - **Компьютер**

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

Процесс будет добавлен в область защиты задачи.

kaspersky

Техники защиты от эксплойтов

Таблица 111. Техники защиты от эксплойтов

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 Exception 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 потенциально опасных 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.

kaspersky

Защита промышленной сети

В этом разделе описаны задачи получения данных и проверки целостности проектов программируемых логических контроллеров (далее также "проектов ПЛК").

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 сетевой доступ к ПЛК со стороны защищаемого компьютера с установленной программой Kaspersky Industrial CyberSecurity for Nodes.

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

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

► *Чтобы просмотреть информацию о проектах ПЛК в задаче Проверка целостности программы,*

откройте окно **Взаимодействие с Сервером администрирования** (см. раздел "**Настройка политики**" на стр. 385) и выберите **Данные о версиях проектов ПЛК**.

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.
Задача Проверка целостности проектов ПЛК в KICS for Nodes 2.5 доступна в Kaspersky Security Center версии 10.5.1781.

kaspersky

Отчеты

Отчетность входит в число базовых функций Сервера администрирования Kaspersky Security Center. Воспользоваться этой функцией можно только через Консоль администрирования Kaspersky Security Center.

После успешного завершения задачи Проверка целостности проектов ПЛК вы можете создать и просмотреть отчет со следующей информацией:

- имя компьютера, на котором завершена задача Проверка целостности проектов ПЛК;
- ПЛК, целостность которых контролируется;
- дата последней проверки;
- результаты проверки целостности.

► *Чтобы создать отчет на Сервере администрирования Kaspersky Security Center, 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 задач Контроль проектов ПЛК с помощью Консоли программы

В этом разделе

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 программы разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. Перейдите по ссылке **Свойства** в панели результатов узла **Получение данных о проектах ПЛК**.

   Откроется окно **Параметры задачи**.
4. Нажмите на кнопку **Добавить**, чтобы открыть окно **Конфигурация ПЛК**.
5. Настройте следующие параметры проекта ПЛК:
   - В разделе **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.
     - В поле **Ожидать соединения** укажите время ожидания соединения для выбранного ПЛК.
   - В разделе **Параметры соединения**:
     - Укажите **IP-адрес**, **Порт**, **Номер стойки** и **Номер слота**.
     - 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.
     - Установите или снимите флажок **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.
6. В окне **ОК** нажмите на кнопку **Конфигурация ПЛК**.

Резервные контроллеры не поддерживаются.

7. Повторите ввод параметров для каждого из остальных ПЛК.

   Указанные параметры будут отображаться в таблице на закладке **Общие**.

8. 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.

9. В окне **Параметры задачи** нажмите на 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 программы разверните узел **Защита промышленной сети** .
2. Выберите вложенный узел **Проверка целостности проектов ПЛК**.
3. Перейдите по ссылке **Свойства** в панели результатов узла **Проверка целостности проектов ПЛК**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне настройте следующие параметры:
   - Расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425) на закладках **Расписание** и **Дополнительно**.
   - На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
5. В 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 проекта ПЛК**.

   Все данные в этом окне получены в результате выполнения задачи Kaspersky Security Center Получение данных о проектах ПЛК.

7. В раскрывающемся списке **Тип контроллера** в окне **Данные проекта 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 **Данные проекта ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.
10. Выберите добавленную конфигурацию ПЛК из списка в окне **Настройка 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 **Параметры проверки целостности проекта ПЛК**.
    - В раскрывающемся списке содержится информация о хеше проекта ПЛК и дате, когда он был получен. Выполните следующие действия:

      a. В списке выберите вариант **Эталонная версия проекта ПЛК**. 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**, чтобы указать промежуток времени, через который программа запрашивает информацию о параметрах проектов ПЛК.
13. Нажмите на кнопку **Сохранить** 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 программы разверните узел **Защита промышленной сети** .
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. В разделе **Управление** в панели результатов узла **Получение данных о проектах ПЛК** перейдите по ссылке **Запустить**.
4. Выберите вложенный узел **Проверка целостности проектов ПЛК**.

5. В разделе **Управление** в панели результатов узла **Проверка целостности проектов ПЛК** выполните одно из следующих действий:
   - Чтобы включить Проверку целостности проектов ПЛК, перейдите по ссылке **Запустить**.

     Задача Проверка целостности проектов ПЛК будет запущена.
   - Чтобы выключить Проверку целостности проектов ПЛК, перейдите по ссылке **Остановить**.

     Задача Проверка целостности проектов ПЛК будет остановлена.

Настройка задачи Контроль проектов ПЛК с помощью Плагина управления

В этом разделе

О реестре конфигураций ПЛК

Реестр конфигураций ПЛК (далее также "Реестр") это единый список всех конфигураций ПЛК, которые используются программами Решения Kaspersky Industrial CyberSecurity. Конфигурация ПЛК - это совокупность частных параметров ПЛК, которые вы можете указать в настройках (IP-адрес, номер слота, модель и т.д.). Вы можете добавлять, изменять и удалять конфигурации ПЛК через реестр.

Реестр конфигураций ПЛК может быть наполнен вручную или с помощью импорта конфигурационного файла, содержащего данные о конфигурациях ПЛК.

Список конфигураций ПЛК в реестре используется для формирования области защиты задачи Проверка целостности проектов ПЛК, настраиваемой через Консоль администрирования Kaspersky Security Center. Во время наполнения списка конфигураций задачи Получение данных о проектах ПЛК вы можете добавлять и удалять конфигурации ПЛК в реестре. При удалении конфигурации ПЛК из списка задач, эта конфигурация не удаляется из реестра.

Каждая конфигурация ПЛК, добавленная в реестр, имеет уникальный идентификационный номер. При внесении изменений в конфигурацию ПЛК, идентификационный номер изменяется. Конфигурации ПЛК, добавленные через задачу Получение данных о проектах ПЛК в локальной Консоли Kaspersky Industrial CyberSecurity for Nodes не имеют идентификационных номеров. Такие конфигурации ПЛК можно добавить в реестр вручную при создании области защиты в задаче Получение данных о проектах ПЛК в Kaspersky Security Center.

Список конфигураций ПЛК в задаче Получение данных о проектах ПЛК в Kaspersky Security Center формируется из двух источников:

- Конфигурации ПЛК без идентификационных номеров, добавленные в список локальной задачи в Консоли программы (список синхронизируется автоматически).
- Конфигурации ПЛК без идентификационных номеров, добавленные администратором из реестра конфигураций ПЛК.

Если конфигурация ПЛК, добавленная в список задачи Получение данных о проектах ПЛК, удалена из Реестра, Kaspersky Industrial CyberSecurity for Nodes уведомляет вас о том, что результаты проверки целостности будут искажены. Перезапустите задачу Получение данных о проектах ПЛК, убедившись, что все конфигурации ПЛК в списке задачи в Kaspersky Security Center существуют в реестре.

Настройка реестра ПЛК

► *Чтобы настроить реестр ПЛК, выполните следующие действия:*

1. В окне Kaspersky Security Center выберите **Сервер администрирования <имя сервера>**.
2. Откройте дочерний узел **Дополнительно**.
3. В папке **Хранилища** дерева консоли Kaspersky Security Center выберите вложенную папку **Оборудование**.
4. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Реестр конфигураций ПЛК**.

   Откроется окно **Управление списком конфигураций ПЛК**.
5. Чтобы добавить новую конфигурацию вручную, нажмите на кнопку **Добавить**.

   Откроется окно **Параметры ПЛК**.
6. В разделе **Общие параметры**:
   a. В поле **Название** укажите название ПЛК.
   b. В раскрывающемся списке **Тип ПЛК** выберите тип ПЛК.

      Раскрывающийся список доступных типов ПЛК, данные о проектах которых можно получить. Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.
   c. В поле **Описание** укажите 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.
   d. В поле **Ожидать соединение** укажите время ожидания в секундах.
7. В разделе **Параметры соединения** введите следующую информацию:
   a. Укажите **IP-адрес**, **Порт**, **Номер стойки** и **Номер слота**.
   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. Снимите или установите флажок **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.

8. Нажмите на кнопку **ОК**.
9. Вы также можете импортировать и экспортировать XML-файл с конфигурацией ПЛК, нажав на соответствующую кнопку в окне **Реестр конфигураций проектов ПЛК**.
10. Чтобы изменить параметры конфигурации, нажмите на кнопку **Изменить**.

Изменение конфигурации ПЛК в реестре ПЛК влияет на результаты задачи Проверка целостности проектов ПЛК. Вам потребуется запустить задачу Получение данных о проектах ПЛК, чтобы получить обновленные данные, и затем снова запустить задачу Проверка целостности проектов ПЛК, чтобы получить актуальные результаты.

11. Нажмите на кнопку **Удалить**, если конфигурация проектов ПЛК больше не используется.

После удаления из реестра ПЛК проект ПЛК становится недоступным для получения данных и проверки целостности.

12. Используйте поле **Фильтр**, чтобы найти конфигурации ПЛК с требуемыми значениями.

Нельзя использовать фильтр по ID реестра ПЛК.

13. Вы также можете установить флажок **Показывать только конфигурации ПЛК, доступные для управления с помощью программы Kaspersky Industrial CyberSecurity for Nodes**, если вам не требуется общий список конфигураций ПЛК для всех программ решения *Kaspersky Industrial CyberSecurity*.
14. Нажмите на кнопку **Закрыть**.

Реестр ПЛК будет сохранен.

kaspersky

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. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Управляемые устройства** выберите закладку **Устройства** и откройте свойства выбранного компьютера.
3. В разделе **Задачи** выберите **Получение данных о проектах ПЛК** > **Свойства**.

   Откроется окно **Свойства: Получение данных о проектах ПЛК**.
4. Выберите раздел **Конфигурации проектов ПЛК**.

   В списке конфигураций ПЛК отображаются конфигурации, добавленные через Консоль Kaspersky Industrial CyberSecurity for Nodes.

   > Добавленные через Консоль Kaspersky Industrial CyberSecurity for Nodes конфигурации появляются в списке задач Kaspersky Security Center только после завершения задачи "Получение данных о проектах ПЛК" на локальном компьютере с Консолью Kaspersky Industrial CyberSecurity for Nodes.
5. Нажмите на кнопку **Добавить из Реестра ПЛК**, чтобы добавить необходимые конфигурации проектов ПЛК из реестра ПЛК (см. раздел "Настройка реестра ПЛК" на стр. 867).

   Откроется окно **Управление списком конфигураций ПЛК**.
6. Выберите конфигурацию ПЛК и нажмите на кнопку **Добавить в список задачи**.
7. Добавьте все требуемые конфигурации ПЛК и закройте окно **Управление списком конфигураций ПЛК**.
8. Чтобы добавить конфигурацию ПЛК, полученную из задачи на локальном компьютере, выполните следующие действия:

   a. В списке конфигураций ПЛК выберите ту, которую хотите добавить в реестр ПЛК.

   b. Нажмите на кнопку **Привязать к Реестру ПЛК**.

   > У каждой конфигурации ПЛК из реестра есть уникальный идентификационный номер, указанный в последнем столбце. После добавления конфигурации ПЛК из задачи на локальном компьютере в реестр ПЛК этой конфигурации присваивается идентификационный номер.
9. Чтобы удалить конфигурацию ПЛК из списка задач, выполните следующие действия:

   a. Выберите конфигурацию ПЛК.

   b. Нажмите на кнопку **Удалить**.

   > ПЛК не удаляется из реестра, и его можно добавить снова в любой момент.

10. В окне **Свойства: Получение данных о проектах ПЛК** нажмите на 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. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Управляемые устройства** выберите закладку **Устройства** и откройте свойства выбранного компьютера.
3. В разделе **Задачи** выберите **Проверка целостности проектов ПЛК** > **Свойства**.

   Откроется окно **Свойства: Проверка целостности проектов ПЛК**.
4. В разделе **Настройка** окна свойств задачи Проверка целостности проектов ПЛК нажмите на кнопку **Добавить**.

   Откроется окно **Данные для проверки целостности проекта ПЛК**. Все данные в этом окне получены в результате выполнения локальной задачи Получение данных о проектах ПЛК (см. раздел "Настройка получения данных о проектах ПЛК" на стр. 862) в Kaspersky Security Center.
5. Для каждого типа ПЛК в таблице при необходимости настройте параметры проверки целостности проектов ПЛК. Для этого выполните следующие действия:
   a. Выберите в таблице запись с данными ПЛК и нажмите на кнопку **Изменить**.

      Откроется окно **Параметры проверки целостности проекта ПЛК**.
   b. Укажите значение параметра **Интервал опроса выбранной конфигурации ПЛК**, чтобы указать интервал времени, через который программа запрашивает информацию о параметрах проектов ПЛК.
   c. Выберите эталонный проект ПЛК из списка. По результатам сравнения с параметрами эталонного проекта программа делает вывод о целостности проекта ПЛК.
   d. В окне **Параметры проверки целостности проекта ПЛК** нажмите на кнопку **ОК**.
6. В графе **Тип ПЛК** окна **Данные для проверки целостности проектов ПЛК** установите флажки напротив тех типов ПЛК, целостность проектов которых вы хотите проверять.
7. В окне **Данные для проверки целостности проектов ПЛК** нажмите на кнопку **ОК**.
8. В окне **Свойства: Проверка целостности проектов ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Включение и выключение проверки целостности проектов ПЛК

Задача Проверка целостности проектов ПЛК выполняется только после того, как Kaspersky Industrial CyberSecurity for Nodes получит данные о проекте ПЛК с помощью задачи Получение данных о проектах ПЛК.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Управляемые устройства** выберите закладку **Устройства** и откройте свойства выбранного компьютера.
3. В разделе **Задачи** выберите **Проверка целостности проектов ПЛК** > **Свойства**.

   Откроется окно **Свойства: Проверка целостности проектов ПЛК**.
4. В разделе **Общие** окна свойств задачи Проверка целостности проектов ПЛК выполните следующие действия:
   - Нажмите на кнопку **Запустить**, чтобы включить Проверку целостности проектов ПЛК.
   - Нажмите на кнопку **Остановить**, чтобы выключить Проверку целостности проекта ПЛК.
5. В окне **Свойства: Проверка целостности проектов ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

kaspersky

Импорт и экспорт данных для задачи Получение данных о проектах ПЛК

► *Чтобы импортировать или экспортировать данные для задачи Получение данных о проектах ПЛК, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Управляемые устройства** выберите закладку **Устройства** и откройте свойства выбранного компьютера.
3. В разделе **Задачи** выберите **Получение данных о проектах ПЛК** > **Свойства**.

   Откроется окно **Свойства: Получение данных о проектах ПЛК**.
4. В разделе **Настройка** выполните одно из следующих действий:
   - Нажмите на кнопку **Импорт**, чтобы импортировать в таблицу Получение данных о проектах ПЛК данные о ПЛК, информацию о проектах которых вы хотите получить.

     Откроется стандартное окно Microsoft Windows **Открыть файл**. Выполните следующие действия:

     a. В окне Microsoft Windows **Открыть файл** выберите XML-файл с параметрами ПЛК.

     b. Нажмите на кнопку **Открыть**.

        Откроется окно **Импорт параметров**.

     c. Выберите метод импортирования параметров ПЛК:

        - Заменить текущие параметры.
        - Добавить в текущие параметры.

     Записи отображаются в списке **Указанные данные проекта ПЛК**.
   - Нажмите на кнопку **Экспорт**, чтобы экспортировать содержимое таблицы Получение данных о проекте ПЛК в XML-файл.
5. В окне **Свойства: Получение данных о проектах ПЛК** нажмите на кнопку **ОК**, чтобы сохранить изменения.

kaspersky

Использование Kaspersky Security Gateway

В этом разделе приведены пошаговые инструкции по использованию Kaspersky Security Gateway.

В этом разделе

kaspersky

О Kaspersky Security Gateway

Kaspersky Security Gateway предназначен для передачи в систему SCADA диагностической информации из Kaspersky Security Center, полученной от Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks, включая информацию об изменениях прошивки ПЛК и потенциально опасных зарегистрированных командах для ПЛК. Информация о состоянии защиты промышленных сетей и сетевых узлов отображается на экранах системы SCADA, что позволяет оператору системы SCADA своевременно реагировать на проблемы защиты промышленных сетей.

Kaspersky Security Gateway использует следующие протоколы связи для взаимодействия с системой SCADA:

- **IEC 60870-5-104**. Единый открытый протокол для систем автоматизации.
- **OPC DA**. Спецификация взаимодействия устройств в промышленных сетях.

Параметры передачи данных (см. раздел "Настройка параметров передачи данных с использованием протоколов связи" на стр. 879) можно настроить как с помощью графического интерфейса Kaspersky Security Gateway, так и с помощью стандартных средств Microsoft Windows. Вы можете назначать теги и значения тегов для событий, указывающих на прерывание технологического процесса.

Kaspersky Security Gateway передает в систему SCADA следующую информацию:

- Состояние доступности Сервера администрирования Kaspersky Security Center:
  - 1. Это состояние показывает, что Kaspersky Security Gateway успешно подключен к Серверу администрирования Kaspersky Security Center.
  - 0. Это состояние показывает, что Kaspersky Security Gateway не может подключиться к Серверу администрирования Kaspersky Security Center.
- Состояние доступности всех защищаемых узлов сети:
  - 0. Это состояние показывает, что все сетевые узлы, управляемые Сервером администрирования Kaspersky Security Center и выбранные для мониторинга в параметрах Kaspersky Security Gateway, доступны на момент определения состояния.
  - 1. Это состояние показывает, что хотя бы один сетевой узел, управляемый Сервером администрирования Kaspersky Security Center и выбранный для мониторинга в параметрах Kaspersky Security Gateway, недоступен на момент определения состояния.
- Состояние защиты каждого узла сети Kaspersky Security Center:
  - 0. Это состояние показывает, что на узле сети, управляемом Сервером администрирования Kaspersky Security Center и выбранном для мониторинга в параметрах Kaspersky Security Gateway, не произошло никаких критических инцидентов или инцидентов, требующих обработки.
  - 1. Это состояние показывает, что на сетевом узле, управляемом Сервером администрирования Kaspersky Security Center и выбранном для мониторинга в параметрах Kaspersky Security Gateway, произошел хотя бы один критический инцидент.
  - 2. Это состояние показывает, что на сетевом узле, управляемом Сервером администрирования Kaspersky Security Center и выбранном для мониторинга в параметрах Kaspersky Security Gateway, произошел хотя бы один инцидент, требующий обработки.

  Состояние защиты каждого узла определяется Kaspersky Security Center для управляемых компьютеров или групп администрирования.

Kaspersky Security Gateway отправляет информацию о состоянии только сетевых узлов, выбранных в параметрах Kaspersky Security Gateway для отображения в системе SCADA.

- Состояние защиты сети (см. Состояние защиты каждого узла в описании сети Kaspersky Security Center):
  - 0. Это состояние показывает, что все узлы сети находятся в состоянии 0 в Kaspersky Security Center.
  - 1. Это состояние показывает, что хотя бы один сетевой узел находится в состоянии 1 в Kaspersky Security Center.
  - 2. Это состояние показывает, что хотя бы один компьютер в сети находится в состоянии 2 в Kaspersky Security Center.

  При определении состояния защиты сети Kaspersky Security Gateway использует информацию о состоянии сетевых узлов, выбранных в параметрах Kaspersky Security Gateway для отображения в системе SCADA.

Ограничения для Kaspersky Security Gateway

Ниже приведен список ограничений для Kaspersky Security Gateway:

- Для подключения Kaspersky Security Gateway, установленного на устройстве с операционной системой Windows 7, к Kaspersky Security Center 14 и более поздних версий требуется, чтобы в операционной системе были включены TLS 1.1 и 1.2. Включение TLS 1.1 и 1.2 в Windows 7 описано в документации Microsoft.
- Аварийное завершение работы gateway_service.exe может быть вызвано ошибками в сторонней библиотеке grpc. Аварийное завершение сервиса происходит при подключении к Kaspersky Industrial CyberSecurity for Networks одновременно с выполнением динамического анализа кода с помощью утилиты проверки программ (Application Verifier).
- Kaspersky Security Gateway совместим с Kaspersky Industrial CyberSecurity for Networks версий 2.9 и ниже.

kaspersky

Запуск и остановка Kaspersky Security Gateway стандартными средствами Microsoft Windows

Kaspersky Security Gateway запускается автоматически при запуске операционной системы. Вы можете запустить или остановить Kaspersky Security Gateway вручную с помощью стандартных средств Microsoft Windows.

► *Чтобы запустить или остановить Kaspersky Security Gateway, выполните следующие действия:*

1. Откройте оснастку Службы в Консоли управления Microsoft (services.msc).
2. В списке служб выберите требуемую службу Kaspersky Security Gateway:
   - Kaspersky Security Gateway
   - Kaspersky Security Gateway IEC 60870-5-104
   - Kaspersky Security Gateway OPC
3. По правой клавише мыши откройте контекстное меню выбранной службы и выполните одно из следующих действий:
   - Выберите **Старт**, чтобы запустить службу.
   - Выберите **Стоп**, чтобы остановить службу.

Интерфейс Консоли Kaspersky Security Gateway

Консоль Kaspersky Security Gateway отображается в дереве Microsoft Management Console в виде узла с именем **Kaspersky Security Gateway**.

В дереве Консоли отображается узел **Kaspersky Security Gateway** и дочерние узлы для настройки использования доступных протоколов связи:

- **IEC 60870-5-104**
- **OPC**

В области результатов узла **Kaspersky Security Gateway** отображаются следующие данные:

- Общая информация о Kaspersky Security Gateway (на стр. 874).
- Подробная информация о текущих параметрах подключения к системе SCADA (см. раздел "Настройка подключения к системе SCADA" на стр. 877) и ссылка на окно настройки.
- Подробная информация о текущих дополнительных параметрах Kaspersky Security Gateway (см. раздел "Настройка дополнительных параметров Kaspersky Security Gateway" на стр. 884) и ссылка на окно настройки.

Настройка подключения к системе SCADA

► *Чтобы настроить подключение к системе SCADA, выполните следующие действия:*

1. В меню **Пуск** Microsoft Windows выберите **Все программы** > **Kaspersky Security Gateway** > **Консоль Kaspersky Security Gateway**.

   Откроется окно **Kaspersky Security Gateway**.

   > Вы можете также открыть Консоль, выбрав пункт **Kaspersky Security Gateway** в меню значка Kaspersky Security Gateway в области уведомлений.

2. Выберите узел **Kaspersky Security Gateway**.
3. В разделе **Параметры соединения** на панели результатов нажмите на ссылку **Настройка соединения**.

   Откроется окно **Настройки соединения**.
4. В разделе **Kaspersky Security Center настройки соединения** укажите следующие параметры подключения к Серверу администрирования Kaspersky Security Center:

   - **Сервер** и **Порт**. Имя Сервера администрирования Kaspersky Security Center и номер порта для подключения к нему. Значение указывается в формате `server:port`. Диапазон возможных значений номера порта: 1–65535.
     - Для поставщика данных klakaut по умолчанию используется номер порта 13291.
     - Для поставщика данных Open API по умолчанию используется номер порта 13299.
   - **Имя пользователя**. Имя учетной записи администратора Сервера администрирования Kaspersky Security Center.
   - **Пароль**. Пароль учетной записи администратора Сервера администрирования Kaspersky Security Center.

   > Если в качестве поставщика данных выбран сервис klakaut, необходимо установить Консоль администрирования Kaspersky Security Center на тот же компьютер, на котором установлен Kaspersky Security Gateway. Сервис Klakaut – это сервис автоматизации Kaspersky Security Center, позволяющий управлять и контролировать сервер Kaspersky Security Center через внешний API с помощью объектов COM (Component Object Model). Если в качестве поставщика данных выбран интерфейс Open API, необходимо установить на компьютер сертификат Kaspersky Security Center (klserver.cer). Подробная информация о настройке Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

5. Нажмите на кнопку **Проверить**.

   Статус *Подключено* показывает, что соединение установлено.

6. Чтобы добавить компьютер с установленной программой Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Настройка соединения с Kaspersky Industrial CyberSecurity for Networks**.
   b. Введите адрес сервера и номер порта.
   c. Нажмите на кнопку **Проверить**.

      Статус *Подключено* показывает, что соединение установлено.
   d. Нажмите на кнопку **OK**.

   Компьютер будет добавлен в список подключенных компьютеров в окне **Настройки соединения**.
7. Нажмите на кнопку **OK**, чтобы закрыть окно **Kaspersky Security Gateway**.

Параметры подключения можно также настроить с помощью конфигурационного файла ConnectionSettings.xm, расположенного в папке C:\ProgramData\Kaspersky Lab\Security Gateway\Settings. Обратите внимание, что в файле конфигурации нельзя задать пароль. Для задания пароля используйте Консоль Kaspersky Security Gateway.

Настройка протокола DCOM

Если компьютеры, участвующие в подключении OPC, не присоединены к домену Active Directory, для каждого из этих компьютеров создайте учетные записи пользователей с одинаковыми именем и паролем.

Чтобы установить соединение OPC, необходимо настроить права доступа для протокола распределенной объектной модели компонентов (DCOM).

► *Чтобы настроить права доступа для протокола DCOM, выполните следующие действия:*

1. Нажмите комбинацию клавиш **WIN+R**.

   Откроется стандартное окно Microsoft Windows **Выполнить**.
2. В поле **Открыть** введите *dcomcnfg* и нажмите на кнопку **OK**.

   Откроется окно **Службы компонентов**.
3. В левой части окна в дереве папок выберите **Службы компонентов** → **Компьютеры** → **Мой компьютер**.
4. По правой клавише мыши откройте контекстное меню папки **Мой компьютер** и выберите **Свойства**.

   Откроется окно **Свойства: Мой компьютер**.
5. В окне **Свойства: Мой компьютер** выберите закладку **Безопасность COM**.
6. В разделе **Права доступа** нажмите на кнопку **Изменить ограничения**.

   В окне **Права доступа** откроется закладка **Ограничения в целях безопасности**.

7. В разделе **Группы или пользователи** выберите группу **АНОНИМНЫЙ ВХОД**.
8. В таблице **Разрешения для группы АНОНИМНЫЙ ВХОД** в столбце **Разрешить** установите флажок **Удаленный доступ**.
9. Чтобы сохранить изменения, нажмите на кнопку **ОК**.
10. Нажмите на кнопку **ОК** в окне **Свойства: Мой компьютер**.
11. Перезагрузите компьютер.

Настройка параметров передачи данных с использованием протоколов связи

В этом разделе приведены инструкции по настройке передачи данных с использованием доступных протоколов связи.

В этом разделе

Настройка передачи данных по протоколу IEC 60870-5-104 через Консоль

► *Чтобы настроить передачу данных по протоколу IEC 60870-5-104 через Консоль Kaspersky Security Gateway, выполните следующие действия:*

1. В меню **Пуск** Microsoft Windows выберите **Все программы** > **Kaspersky Security Gateway** > **Консоль Kaspersky Security Gateway**.

   Откроется окно **Kaspersky Security Gateway**.

   > Вы можете также открыть Консоль, выбрав пункт **Kaspersky Security Gateway** в меню значка Kaspersky Security Gateway в области уведомлений.

2. В узле **Kaspersky Security Gateway** выберите вложенный узел **IEC 60870-5-104**.
3. В разделе **Настройка передачи данных** на панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Настройки**.

4. В группе **Параметры передачи данных** снимите или установите флажок **Включить передачу данных**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes передает состояние защиты узлов промышленной сети из Kaspersky Security Center в систему SCADA.

   Если флажок снят, передача данных не выполняется.

   По умолчанию флажок снят.

5. В группе **Параметры соединения** настройте следующие параметры:

   - **Адрес устройства**. Дополнительный адрес, присвоенный компьютеру в системе SCADA.Диапазон возможных значений: 0–65535.
   - **Порт устройства**. Номер порта для подключения к системе SCADA. Диапазон возможных значений: 0–65535.
   - **Период ожидания TCP-соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания отправки сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания подтверждения сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Максимальное количество получаемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.
   - **Максимальное количество отправляемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.

6. Нажмите на кнопку **OK**.
7. В разделе **Отслеживаемые значения** на панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Параметры отслеживаемых значений**.

8. В списке отображаются текущие параметры для значений с присвоенными тегами. Если требуется, измените следующие параметры:

   - Установите флажки рядом со значениями, которые требуется отслеживать.
   - Назначьте новый служебный тег в столбце **Служебный тег**.

9. Нажмите на кнопку **OK**.

Новые параметры будут сохранены.

kaspersky

Настройка передачи данных по протоколу OPC через Консоль

Для успешной передачи данных по протоколу OPC должны быть выполнены следующие условия:

- Программе OPCEnum предоставлены необходимые права DCOM в системе SCADA и в Kaspersky Security Gateway.
- Для компьютера с установленным Kaspersky Security Gateway и системой SCADA применяется единая аутентификация: либо используется доменная аутентификация, либо для всех компьютеров рабочей группы используется одно и то же имя пользователя и пароль.

► *Чтобы настроить передачу данных по протоколу OPC через Консоль Kaspersky Security Gateway, выполните следующие действия:*

1. В меню **Пуск** Microsoft Windows выберите **Все программы** > **Kaspersky Security Gateway** > **Консоль Kaspersky Security Gateway**.

   Откроется окно **Kaspersky Security Gateway**.

   > Вы можете также открыть Консоль, выбрав пункт **Kaspersky Security Gateway** в меню значка Kaspersky Security Gateway в области уведомлений.

2. В узле **Kaspersky Security Gateway** выберите вложенный узел **OPC**.
3. В разделе **Параметры передачи данных** на панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Настройки**.
4. Снимите или установите флажок **Включить передачу данных**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes передает состояние защиты узлов промышленной сети из Kaspersky Security Center в систему SCADA.

   Если флажок снят, передача данных не выполняется.

   По умолчанию флажок снят.
5. Нажмите на кнопку **OK**.
6. В разделе **Отслеживаемые значения** на панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Параметры отслеживаемых значений**.
7. В списке отображаются текущие параметры для значений с присвоенными тегами. Если требуется, измените следующие параметры:
   - Установите флажки рядом со значениями, которые требуется отслеживать.
   - Назначьте новый служебный тег в столбце **Служебный тег**.

Новые параметры будут сохранены.

kaspersky

Настройка передачи данных по протоколу IEC 60870-5-104 через конфигурационный файл

► *Чтобы настроить передачу данных по протоколу IEC 60870-5-104 через конфигурационный файл Kaspersky Security Gateway, выполните следующие действия:*

1. В любом доступном текстовом редакторе откройте конфигурационный файл C:\ProgramData\Kaspersky Lab\Security Gateway\Settings\ProtocolIECSettings.xml.
2. Укажите общие параметры подключения Kaspersky Security Gateway к системе SCADA:
   - **Адрес устройства**. Дополнительный адрес, присвоенный компьютеру в системе SCADA. Диапазон возможных значений: 0–65535.
   - **Порт устройства**. Номер порта для подключения к системе SCADA. Диапазон возможных значений: 0–65535.
   - **Период ожидания TCP-соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания отправки сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания подтверждения сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Максимальное количество получаемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.
   - **Максимальное количество отправляемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.
3. Укажите данные отслеживаемых компьютеров. Для этого в разделе <MonitoredHosts/> укажите пары имен и адресов с помощью тегов <MonitoredHosts Name="" Address=""/>, разделенных точкой с запятой (;):
   - **Имя ПЛК**. Имя компьютера с установленной программой Kaspersky Industrial CyberSecurity for Nodes, состояние защиты которого Kaspersky Security Gateway отправляет в систему SCADA.
   - **IP-адрес**. IP-адрес компьютера с установленной программой Kaspersky Industrial CyberSecurity for Nodes, состояние защиты которого Kaspersky Security Gateway отправляет в систему SCADA.
4. Сохраните конфигурационный файл.
5. Перезапустите службу Kaspersky Security Gateway, чтобы новые параметры вступили в силу.

Ниже приведен пример файла конфигурации для протокола IEC 60870-5-104:

Пример:

```
<?xml version="1.0" encoding="utf-8"?>
<KSGTW-Settings>
<DataTransmissionOptions>
<SlaveAddress>1</SlaveAddress>
<SlavePort>2404</SlavePort>
<TcpConnectionTimeoutSeconds>30</TcpConnectionTimeoutSeconds>
<MessageSendTimeoutSeconds>15</MessageSendTimeoutSeconds>
<MessageConfirmationTimeoutSeconds>10</MessageConfirmationTimeoutSeconds>
<ConnectionTestTimeoutSeconds>20</ConnectionTestTimeoutSeconds>
<MaxUnconfirmedMessagesAllowSend>12</MaxUnconfirmedMessagesAllowSend>
<MaxUnconfirmedMessagesAllowRecieve>8</MaxUnconfirmedMessagesAllowRecieve>
<EnableDataTransmission>yes</EnableDataTransmission>
<SpontaneousTransmission>yes</SpontaneousTransmission>
</DataTransmissionOptions>
<MonitoredHosts/>
<MonitoredDevices/>
</KSGTW-Settings>
```

Настройка передачи данных по протоколу OPC через конфигурационный файл

► *Чтобы настроить параметры сервера OPC с помощью конфигурационного файла, выполните следующие действия:*

1. В любом доступном текстовом редакторе откройте конфигурационный файл со служебными параметрами Kaspersky Security Gateway для сервера OPC, который находится по следующему пути: C:\ProgramData\Kaspersky Lab\Security Gateway\Settings\ProtocolOPCSettings.xml.
2. Настройте передачу данных.
3. Сохраните конфигурационный файл.
4. Перезапустите службу Kaspersky Security Gateway, чтобы новые параметры вступили в силу.

Пример:

```
<?xml version="1.0" encoding="utf-8"?>
<KSGTW-Settings>
<DataTransmissionOptions>
<EnableDataTransmission>yes</EnableDataTransmission>
<SpontaneousTransmission>yes</SpontaneousTransmission>
</DataTransmissionOptions>
<MonitoredHosts/>
<MonitoredDevices/>
</KSGTW-Settings>
```

Настройка дополнительных параметров Kaspersky Security Gateway

► *Чтобы настроить дополнительные параметры Kaspersky Security Gateway, выполните следующие действия:*

1. В меню **Пуск** Microsoft Windows выберите **Все программы** > **Kaspersky Security Gateway** > **Консоль Kaspersky Security Gateway**.

   Откроется окно **Kaspersky Security Gateway**.

   Вы можете также открыть Консоль, выбрав пункт **Kaspersky Security Gateway** в меню значка Kaspersky Security Gateway в области уведомлений.

2. Выберите узел **Kaspersky Security Gateway**.
3. В разделе **Параметры программы** на панели результатов нажмите на ссылку **Настройка программы**.

   Откроется окно **Настройки программы**.
4. В разделе **Опрос** задайте **Период опроса (сек)**.
5. В разделе **Трассировка**:
   - Снимите или установите флажок **Записывать файл трассировки**.
   - В раскрывающемся списке выберите **Уровень** детализации регистрируемой информации.
6. В окне **Настройки программы** нажмите на кнопку **OK**.

Дополнительные параметры Kaspersky Security Gateway можно настроить с помощью конфигурационного файла AppSettings.xml, расположенного в папке C:\ProgramData\Kaspersky Lab\Security Gateway\Settings.

kaspersky

Просмотр событий Kaspersky Security Gateway

Во время работы Kaspersky Security Gateway могут происходить следующие события:

- Включение и выключение экземпляров службы Kaspersky Security Gateway.
- Проблемы взаимодействия Kaspersky Security Gateway с системой SCADA.
- Проблемы подключения к Серверу администрирования Kaspersky Security Center и получения данных от Сервера администрирования.
- Проблемы с доступом к конфигурационному файлу Kaspersky Security Gateway.

Kaspersky Security Gateway сохраняет записи об этих событиях в журнале событий Microsoft Windows.

► *Чтобы просмотреть записи о событиях,*

в меню **Пуск** выберите **Панель управления > Администрирование > Просмотр событий > Журналы приложений и служб > Kaspersky Security Gateway**.

kaspersky

Интеграция со сторонними системами

Этот раздел содержит описание интеграции Kaspersky Industrial CyberSecurity for Nodes с функциями и технологиями сторонних производителей.

В этом разделе

Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы "Системный монитор" Microsoft Windows, которые регистрирует Kaspersky Industrial CyberSecurity for Nodes во время установки.

В этом разделе

О счетчиках производительности Kaspersky Industrial CyberSecurity for Nodes

Счетчики производительности – компонент Kaspersky Industrial CyberSecurity for Nodes, с помощью которого вы можете контролировать производительность программы во время выполнения задач постоянной защиты компьютера. Вы можете обнаружить узкие места и недостаточность ресурсов при совместной работе с другими программами. Вы можете диагностировать сбои в работе и неоптимальную настройку Kaspersky Industrial CyberSecurity for Nodes.

Вы можете просматривать счетчики производительности Kaspersky Industrial CyberSecurity for Nodes, открыв консоль **Производительность** Панели управления Windows в разделе **Администрирование**.

В следующих разделах приведены определения счетчиков, рекомендованные интервалы считывания показаний, пороговые значения и рекомендованные значения параметров Kaspersky Industrial CyberSecurity for Nodes для случаев, когда значения счетчиков превышают пороговые значения.

Общее количество отвергнутых запросов

Таблица 112. Общее количество отвергнутых запросов

Название	Общее количество отвергнутых запросов
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты процессами программы; рассчитывается с момента последнего запуска Kaspersky Industrial CyberSecurity for Nodes. Программа пропускает объекты, запросы на обработку которых отвергаются процессами Kaspersky Industrial CyberSecurity for Nodes.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • снижение эффективности постоянной защиты компьютера из-за повышенной нагрузки на процессы Kaspersky Industrial CyberSecurity for Nodes; • прерывание постоянной защиты компьютера из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: • Счетчик показывает несколько запросов, отвергнутых в течение длительного времени: все процессы Kaspersky Industrial CyberSecurity for Nodes были полностью загружены, поэтому программа Kaspersky Industrial CyberSecurity for Nodes не смогла проверить объекты. Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты компьютера. Можно использовать такой параметр Kaspersky Industrial CyberSecurity for Nodes, как **Количество процессов для постоянной защиты**. • Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Industrial CyberSecurity for Nodes не проверяет объекты при обращении к ним. Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

Общее количество пропущенных запросов

Таблица 113. Общее количество пропущенных запросов

Название	Общее количество пропущенных запросов
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Industrial CyberSecurity for Nodes, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Industrial CyberSecurity for Nodes пропускает такой объект и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1.
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за сбоев диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Kaspersky Industrial CyberSecurity for Nodes, чтобы восстановить простаивающие потоки.

kaspersky

Количество запросов, не обработанных из-за нехватки системных ресурсов

Таблица 114. Количество запросов, не обработанных из-за нехватки системных ресурсов

Название	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
Определение	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes пропускает запросы на обработку объектов, которые не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты компьютера, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, рабочим процессам Kaspersky Industrial CyberSecurity for Nodes требуется больший объем оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

kaspersky

Количество запросов, отправленных на обработку

Таблица 115. Количество запросов, отправленных на обработку

Название	Количество запросов, отправленных на обработку.
Определение	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Industrial CyberSecurity for Nodes и общий уровень файловой активности на защищаемом компьютере.
Нормальное / пороговое значение	Значение счетчика может изменяться в зависимости от уровня файловой активности на защищаемом компьютере.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Недоступно

kaspersky

Среднее количество потоков диспетчера файловых перехватов

Таблица 116. Среднее количество потоков диспетчера файловых перехватов

Название	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams)
Определение	Количество потоков диспетчера файловых перехватов в одном процессе и среднее по всем процессам, участвующим в задачах постоянной защиты компьютера.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение уровня постоянной защиты компьютера из-за полной загрузки процессов Kaspersky Industrial CyberSecurity for Nodes.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Kaspersky Industrial CyberSecurity for Nodes пропустит объект. Увеличьте количество процессов Kaspersky Industrial CyberSecurity for Nodes для задач постоянной защиты компьютера. Можно использовать такой параметр Kaspersky Industrial CyberSecurity for Nodes, как **Количество процессов для постоянной защиты**.

kaspersky

Максимальное количество потоков диспетчера файловых перехватов

Таблица 117. Максимальное количество потоков диспетчера файловых перехватов

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном процессе и максимальное по всем процессам, участвующим в задачах постоянной защиты компьютера.
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Kaspersky Industrial CyberSecurity for Nodes неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

Количество элементов в очереди зараженных объектов

Таблица 118. Количество элементов в очереди зараженных объектов

Название	Количество элементов в очереди зараженных объектов.
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • прерывание постоянной защиты компьютера из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессов из-за неравномерного распределения процессорного времени между рабочими процессами и Kaspersky Industrial CyberSecurity for Nodes; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Industrial CyberSecurity for Nodes обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Kaspersky Industrial CyberSecurity for Nodes не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов). Перезапустите Kaspersky Industrial CyberSecurity for Nodes. • Не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes дополнительного процессорного времени, например, снизив нагрузку на защищаемый компьютер со стороны других программ. • Возникла вирусная эпидемия. О возникновении вирусной эпидемии свидетельствует большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи.

kaspersky

Количество объектов, обрабатываемых за секунду

Таблица 119. Количество объектов, обрабатываемых за секунду

Название	Количество объектов, обрабатываемых за секунду (Number of objects processed per second)
Определение	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.
Назначение	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности защищаемого компьютера, возникшее из-за недостаточности процессорного времени, выделяемого рабочим процессам Kaspersky Industrial CyberSecurity for Nodes, или из-за сбоев в работе Kaspersky Industrial CyberSecurity for Nodes.
Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от установленных значений параметров Kaspersky Industrial CyberSecurity for Nodes и от загрузки защищаемого компьютера процессами других программ. Отслеживайте среднее значение показаний счетчика в течение продолжительного времени. Если среднее значение показаний счетчика снизилось, то могла возникнуть одна из следующих ситуаций: • Рабочим процессам Kaspersky Industrial CyberSecurity for Nodes не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes дополнительного процессорного времени, например, снизив нагрузку на защищаемый компьютер со стороны других программ. • Возник сбой в работе Kaspersky Industrial CyberSecurity for Nodes (простаивает несколько потоков). Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

SNMP-счетчики и ловушки в Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о счетчиках и ловушках Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

О SNMP-счетчиках и ловушках Kaspersky Industrial CyberSecurity for Nodes

Если вы включили компонент Счетчики и ловушки SNMP в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes на компьютере-рабочем месте администратора, запустите на защищаемом компьютере Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

SNMP-счетчики Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

Счетчики производительности

Таблица 120. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отправленных на обработку (на стр. 890)
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов (на стр. 893)
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (на стр. 894)
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Industrial CyberSecurity for Nodes в текущий момент

Счетчики карантина

Таблица 121. Счетчики карантина

Счетчик	Определение
totalObjects	Количество объектов в папке карантина в текущий момент
totalSuspiciousObjects	Количество возможно зараженных объектов в папке карантина в текущий момент
currentStorageSize	Общий объем данных в папке карантина (МБ)

Счетчик резервного хранилища

Таблица 122. Счетчик резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Общий объем данных в папке резервного хранилища (МБ)

kaspersky

Общие счетчики

Таблица 123. Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней полной проверки важных областей защищаемого компьютера (промежуток времени в секундах с момента завершения задачи Проверка важных областей).
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлен активный и дополнительный ключ, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом.
currentApplicationUptime	Время работы Kaspersky Industrial CyberSecurity for Nodes с момента его последнего запуска, в сотых долях секунды.

Счетчик обновлений

Таблица 124. Счетчик обновлений

Счетчик	Определение
avBasesAge	"Возраст" баз (промежуток времени в сотых долях секунды с момента создания последних установленных обновлений баз)

Счетчики постоянной защиты файлов

Таблица 125. Счетчики постоянной защиты файлов

Счетчик	Определение
totalObjectsProcessed	Общее количество проверенных объектов с момента последнего запуска задачи Постоянная защита файлов
totalInfectedObjectsFound	Общее количество обнаруженных зараженных и других объектов с момента последнего запуска задачи Постоянная защита файлов
totalSuspiciousObjectsFound	Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска задачи Постоянная защита файлов
totalVirusesFound	Общее количество обнаруженных объектов с момента последнего запуска задачи Постоянная защита файлов
totalObjectsQuarantined	Общее количество зараженных, возможно зараженных и прочих объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes поместила на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось поместить на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDisinfected	Общее количество зараженных объектов, которые вылечила программа Kaspersky Industrial CyberSecurity for Nodes; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и прочих объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось вылечить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые удалила программа Kaspersky Industrial CyberSecurity for Nodes; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось удалить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsBackedUp	Общее количество зараженных и прочих объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes поместила в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotBackedUp	Общее количество зараженных и прочих объектов, которые программе Kaspersky Industrial CyberSecurity for Nodes не удалось поместить в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

kaspersky

SNMP-ловушки Kaspersky Industrial CyberSecurity for Nodes и их параметры

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие параметры SNMP-ловушек:

- eventThreatDetected: Обнаружен объект.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в резервном хранилище превысил значение, заданное параметром **Максимальный размер резервного хранилища (МБ)**. Kaspersky Industrial CyberSecurity for Nodes продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: Достигнут порог свободного места в резервном хранилище. Объем свободного места в резервном хранилище меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Industrial CyberSecurity for Nodes продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventQuarantineStorageSizeExceeds: Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, заданное параметром **Максимальный размер карантина (МБ)**. Kaspersky Industrial CyberSecurity for Nodes продолжает помещать возможно зараженные объекты на карантин.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds: Достигнут порог свободного места в карантине. Объем свободного места в папке карантина меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Industrial CyberSecurity for Nodes продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined: Ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason
- eventObjectNotBackuped: Ошибка сохранения копии объекта в резервное хранилище.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError: Внутренняя ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: Ошибка резервного хранилища.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: Базы программы устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated: Базы программы сильно устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted: программа Kaspersky Industrial CyberSecurity for Nodes запущена.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown: программа Kaspersky Industrial CyberSecurity for Nodes остановлена.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей давно не выполнялась. Количество дней с момента последнего завершения задачи Проверка важных областей.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: Срок действия лицензии истек.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: Ошибка выполнения задачи.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName
- eventUpdateError: Ошибка при выполнении задачи обновления.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

kaspersky

Описания и возможные значения параметров SNMP-ловушек Kaspersky Industrial CyberSecurity for Nodes

Ниже приведено описание и допустимые значения параметров ловушек:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.

  Параметр может принимать следующие значения:

  - critical (1) – критический;
  - warning (2) – предупреждение;
  - info (3) – информационный.
- userName: имя пользователя (например, имя пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя защищаемого устройства (например, имя защищаемого устройства, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

  Параметр может принимать следующие значения:

  - unknown (0) – функциональный компонент не определен;
  - quarantine (1) – Карантин;
  - backup (2) – Резервное хранилище;
  - reporting (3) – Журналы выполнения задач;
  - updates (4)– Обновление;
  - realTimeProtection (5) – Постоянная защита файлов;
  - onDemandScanning (6) – Проверка по требованию;
  - product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Industrial CyberSecurity for Nodes в целом;
  - systemAudit (8) – Журнал системного аудита.
- eventReason: причина возникновения события.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Industrial CyberSecurity for Nodes будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).
- threatName: имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.

- detectType: тип обнаруженного объекта.

  Параметр может принимать следующие значения:

  - undefined (0) – не определен;
  - virware – классические вирусы и сетевые черви;
  - trojware – троянские программы;
  - malware – прочие вредоносные программы;
  - adware – рекламные программы;
  - pornware – порнографические программы;
  - riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройству или личным данным.
- detectCertainty: степень уверенности обнаружения угрозы.

  Параметр может принимать следующие значения:

  - Suspicion (возможно зараженный) – программа Kaspersky Industrial CyberSecurity for Nodes обнаружила частичное совпадение участка кода объекта с известным участком вредоносного кода.
  - Sure (зараженный) – программа Kaspersky Industrial CyberSecurity for Nodes обнаружила полное совпадение участка кода объекта с известным участком вредоносного кода.
- days: количество дней (например, количество дней до окончания срока действия лицензии).
- errorCode: код ошибки.
- knowledgeBaseId: адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
- taskName: название задачи.
- updaterErrorEventReason: причина ошибки обновления.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonAccessDenied – доступ запрещен;
  - reasonUrlsExhausted – список источников обновлений исчерпан;
  - reasonInvalidConfig – неправильный файл конфигурации;
  - reasonInvalidSignature – неверная подпись;
  - reasonCantCreateFolder – невозможно создать папку;
  - reasonFileOperError – файловая ошибка;
  - reasonDataCorrupted – объект поврежден;
  - reasonConnectionReset – сброс соединения;
  - reasonTimeOut – истекло время ожидания при соединении;
  - reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;
  - reasonServerAuthError – ошибка проверки подлинности на сервере;
  - reasonHostNotFound – устройство не найдено;

- reasonServerBusy – сервер недоступен;
- reasonConnectionError – ошибка соединения;
- reasonModuleNotFound – объект не найден;
- reasonBlstCheckFailed(16) – ошибка проверки списка запрещенных ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.

- storageObjectNotAddedEventReason: причина, по которой объект не был помещен в резервное хранилище или на карантин.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonStorageInternalError – ошибка базы данных; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageReadOnly – база данных доступна только для чтения; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageIOError – ошибка ввода-вывода: а) программа Kaspersky Industrial CyberSecurity for Nodes повреждена и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Industrial CyberSecurity for Nodes, поврежден.
  - reasonStorageCorrupted – хранилище повреждено; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageFull – база данных заполнена; требуется свободное место на диске.
  - reasonStorageOpenError – не удается открыть файл базы данных; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Industrial CyberSecurity for Nodes.
  - reasonObjectNotFound – помещаемый на карантин объект отсутствует на диске.
  - reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
  - reasonDiskOutOfSpace – недостаточно места на диске.

Интеграция с WMI

Kaspersky Industrial CyberSecurity for Nodes поддерживает интеграцию с инструментарием управления Windows (Windows Management Instrumentation, WMI): вы можете использовать клиентские системы, которые получают с помощью WMI данные по стандарту Web-Based Enterprise Management (WBEM), для получения данных о статусе программы Kaspersky Industrial CyberSecurity for Nodes и ее компонентов.

В момент установки Kaspersky Industrial CyberSecurity for Nodes регистрирует в системе собственный модуль для создания пространства имен Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве. Пространство имен Kaspersky Industrial CyberSecurity for Nodes позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Industrial CyberSecurity for Nodes.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

Непериодические задачи – это задачи программы, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения.

Результаты выполнения таких задач фиксируются непрерывно в ходе выполнения и представляют собой отдельные события (например, обнаружение зараженного объекта одной из задач постоянной защиты компьютера). Задачами такого типа можно управлять с помощью политик Kaspersky Security Center.

Периодические задачи – это задачи программы, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде количества процентов. Результаты выполнения таких задач фиксируются по завершении задачи и представляют собой отдельный элемент или факт изменения состояния программы (например, завершение Обновления баз программы, сформированные конфигурационные файлы для задач автоматического формирования правил). На одном защищаемом устройстве одновременно может быть запущено несколько периодических задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять периодическими задачами с помощью групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из него динамические данные, вы сможете получить следующие данные о текущем состоянии программы.

Таблица 126. Данные о состоянии программы

Свойство экземпляра класса	Описание	Значения
ProductName	Название установленной программы.	Полное название программы без номера версии.
ProductVersion	Полный номер версии установленной программы.	Полный номер версии программы, включая номер сборки.
InstalledPatches	Набор отображаемых имен установленных патчей.	Перечень критических исправлений, установленных для программы.
IsLicenseInstalled	Статус активации программы.	Статус ключа, с помощью которого активирована программа. Возможные значения: • False – В программе не добавлен лицензионный ключ. • True - В программе добавлен лицензионный ключ.
LicenseDaysLeft	Количество дней до истечения срока действия текущей лицензии.	Количество дней, оставшихся до истечения срока действия текущей лицензии. Возможные неположительные значения: • 0 - Срок действия лицензии истек. • -1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по причине нахождения в списке запрещенных ключей).

Свойство экземпляра класса	Описание	Значения
AVBasesDatetime	Временная отметка для текущей версии антивирусных баз.	Дата и время формирования антивирусных баз, используемых в текущий момент. Если установленная программа не использует антивирусные базы, поле содержит значение Not installed.
IsExploitPreventionEnabled	Статус компонента Защита от эксплойтов.	Статус компонента Защита от эксплойтов. Возможные значения: • True - Компонент Защита от эксплойтов включен и выполняет функции защиты. • False - Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
ProtectionTasksRunning	Набор запущенных задач защиты.	Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные непериодические задачи. Если не запущена ни одна из непериодических задач, поле содержит значение "Нет".
IsAppControlRunning	Статус выполнения задачи Контроль запуска программ.	Статус выполнения задачи Контроль запуска программ. • True - Задача Контроль запуска программ выполняется в текущий момент. • False - Задача Контроль запуска программ не выполняется в текущий момент или компонент Контроль запуска программ не установлен.

Свойство экземпляра класса	Описание	Значения
AppControlMode	Режим работы задачи Контроль запуска программ.	Описание текущего состояния компонента Контроль запуска программ, а также выбранного режима соответствующей задачи. Возможные значения: • Active - в параметрах задачи указан режим **Активный**. • Statistics Only - в параметрах задачи указан режим **Только статистика**. • Not installed - Компонент Контроль запуска программ не установлен.
AppControlRulesNumber	Общее количество правил контроля запуска программ.	Количество правил, заданных в параметрах задачи Контроль запуска программ в текущий момент.
AppControlLastBlocking	Временная отметка последней блокировки запуска программы, выполненной задачей Контроль запуска программ в любом режиме.	Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима выполнения задачи. Если на момент выполнения запроса WMI не зарегистрировано ни одного случая блокировки запуска программы, в поле отображается значение "Нет".
PeriodicTasksRunning	Набор запущенных периодических задач.	Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны отображаться все запущенные периодические задачи. Если не запущена ни одна из периодических задач, поле содержит значение "Нет".
ConnectionState	Состояние соединения между компонентом Поставщик WMI и службой Kaspersky Security (KAVFS).	Информация о статусе соединения между компонентом Поставщик WMI и службой Kaspersky Security. Возможные значения: • Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы. • Failed. Error Code: <code> - Соединение не удалось установить из-за ошибки с указанным кодом.

Указанные данные являются свойствами экземпляра класса KasperskySecurity_ProductInfo.ProductName=Kaspersky Industrial CyberSecurity for Nodes, где:

- KasperskySecurity_ProductInfo – имя класса Kaspersky Industrial CyberSecurity for Nodes;
- .ProductName=Kaspersky Industrial CyberSecurity for Nodes – ключевые свойства Kaspersky Industrial CyberSecurity for Nodes.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

kaspersky

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 перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.

kaspersky

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли программы 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. 911) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. 911).

В этом разделе

Сортировка объектов на карантине

По умолчанию объекты на карантине отсортированы в таблице по дате помещения на карантин в обратном хронологическом порядке. Чтобы найти нужный объект, можно отсортировать объекты по столбцам с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок столбца, по которому вы хотите отсортировать объекты в таблице.

Объекты в таблице писке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, можно отфильтровать объекты в таблице – отобразить только те объекты, которые удовлетворяют заданным критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать фильтры, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в таблице могут различаться в зависимости от значения, выбранного 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 в списке в окне **Параметры фильтра**. Отредактируйте требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.
5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы вернуть отображение всех объектов на карантине,*

в контекстном меню узла **Снять фильтр** выберите пункт **Карантин**.

kaspersky

Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Industrial CyberSecurity for Nodes выполняет локальную системную задачу Проверка объектов на карантине. Параметры задачи приведены в следующей таблице. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Можно настраивать расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Industrial CyberSecurity for Nodes может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Industrial CyberSecurity for Nodes может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Таблица 127. Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки.	Папка карантина
Параметры безопасности.	Единые для всей области проверки (значения приводятся в следующей таблице)

Таблица 128. Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверять объекты	Все объекты области проверки
Оптимизация	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действия над возможно зараженными объектами	Пропускать
Исключать файлы	Нет
Не обнаруживать	Нет
Останавливать проверку, если она длится более (сек.)	Не задано

Параметр безопасности	Значение
Не проверять объекты размером более (МБ)	Не задано
Альтернативные потоки NTFS	Включено
Загрузочные секторы дисков и 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.
Проверять подпись 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 помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстановить любой объект с 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 защищаемого компьютера и хотите его использовать. Чтобы программа Kaspersky Industrial CyberSecurity for Nodes не изолировала 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 "Доверенная зона" на стр. 606).

При восстановлении объектов можно выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом компьютере, в указанной папке на защищаемом компьютере, на котором установлена Консоль программы.

Можно указать папку 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 защищаемого 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 не включает его в составной объект при восстановлении. Объект, помещенный на карантин, сохраняется отдельно в выбранную папку.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты с карантина, выполните следующие действия:*

1. В дереве Консоли программы 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 клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного 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.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.
5. Выполните одно из следующих действий:
   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другую папку на защищаемом компьютере, на котором установлена Консоль программы, выберите **Восстановить в папку на локальном компьютере**, а затем выберите нужную папку или укажите путь к ней.
6. Чтобы сохранить копию объекта в папке *Карантин* после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

7. 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 местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Industrial CyberSecurity for Nodes:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Применить ко всем выбранным объектам** или **Заменить**, к остальным выбранным объектам, установите флажок **Переименовать**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

   c. Нажмите на кнопку **ОК**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

   Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (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 программы откройте контекстное меню узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes поместит указанный файл на карантин.

kaspersky

Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет из папки карантина объекты, статус которых изменился на *Зараженный или обнаруживаемый* при проверке карантина с использованием обновленных баз, если программа Kaspersky Industrial CyberSecurity for Nodes не смогла их вылечить. Kaspersky Industrial CyberSecurity for Nodes не удаляет остальные объекты из карантина.

Можно удалять объекты с карантина.

► *Чтобы удалить объекты с карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены с 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 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 в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Industrial CyberSecurity for Nodes признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы с карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Нельзя отправлять объекты с 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** 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 защищаемом компьютере, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** 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.

   К сообщению будет приложен архив <имя объекта>.cab. Архив содержит файл <uuid>.klq с зашифрованным объектом, файл <uuid>.txt с информацией об объекте, полученной из Kaspersky Industrial CyberSecurity for Nodes, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Industrial CyberSecurity for Nodes и операционной системе защищаемого компьютера:

   - название и версию операционной системы;
   - название и версию Kaspersky Industrial CyberSecurity for Nodes;
   - дату выпуска последних установленных обновлений баз программы;
   - активный ключ.

   Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и более эффективно проанализировать файл. Однако если вы не хотите передавать эту информацию, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на защищаемом компьютере, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл можно 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 **ОК**.
2. Выберите папку на диске защищаемого компьютера, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

kaspersky

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 программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Карантин: свойства** настройте параметры карантина в соответствии с вашими требованиями:
   - В разделе **Параметры карантина**:
     - **Папка карантина**

       Путь к папке карантина в формате UNC (Universal Naming Convention).

       По умолчанию используется путьC:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Quarantine\.

     - **Максимальный размер карантина (МБ)**

       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 регистрирует 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 отслеживает суммарный размер размещенных в карантине объектов.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в карантине.

       По умолчанию флажок снят.

     - **Порог доступного пространства (МБ)**

       Флажок включает или выключает отслеживание минимального объема свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в папке карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает размер свободного места в папке карантина.

Флажок **Порог доступного пространства (МБ)** активен, если установлен флажок **Максимальный размер карантина (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 уведомит вас об этом, не переставая помещать объекты на карантин.

- В разделе **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:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в дереве Консоли программы в контекстном меню узла **Карантин** выберите пункт **Статистика**.

В окне **Статистика карантина** 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 признала возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которым присвоен статус *Ложное срабатывание*, поскольку при проверке карантина с применением обновленных баз они были признаны незараженными.
Вылечено объектов	Количество объектов, которым присвоен статус *Вылечен* после проверки карантина.
Всего объектов	Общее количество объектов на карантине.

kaspersky

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 сохраняет зашифрованные копии объектов со статусом *Зараженный* в папке *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 сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Industrial CyberSecurity for Nodes признает зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Industrial CyberSecurity for Nodes помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Можно восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом компьютере. Вы можете восстановить файл из резервного хранилища, если зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Industrial CyberSecurity for Nodes не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого компьютера.

kaspersky

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только с помощью узла **Резервное хранилище** Консоли программы.. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы 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.

В этом разделе

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их попадания в резервное хранилище в обратном хронологическом порядке. Чтобы найти нужный файл, отсортируйте файлы по содержимому любого столбца в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы 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 программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В таблице файлов в узле **Резервное 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 сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы 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 программы 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, по которому выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут различаться в зависимости значения, выбранного в поле **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 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 требуемые значения в полях **Название поля**, **Оператор** и **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 **Снять фильтр** выберите пункт **Резервное хранилище**.

Восстановление файлов из резервного хранилища

Kaspersky Industrial CyberSecurity for Nodes 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 зараженный файл содержал важную информацию и при лечении файла программа Kaspersky Industrial CyberSecurity for Nodes не смогла сохранить его целостность, в результате чего информация в файле стала недоступной;

- если вы считаете файл безопасным для защищаемого компьютера и хотите его использовать. Чтобы программа Kaspersky Industrial CyberSecurity for Nodes не признавала 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 значения параметра **Исключать файлы** или **Не обнаруживать** соответствующих задач.

  Восстановление файлов из резервного хранилища может привести к заражению защищаемого компьютера.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходное местоположение (по умолчанию), в специальную папку для восстановленных объектов на защищаемом компьютере, в указанную папку на защищаемом компьютере, на котором установлена Консоль программы.

Можно указать папку 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. 926).

По умолчанию, когда Kaspersky Industrial CyberSecurity for Nodes восстанавливает файл, его копия сохраняется в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы 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 клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного 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.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.
5. Выполните одно из следующих действий:
   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другую папку на защищаемом компьютере, на котором установлена Консоль программы, выберите **Восстановить в папку на локальном компьютере**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалить объекты из хранилища после восстановления** (по умолчанию флажок снят).
7. 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 местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере**, все объекты будут сохранены в одну указанную папку.
8. Нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes начнет восстанавливать первый из выбранных вами объектов.
9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.
   a. Выберите одно из следующих действий Kaspersky Industrial CyberSecurity for Nodes:
      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.
   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Применить ко всем выбранным объектам** или **Заменить**, к остальным выбранным объектам, установите флажок **Переименовать**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.
   c. Нажмите на кнопку **ОК**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

► *Чтобы удалить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.

4. В окне подтверждения 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 программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Резервное хранилище: свойства** настройте параметры резервного хранилища в соответствии с вашими требованиями:

   В разделе **Параметры резервного хранилища**:

   - **Папка резервного хранилища**

     Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

     По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Backup\.

   - **Максимальный размер резервного 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 регистрирует 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 отслеживает суммарный размер размещенных в резервном хранилище объектов.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в резервном хранилище.

     По умолчанию флажок снят.

   - **Порог доступного пространства (МБ)**

     Флажок включает или выключает отслеживание минимального объема свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог доступного пространства в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 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 уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В разделе **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:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Можно просматривать информацию о текущем состоянии резервного хранилища – статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

Таблица 129. 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

kaspersky

Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры списка заблокированных сетевых сеансов.

В этом разделе

Список заблокированных сетевых сеансов

По умолчанию Список заблокированных сетевых сеансов доступен, если установлен хотя бы один из следующих компонентов: Постоянная защита файлов, Защита от сетевых угроз. Эти компоненты обнаруживают удаленные попытки зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого компьютера или сетевого хранилища в соответствии со списком заблокированных сетевых сеансов. Информация о заблокированных сетевых сеансах со всех защищаемых компьютеров отправляется в Kaspersky Security Center. Kaspersky Industrial CyberSecurity for Nodes блокирует текущий сеанс и делает недоступными общие папки или папки сетевого хранилища в рамках текущего сеанса.

Список заблокированных сетевых сеансов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать сетевые сессии, с которых ведется вредоносная деятельность**.
- Для задачи Защита от сетевых угроз: обнаружена активность, характерная для сетевых атак.

При обнаружении вредоносной активности или попыток шифрования задача отправляет информацию об атакующем сетевом сеансе в Список заблокированных сетевых сеансов, а для текущего сеанса атакующего устройства создается событие *Предупреждение*. Все попытки данного сеанса получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локальный уникальный идентификатор (LUID) узла, инициировавшего атакующий сетевой сеанс, добавлен в Список заблокированных сетевых сеансов, Kaspersky Industrial CyberSecurity for Nodes определяет IP-адрес этого узла и добавляет его в Список заблокированных сетевых сеансов вместо идентификатора LUID атакующего узла.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes удаляет заблокированные сетевые сеансы из списка через 30 минут после добавления. Доступ к сетевым файловым ресурсам восстанавливается автоматически после удаления сетевых сеансов из Списка заблокированных сетевых сеансов. Вы можете указать период, после которого заблокированные сетевые сеансы автоматически разблокируются.

В случае запрета доступа к управлению хранилищами какому-либо пользователю, Список заблокированных сетевых сеансов останется доступным. Параметры заблокированных сетевых сеансов не могут быть изменены, если у пользователя отсутствует разрешение типа **Права на изменение** для управления Kaspersky Industrial CyberSecurity for Nodes.

Управление списком заблокированных сетевых сеансов с помощью Плагина управления

В этом разделе описано, как настроить параметры Списка заблокированных сетевых сеансов с помощью интерфейса Плагина управления.

В этом разделе

Включение блокировки недоверенных сетевых сеансов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в список заблокированных сетевых сеансов и заблокировать для них доступ к сетевым файловым ресурсам, хотя бы 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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** > **Постоянная защита компьютера** > **Настройка** в разделе **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.
3. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**, чтобы программа Kaspersky Industrial CyberSecurity for Nodes блокировала текущий сеанс и устанавливала недоступность общих сетевых ресурсов для сетевых сеансов, проявляющих вредоносную активность.
4. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
5. В окне **Постоянная защита файлов** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** > **Контроль активности в сети** > **Настройка** в разделе **Защита от шифрования**.

   Откроется окно **Защита от шифрования**.
3. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
4. В окне **Защита от шифрования** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Параметры хранилищ**.
5. В разделе **Условия блокировки сетевых сессий** на закладке **Заблокированные сетевые сессии** укажите количество дней, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.
6. Нажмите на кнопку **ОК**.

kaspersky

Управление списком заблокированных сетевых сеансов с помощью Консоли программы

В этом разделе описано, как настроить параметры списка заблокированных сетевых сеансов с помощью интерфейса Консоли программы.

В этом разделе

Включение блокировки недоверенных сетевых сеансов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в **Заблокированные сетевые сессии** и заблокировать для них 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 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 разделе **Глубокий** установите флажок **Блокировать сетевые сессии, с которых ведется вредоносная деятельность**, чтобы программа Kaspersky Industrial CyberSecurity for Nodes блокировала доступ к сетевым файловым ресурсам для сетевых сеансов, проявляющих вредоносную активность, во время выполнения задачи Постоянная защита файлов.
5. Если задача не была запущена, выберите закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
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 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, выберите закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированные сетевые сессии**.
3. Выберите пункт меню **Свойства**.

   Откроется окно **Параметры Списка заблокированных сетевых сессий**.
4. В разделе **Условия блокировки сетевых сессий** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.
5. Нажмите на кнопку **ОК**.
6. Чтобы восстановить доступ для всех заблокированных сетевых сеансов, выполните следующие действия:
   a. Откройте контекстное меню вложенного узла **Заблокированные сетевые сессии**.
   b. Выберите пункт **Разблокировать все**.

      Все сетевые сеансы будут удалены из списка и разблокированы.
7. Чтобы удалить сетевые сеансы из списка заблокированных, выполните следующие действия:
   a. В списке заблокированных сетевых сеансов в панели результатов выберите один или несколько сеансов.
   b. Откройте контекстное меню вложенного узла **Заблокированные сетевые сессии**.
   c. Выберите пункт **Разблокировать выбранное**.

      Выбранные сетевые сеансы будут разблокированы.

Управление списком заблокированных сетевых сеансов с помощью Веб-плагина

В этом разделе описано, как настроить список заблокированных сетевых сеансов с помощью интерфейса Веб-плагина.

kaspersky

В этом разделе

Включение блокировки сетевых сеансов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в **Заблокированные сетевые сессии** и заблокировать для них доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

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

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Постоянная защита файлов**.
6. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**, чтобы программа Kaspersky Industrial CyberSecurity for Nodes блокировала текущий сеанс и устанавливала недоступность общих сетевых ресурсов для сетевых сеансов, проявляющих вредоносную активность.
7. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
8. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Параметры** в подразделе **Хранилища**.

6. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Хранилища**.

7. В разделе **Условия блокировки сетевых сессий** на закладке **Заблокированные сетевые сессии** укажите количество дней, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.

8. Нажмите на кнопку **ОК**.

kaspersky

Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes, о копировании обновлений и об откате обновлений баз Kaspersky Industrial CyberSecurity for Nodes, а также инструкции по настройке задач обновления баз и модулей программы.

В этом разделе

О задачах обновления

В Kaspersky Industrial CyberSecurity for Nodes предусмотрено четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

Для поддержания сертифицированного состояния программы запрещается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу программы из сертифицированного состояния.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского" – каждый час. Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. 941), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Industrial CyberSecurity for Nodes 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 копирует базы из источника обновлений на устройство и сразу переходит к их использованию в выполняющейся задаче Постоянная защита компьютера. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу Обновление баз программы каждый час.

Обновление модулей программы

По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет доступность обновлений модулей программы в источнике обновлений. Для использования установленных программных модулей требуется перезагрузка защищаемого устройства и / или перезапуск Kaspersky Industrial CyberSecurity for Nodes.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Industrial CyberSecurity for Nodes, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes загружает файлы обновлений баз программы 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 возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении модулей программы

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Industrial CyberSecurity for Nodes. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные (критичные) 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 запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Industrial CyberSecurity for Nodes с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждый защищаемый компьютер или использовать одно защищаемое устройство в качестве посредника, копируя на него обновления без установки, а затем распределяя их на защищаемые компьютеры в сети. Чтобы копировать и сохранять обновления без установки, используйте задачу Копирование обновлений.

Перед установкой обновлений модулей, Kaspersky Industrial CyberSecurity for Nodes создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Industrial CyberSecurity for Nodes 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 программы

Базы Kaspersky Industrial CyberSecurity for Nodes, 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 программы 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 устройства к минимуму, рекомендуется регулярно получать обновления баз программы.

По умолчанию, если базы Kaspersky Industrial CyberSecurity for Nodes не обновляются в течение недели с момента создания 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" на стр. 435) отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** в дереве Консоли программы. Вы можете использовать общие параметры Kaspersky Industrial CyberSecurity for Nodes, чтобы указать другое количество дней до возникновения этих событий. Вы можете также настроить уведомления администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. 965).

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 из других источников обновлений.

Можно загружать обновления на каждый защищаемый компьютер или использовать один защищаемый компьютер в качестве посредника. На него будут копироваться обновления, а затем распространяться на защищаемые устройства. Если вы используете программу Kaspersky Security Center для централизованного управления защитой устройств в организации, можно использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз программы вручную или по расписанию (см. раздел "Настройка параметров расписания задач" на стр. 425). По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу Обновление баз программы каждый час.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Industrial CyberSecurity for Nodes автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Industrial CyberSecurity for Nodes можно вручную откатить (см. раздел "Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes" на стр. 948) базы до ранее установленных обновлений.

Схемы обновления баз и модулей антивирусных программ в организации

Выбор источника обновлений в задачах обновления зависит используемой в организации схемы обновления баз и модулей программы.

Вы можете обновлять базы и модули Kaspersky Industrial CyberSecurity for Nodes на защищаемых компьютерах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый компьютер (схема 1);
- Загружать обновления из интернета на устройство-посредник и распределять обновления на защищаемые компьютеры с этого устройства.

  Посредником может служить любое устройство, на котором установлены следующие программы:

  - Kaspersky Industrial CyberSecurity for Nodes (схема 2).
  - Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через устройство-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность защищаемых компьютеров в сети.

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление баз и модулей программы напрямую из интернета

► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes напрямую из интернета,*

на каждом защищаемом компьютере в параметрах задач Обновление баз программы и Обновление модулей программы укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.

Вы можете указать в качестве источников обновлений другие HTTP- или FTP-серверы, на которых имеется папка обновлений.

Схема 2. Обновление баз и модулей программы через один из защищаемых компьютеров

► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes через один из защищаемых компьютеров, выполните следующие действия:*

1. Скопируйте обновления на выбранный защищаемый компьютер. Для этого выполните следующие действия:
   - На выбранном защищаемом компьютере настройте параметры задачи Копирование обновлений:
     a. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».
     a. 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 устройства-посредника, в которую будут загружаться обновления.

Kaspersky Industrial CyberSecurity for Nodes будет получать обновления через один из защищаемых компьютеров.

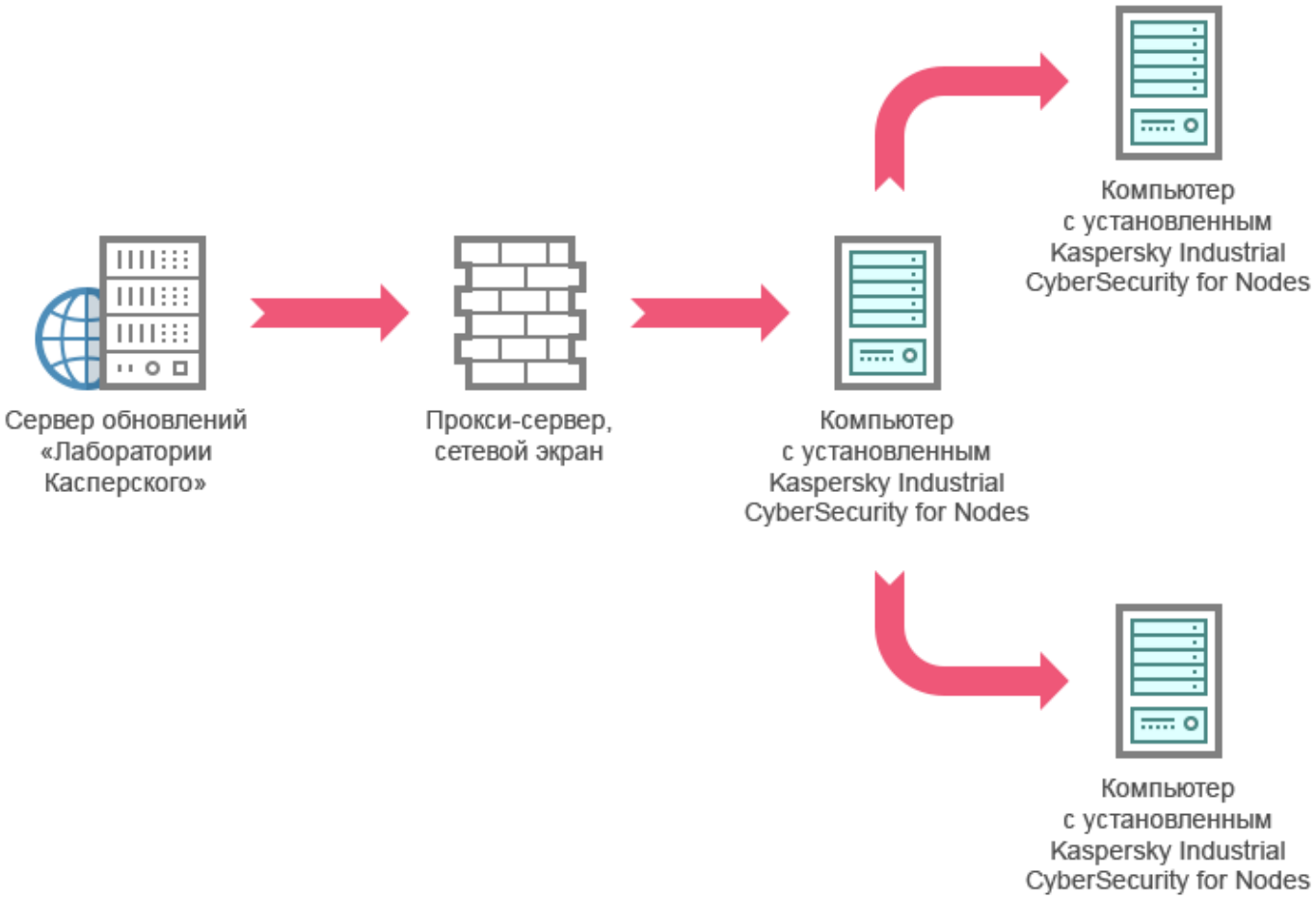


Схема 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств, можно загружать обновления с помощью Сервера администрирования Kaspersky Security Center, установленного в локальной сети (см. рис. ниже).

► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с серверов обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора защищаемых устройств:
     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).

     Частоту запуска **После получения обновлений Сервером администрирования** нельзя указать в Консоли программы.

   - 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 (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 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 Агент администрирования – программный компонент, входящий в комплект поставки Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Industrial CyberSecurity for Nodes на защищаемом компьютере. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

kaspersky

Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, можно 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 программы 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 разделе **Источник обновлений** выберите тип источника обновлений Kaspersky Industrial CyberSecurity for Nodes:

   - **Сервер администрирования Kaspersky Security Center**

     Kaspersky Industrial CyberSecurity for Nodes использует Сервер администрирования Kaspersky Security Center в качестве источника обновления.

     Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" осуществляется с помощью системы удаленного доступа Kaspersky Security Center и на защищаемом компьютере установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь защищаемых компьютеров с Сервером администрирования.

   - **Серверы обновлений "Лаборатории Касперского"**

     Kaspersky Industrial CyberSecurity for Nodes использует в качестве источников обновлений веб-сайты "Лаборатории Касперского". На этих веб-сайтах публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

     Этот вариант выбран по умолчанию.

   - **Другие HTTP-, FTP-серверы или сетевые ресурсы**

     Kaspersky Industrial CyberSecurity for Nodes использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы или папки на серверах локальной сети.

     Вы можете сформировать список источников, которые содержат актуальный набор обновлений, перейдя по ссылке **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 **ОК**.
   b. В разделе **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**.

      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 или выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского" или если установлен флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**.

     Если флажок установлен, используются параметры прокси-сервера.

     По умолчанию флажок установлен.
   - 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, используются параметры прокси-сервера.

     По умолчанию флажок снят.

   Информация о настройке дополнительных параметров прокси-сервера и параметров аутентификации для доступа к прокси-серверу приведена в разделе Запуск и настройка задачи Обновление баз программы.
7. Нажмите на кнопку **ОК**.

Настроенные параметры источника обновлений Kaspersky Industrial CyberSecurity for Nodes будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Industrial CyberSecurity for Nodes.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли программы 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, нажмите на кнопку **Добавить** и 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 к пользовательским источникам обновлений, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, когда он должен использоваться: до или после других источников.
   - Чтобы изменить путь к пользовательскому источнику обновлений, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
   - Чтобы удалить пользовательский источник обновлений, выберите его в списке и нажмите на кнопку **Удалить**.

     Вы не можете удалить единственный пользовательский источник из списка.
6. Нажмите на кнопку **ОК**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Industrial CyberSecurity for Nodes размещает файлы обновлений на локальном диске защищаемого компьютера. Вы можете снизить нагрузку на дисковую подсистему защищаемого компьютера за счет размещения файлов обновлений на виртуальном диске в оперативной памяти при выполнении задачи обновления.

Эта функция доступна для операционных систем Microsoft Windows 7 и выше.

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 защищаемого устройства при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Обновление баз программы**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Оптимизация использования дисковой подсистемы** настройте следующие параметры:
   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

     Флажок включает или выключает оптимизацию 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, используемой для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

     При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

     - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

       В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.
     - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключитсяи задача обновления баз программы будет работать без оптимизации.

       В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.
5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

kaspersky

Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Копирование обновлений**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes" на стр. 942).
5. На закладке **Общие** в разделе **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.

       Этот вариант выбран по умолчанию.
     - **Копировать критические обновления модулей программы**.

       Kaspersky Industrial CyberSecurity for Nodes загружает только срочные обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes.
     - **Копировать обновления баз программы и критические обновления модулей программы**.

       Kaspersky Industrial CyberSecurity for Nodes загружает обновления баз и срочные обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes.
   - Укажите локальную или сетевую папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет копировать полученные обновления.
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

kaspersky

Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Обновление модулей программы**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes" на стр. 942).
5. На закладке **Общие** в разделе **Параметры обновления** настройте параметры обновления модулей программы:
   - **Только проверять наличие доступных критических обновлений модулей программы**

     Kaspersky Industrial CyberSecurity for Nodes отображает уведомление об имеющихся срочных обновлениях программных модулей без загрузки обновлений. Уведомление отображается, если включено оповещение о событиях этого типа.

     Этот вариант выбран по умолчанию.
   - **Копировать и устанавливать критические обновления модулей программы**

     Kaspersky Industrial CyberSecurity for Nodes загружает и устанавливает критические 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**

     Отображаются уведомления обо всех плановых обновлениях программных модулей Kaspersky Industrial CyberSecurity for Nodes, доступных в источнике обновлений. Программа отображает уведомление, если для данного типа событий включены уведомления.

     Если флажок установлен, отображается уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений.

     По умолчанию флажок установлен.
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 425). По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера).

7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 427).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступны критические и плановые обновления*, в котором будет содержаться адрес веб-страницы, откуда можно загрузить плановые обновления.

Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes

Перед обновлением баз Kaspersky Industrial CyberSecurity for Nodes создает резервные копии баз, которые использовались ранее. Если обновление было прервано или завершилось с ошибкой, Kaspersky Industrial CyberSecurity for Nodes автоматически возвращается к использованию ранее установленных баз.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз программы.

► *Чтобы запустить задачу Откат обновления баз программы,*

В панели результатов узла **Откат обновления баз программы** нажмите на ссылку **Запустить**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes создает резервные копии модулей, используемых в текущий момент. Если обновление модулей было прервано или завершилось с ошибкой, Kaspersky Industrial CyberSecurity for Nodes автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте функцию Microsoft Windows **Установка и удаление программ**.

kaspersky

Статистика задач обновления

Во время выполнения задачи обновления вы отображается актуальная информация об объеме данных, загруженных с момента запуска задачи, а также прочая информация о выполнении задачи.

После завершения или остановки задачи эта информация доступна в журнале выполнения задачи.

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

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

Если вы просматриваете задачу Обновление баз программы или Копирование обновлений, в разделе **Статистика** отображается объем данных, загруженных Kaspersky Industrial CyberSecurity for Nodes на текущий момент (**Полученные данные**).

В следующей таблице приведена подробная информация о задаче Обновление модулей программы.

Таблица 130. 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. Название обновления, вызвавшего ошибку, можно посмотреть в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач" на стр. 957).

kaspersky

Запись событий. Журналы Kaspersky Industrial CyberSecurity for Nodes

В этом разделе приведена информация о работе с журналами Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

Способы записи событий Kaspersky Industrial CyberSecurity for Nodes

События Kaspersky Industrial CyberSecurity for Nodes делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Industrial CyberSecurity for Nodes;
- события, связанные с управлением Kaspersky Industrial CyberSecurity for Nodes, например: запуск программы, создание или удаление задач, изменение параметров задач.

Kaspersky Industrial CyberSecurity for Nodes использует следующие способы записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о 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.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Industrial CyberSecurity for Nodes. Журнал событий доступен в "Просмотре событий" Microsoft Windows.
- **Журнал событий безопасности**. Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом компьютере.

Если в работе Kaspersky Industrial CyberSecurity for Nodes возникла проблема (например, Kaspersky Industrial CyberSecurity for Nodes или отдельная задача завершилась аварийно или не запустилась), то для ее диагностики можно создать файл трассировки и файл дампа процессов Kaspersky Industrial CyberSecurity for Nodes и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

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

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Файлы, доступные для загрузки по следующим ссылкам, содержат таблицы с полными списками событий Kaspersky Industrial CyberSecurity for Nodes следующих категорий:

- События, которые Kaspersky Industrial CyberSecurity for Nodes записывает в журнал событий.

  https://support.kaspersky.com/KICS4Nodes/3.2/ru-RU/KICS-WEL-EVENTS.zip

- События, которые Kaspersky Industrial CyberSecurity for Nodes отправляет на Сервер администрирования.

  https://support.kaspersky.com/KICS4Nodes/3.2/ru-RU/KICS-KSC-EVENTS.zip

Настройка параметров журналов с помощью Консоли программы

Вы можете настраивать следующие параметры журналов Kaspersky Industrial CyberSecurity for Nodes:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Industrial CyberSecurity for Nodes сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*;
- события, которые Kaspersky Industrial CyberSecurity for Nodes сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий";
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

► *Чтобы настроить параметры журналов с помощью Консоли программы:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На вкладке **Общие**, если требуется, выберите события, которые Kaspersky Industrial CyberSecurity for Nodes сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий":

   a. В списке **Компонент** выберите компонент Kaspersky Industrial CyberSecurity for Nodes, уровень детализации событий которого вы хотите указать.

   b. В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.

      В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

   c. Если вы хотите вручную включить запись отдельных событий для выбранного компонента или задачи:

      i. В списке **Уровень важности** выберите **Другой**.

      ii. 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.

3. На вкладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий для состояния защиты устройства:

   - В блоке **Хранение журналов**:

     - **Папка с журналами**;

       Путь к папке с журналами в формате UNC (Universal Naming Convention).

       По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Reports\.

       Если используемый по умолчанию путь изменился, создается папка с соответствующим именем. Новые файлы журналов будут сохранены в новую папку. Созданные ранее файлы журналов останутся в старой папке.

     - **Удалять события в журналах выполнения задач старше, чем (сут)**;

       Флажок включает или выключает функцию, которая удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени.

       По умолчанию флажок установлен.

     - **Удалять события в журнале системного аудита старше, чем (сут)**.

       Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

       По умолчанию флажок снят.

- В блоке **Пороги формирования** укажите количество дней, по истечении которого будут регистрироваться события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.

Таблица 131. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих типов: *Базы программы устарели* и *Базы программы сильно устарели*. События возникают, если базы Kaspersky Industrial CyberSecurity for Nodes не обновляются в течение указанного параметром количества дней с момента выпуска последних установленных обновлений баз. Вы можете настроить уведомление администратора об этих событиях. *Проверка важных областей защищаемого устройства 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.

4. На вкладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере (см. раздел "Настройка параметров интеграции с SIEM" на стр. 960).
5. Нажмите на кнопку **OK**, чтобы сохранить изменения.

В этом разделе

Журнал системного аудита

Kaspersky Industrial CyberSecurity for Nodes ведет системный аудит событий, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Industrial CyberSecurity for Nodes, 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 программы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 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 которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

В этом разделе

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 программы 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 условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы 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 вы хотите отфильтровать события.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:
   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий 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 выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы 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 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 программы 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.

kaspersky

Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Industrial CyberSecurity for Nodes и инструкции по работе с ними.

В этом разделе

О журналах выполнения задач

Информация о выполнении задач Kaspersky Industrial CyberSecurity for Nodes отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи можно просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи, а также параметры задачи.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 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 сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Можно также выбрать события, записи о которых Kaspersky Industrial CyberSecurity for Nodes сохраняет в журналах выполнения задач.

Сортировка журналов выполнения задач

По умолчанию журналу выполнения задач отображаются в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы 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 журналы выполнения задач Kaspersky Industrial CyberSecurity for Nodes.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация журналов выполнения задач

Вы можете настроить отображение в списке журналов выполнения задач только журналы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

► *Чтобы отфильтровать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы 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 вы хотите отфильтровать журналы выполнения задач.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации в списке журналов выполнения задач.

В списке журналов выполнения задач отобразятся только журналы, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке журналов выполнения задач отобразятся все журналы.

Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. В дереве Консоли программы 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 его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
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 во время выполнения 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 программы 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 его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
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 журналов выполнения задач

По умолчанию Kaspersky Industrial CyberSecurity for Nodes хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Можно вручную удалить журналы выполнения завершившихся задач.

> События из журналов задач, выполняющихся в данный момент, и задач, используемых другими пользователями, удалены не будут.

► *Чтобы удалить журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Чтобы удалить журналы выполнения всех завершившихся задач, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Чтобы очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню журнала, который вы хотите очистить, и выберите пункт **Удалить**.
   - Чтобы очистить журналы выполнения нескольких задач, выполните следующие действия:
     a. В панели результатов с помощью клавиш **CTRL** и **SHIFT** выберите журналы выполнения задач, которые вы хотите очистить.
     b. Откройте контекстное меню любого журнала выполнения задач и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление журналов.

Выбранные журналы выполнения задач будут очищены. Удаление журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал безопасности

Kaspersky Industrial CyberSecurity for Nodes 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. При очистке журнала безопасности Kaspersky Industrial CyberSecurity for Nodes регистрирует событие системного аудита.

kaspersky

Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он хранит и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  > Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Industrial CyberSecurity for Nodes может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

Параметры надежности

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Также Kaspersky Industrial CyberSecurity for Nodes использует события системного аудита для уведомления о неудачных попытках подключения к SIEM-серверу и об ошибках отправки событий на SIEM-сервер.

Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Таблица 132. 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 на SIEM-сервер, установив или сняв флажок.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.
Протокол подключения	TCP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UDP 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 дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.
3. Выберите вкладку **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 на SIEM-сервер 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 выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

   Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

   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 программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В блоке **Параметры подключения**:

   - Укажите протокол подключения к SIEM.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к основному syslog-серверу.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к дополнительному syslog-серверу.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

Просмотр журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий"

С помощью оснастки "Просмотр событий" в Microsoft Management Console можно просматривать журнал событий Kaspersky Industrial CyberSecurity for Nodes. В журнале содержатся события, зарегистрированные Kaspersky Industrial CyberSecurity for Nodes и необходимые для диагностики сбоев в работе программы.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий**;
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются все события. Наименее подробным является уровень Критические события, при котором регистрируются только критические события.

► *Чтобы просмотреть журнал событий Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется Microsoft Management Console.

2. Выберите **Файл** > **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите защищаемое устройство, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes, и нажмите на кнопку **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**.

Откроется журнал событий Kaspersky Industrial CyberSecurity for Nodes.

kaspersky

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Industrial CyberSecurity for Nodes о событиях программы и о состоянии защиты устройства, а также инструкцию по настройке уведомлений.

В этом разделе

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к устройству, о событиях, связанных с работой Kaspersky Industrial CyberSecurity for Nodes, и о состоянии антивирусной защиты устройства.

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к устройству, и пользователи терминального устройства могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли программы можно активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения пользователей терминального защищаемого компьютера, 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.

     При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого компьютера.

  c. Отправка по электронной почте.

     Этот способ использует для передачи сообщений электронную почту.

Вы можете составить текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

kaspersky

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 программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** выберите способ уведомления:

   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.

   > Уведомление пользователя можно настроить только для следующих событий: **Обнаружен объект**, **Обнаружено и запрещено недоверенное устройство** и **Сетевая сессия добавлена в список недоверенных**.

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 выбора способа уведомлений для одного типа событий, выберите остальные типы событий, для которых вы хотите использовать этот же текст сообщения, с помощью клавиш **CTRL** и **SHIFT**, а затем нажмите 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. Чтобы настроить способы уведомления администраторов о выбранном событии, выберите закладку **Уведомления** и в разделе **Настройка** нажмите на кнопку **Уведомление администраторов**. Затем в окне **Дополнительные параметры** выполните настройку выбранных способов уведомления. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте выберите закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса точкой с запятой), имя или сетевой адрес SMTP-сервера и номер порта. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** можно также добавлять переменные с информацией о событии (см. таблицу ниже).

      Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Использовать SMTP-аутентификацию** установите флажок **Параметры аутентификации** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

b. Для уведомлений средствами службы сообщений Windows составьте список защищаемых устройств, получающих уведомления, на закладке **Служба сообщений**: для каждого защищаемого устройства, которое 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 файл на локальном диске защищаемого компьютера или введите полный путь к нему. Этот файл будет выполняться на защищаемом компьютере при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

   Если вы хотите ограничить количество уведомлений о событиях одного типа за период времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите количество экземпляров и период времени.

5. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Таблица 133. Поля с информацией о событии

Переменная	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты компьютера и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя объекта согласно классификации Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач" на стр. 957).
%VIRUS_TYPE%	Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%USER_COMPUTER%	В задачах Постоянная защита файлов имя защищаемого устройства пользователя, который обратился к объекту на устройстве.
%USER_NAME%	В задачах Постоянная защита файлов имя пользователя, который обратился к объекту на устройстве.
%FROM_COMPUTER%	Имя защищаемого компьютера, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (только для события "внутренняя ошибка задачи").
%TASK_NAME%	Название задачи (имеется только у событий, связанных с выполнением задач).

Настройка параметров журналов и уведомлений с помощью Плагина управления

В Консоли администрирования Kaspersky Security Center можно настроить уведомление администратора и пользователей о следующих событиях в работе Kaspersky Industrial CyberSecurity for Nodes и с состоянием антивирусной защиты устройства:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому устройству, и пользователи терминального защищаемого устройства могут получать информацию о событиях *Обнаружен объект*.

Можно настроить уведомления о событиях Kaspersky Industrial CyberSecurity for Nodes как для отдельного защищаемого устройства в окне **Свойства: <Имя защищаемого устройства>** выбранного защищаемого устройства, так и для группы защищаемых устройств в окне **Свойства: <Имя политики>** выбранной группы администрирования.

На закладке **Уведомления о событиях** или в окне **Настройка уведомлений** можно настроить следующие типы уведомлений:

- На закладке **Уведомления о событиях** (стандартная закладка в Kaspersky Security Center) можно настроить уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений приведена в *Справке Kaspersky Security Center*.
- В окне **Настройка уведомлений** можно настроить уведомления как администратора, так и пользователей.

Уведомления о событиях некоторых типов можно настраивать только на закладке или только в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите уведомления о событиях одного типа в одинаковом режиме на закладке **Уведомления о событиях** и в окне **Настройка уведомлений**, системный администратор будет получать уведомления об этих событиях дважды.

В этом разделе

Настройка параметров журналов задач

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры журналов для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры журналов для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Журналы и уведомления** в блоке **Журналы выполнения задач** нажмите на кнопку **Настройка**.
5. Откроется окно **Параметры журналов** на вкладке **Журналы**.
6. Настройте уровень детализации событий в журналах:
   a. В списке **Компонент** выберите компонент Kaspersky Industrial CyberSecurity for Nodes, уровень детализации событий которого вы хотите указать.
   b. В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.

      В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.
   c. Если вы хотите вручную включить запись отдельных событий для выбранного компонента или задачи:
      i. В списке **Уровень важности** выберите **Другой**.
      ii. 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.
7. В блоке **Хранение журналов** настройте параметры хранения журналов:
   - **Папка с журналами**;

     Путь к папке с журналами в формате UNC (Universal Naming Convention).

     По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Reports\.

     Если используемый по умолчанию путь изменился, создается папка с соответствующим именем. Новые файлы журналов будут сохранены в новую папку. Созданные ранее файлы журналов останутся в старой папке.

- **Удалять события в журналах выполнения задач старше, чем (сут)**;

  Флажок включает или выключает функцию, которая удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени.

  По умолчанию флажок установлен.

- **Удалять события в журнале системного аудита старше, чем (сут)**.

  Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

  По умолчанию флажок снят.

8. На вкладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере (см. раздел "Настройка параметров интеграции с SIEM" на стр. 970).
9. Нажмите на кнопку **OK**.

Настроенные параметры журналов будут сохранены.

Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он хранит и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  > Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Industrial CyberSecurity for Nodes может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Таблица 134. 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 на SIEM-сервер, установив или сняв флажок.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.
Протокол подключения	TCP	С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам UDP или TCP, к дополнительному syslog-серверу по протоколу TCP.
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.

Параметр	Значение по умолчанию	Описание
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 дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры журналов для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры журналов для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Журналы и уведомления** в блоке **Настройка** нажмите на кнопку **Журналы выполнения задач**.

   Откроется окно **Параметры журналов и уведомлений**.
5. Выберите вкладку **Интеграция с SIEM**.
6. 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 на SIEM-сервер 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.

7. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Флажок включает или выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

   Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

   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.

8. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

9. В блоке **Параметры подключения**:

   - Укажите протокол подключения к SIEM.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к основному syslog-серверу.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к дополнительному syslog-серверу.

10. Нажмите на кнопку **OK**.

Настроенные параметры интеграции с SIEM будут применены.

Настройка параметров уведомлений

► *Чтобы настроить уведомления Kaspersky Industrial CyberSecurity for Nodes:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

4. В разделе **Журналы и уведомления** в подразделе **Настройка** нажмите на кнопку **Уведомления о событиях**.
5. В окне **Настройка уведомлений** настройте следующие параметры Kaspersky Industrial CyberSecurity for Nodes согласно вашим требованиям:

   - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.
   - В разделе **Уведомление пользователей** настройте способ уведомления пользователей. Если требуется, задайте текст уведомления.
   - В разделе **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
   - В разделе **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Industrial CyberSecurity for Nodes регистрирует события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.

     - **Базы программы устарели (сут);**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 7 дней.

     - **Базы программы сильно устарели (сут);**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 14 дней.

     - **Проверка важных областей защищаемого устройства давно не выполнялась (сут).**

       Количество дней с момента последнего успешного завершения задачи Проверка важных областей.

       По умолчанию установлено 30 дней.

6. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

kaspersky

Настройка формирования инцидентов и взаимодействия с Сервером администрирования

► *Чтобы выбрать типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Журналы и уведомления** в подразделе **Настройка** нажмите на кнопку **Взаимодействие с Сервером администрирования**.

   Откроется окно **Взаимодействие с Сервером администрирования**.
5. В окне **Взаимодействие с Сервером администрирования** выберите типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования Kaspersky Security Center:
   - Данные об объектах карантина.
   - Данные об объектах резервного хранилища.
   - Данные о доступных для подключения сетях Wi-Fi.
   - Данные о заблокированных сеансах (приведены в разделе "Необработанные объекты" на стороне KSC).
   - Данные о версиях проектов ПЛК.

   Чтобы настроить параметры задачи Контроль Wi-Fi для группы защищаемых компьютеров с помощью политики Kaspersky Security Center, включите отправку данных о доступных сетях Wi-Fi на Сервер администрирования.
6. Нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes будет передавать информацию о выбранных типах объектов на Сервер администрирования.

Формирование инцидентов

В базе данных Сервера администрирования хранится информация о событиях программы, произошедших на управляемых защищаемых компьютерах.

► *Чтобы настроить уведомления, на основании которых Kaspersky Industrial CyberSecurity for Nodes будет формировать инциденты в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Журналы и уведомления** в подразделе **Настройка** нажмите на кнопку **Инциденты**.

   Откроется окно **Инциденты**.
5. В окне **Инциденты** измените выборку событий в таблице ниже, на основании которых Kaspersky Industrial CyberSecurity for Nodes будет формировать инциденты:

Таблица 135. Список событий для формирования инцидентов

Событие	Значение по умолчанию
Проект ПЛК не соответствует эталонному	Выбрано.
Не удалось сравнить проект ПЛК с эталонным	Выбрано.
Не удалось получить данные о проекте ПЛК	Выбрано.
Срок действия лицензии истек	Не выбрано
нарушение Лицензионного соглашения	Выбрано.
Не обновлено	Не выбрано
Базы программы повреждены	Не выбрано
Базы программы сильно устарели	Не выбрано
Базы программы устарели	Не выбрано
Целостность модулей программы нарушена	Выбрано.
Сетевая сессия добавлена в список недоверенных	Выбрано.
Запуск программы запрещен	Не выбрано

Событие	Значение по умолчанию
Режим Только статистика: запуск программы запрещен	Выбрано.
Запуск программы не обработан	Не выбрано
Подключение устройства не обработано	Выбрано.
Только статистика: обнаружено недоверенное устройство	Не выбрано
Обнаружено и запрещено недоверенное устройство	Выбрано.
Только статистика: Обнаружено недоверенное внешнее устройство	Выбрано.
Обнаружен зараженный объект или объект другого типа	Не выбрано
Обнаружен объект, недоверенный в KSN	Выбрано.
Обнаружен возможно зараженный объект	Выбрано.
Объект не вылечен	Не выбрано
Объект не помещен в резервное хранилище	Не выбрано
Объект не помещен на карантин	Не выбрано

6. Нажмите на кнопку **ОК** в окне **Параметры программы**.

   Параметры формирования инцидентов будут сохранены.

kaspersky

Механизмы самозащиты Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Industrial CyberSecurity for Nodes.

В этом разделе

О механизмах самозащиты Kaspersky Industrial CyberSecurity for Nodes

В Kaspersky Industrial CyberSecurity for Nodes реализованы механизмы самозащиты, обеспечивающие защиту от изменения или удаления папок программы, процессов памяти и записей системного реестра.

Защита от изменений папок с установленными компонентами Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запрещает всем пользователям переименовывать и удалять папки с установленными компонентами программы. По умолчанию используются следующие пути к папкам установки программы:

- В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\
- В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\

Защита от изменений ключей реестра Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к следующим ключам и ветвям реестра, обеспечивающим загрузку драйверов и служб программы:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\3.2\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\3.2] (в Microsoft Windows 64-разрядной версии)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\3.2\Trace]

Права на изменение этих ветвей и ключей реестра имеют только пользователи с учетной записью Локальная система (SYSTEM). Пользователи с учетными записями Пользователь и Администратор имеют права только на чтение.

Защита от изменений в памяти служебных компонентов программы

Для защиты служебных компонентов программы от сторонних процессов драйверы Kaspersky Industrial CyberSecurity for Nodes ограничивают доступ к следующим исполняемым файлам:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

По умолчанию доступ к памяти служебных компонентов Kaspersky Industrial CyberSecurity for Nodes ограничен для сторонних процессов.

Функции самозащиты можно включить в свойствах политики Консоли Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 416) и Плагина управления Kaspersky Industrial CyberSecurity for Nodes (см. раздел "Настройка параметров безопасности в Kaspersky Security Center" на стр. 370).

kaspersky

Регистрация службы Kaspersky Security как защищенной службы

Технология *Protected Process Light* (PPL) гарантирует, что операционная система выполняет загрузку только доверенных служб и процессов. Для того чтобы запустить службу как защищенную, на устройстве должен быть установлен драйвер *Early Launch Antimalware*.

Драйвер *Early Launch Antimalware* (далее "драйвер ELAM") обеспечивает защиту устройств в сети при их включении и при инициализации драйверов сторонних производителей.

Драйвер ELAM устанавливается автоматически во время установки Kaspersky Industrial CyberSecurity for Nodes и используется для регистрации службы Kaspersky Security как защищенной во время запуска операционной системы. Когда служба Kaspersky Security (KAVFS) запускается как системный защищенный процесс, другие незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищенного процесса и останавливать службу.

При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM возможна в операционной системе Microsoft Windows Server 2016 RS3 сборка 16299 и более поздних версий. Если программа Kaspersky Industrial CyberSecurity for Nodes установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

► *Чтобы установить Kaspersky Industrial CyberSecurity for Nodes как защищенный процесс, выполните следующую команду:*

```
msiexec /i kics_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Управление правами доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

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

В этом разделе

kaspersky

О правах на управление Kaspersky Industrial CyberSecurity for Nodes

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

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

Пользователи, не зарегистрированные в списке пользователей Kaspersky Industrial CyberSecurity for Nodes, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа:

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

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

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

Таблица 136. Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Industrial CyberSecurity for Nodes.
Создание и удаление задач проверки по требованию	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes. • Редактировать настройки программы.

Права доступа	Описание
Чтение параметров	Возможности: • просматривать общие параметры Kaspersky Industrial CyberSecurity for Nodes и параметры задач; • экспортировать в конфигурационный файл параметры Kaspersky Industrial CyberSecurity for Nodes; • Просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • Помещать объекты на карантин. • Удалять объекты из карантина и резервного хранилища. • Восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Industrial CyberSecurity for Nodes.
Лицензирование программы	Возможность активировать Kaspersky Industrial CyberSecurity for Nodes.
Чтение прав	Возможность просматривать список и права доступа пользователей Kaspersky Industrial CyberSecurity for Nodes.
Изменение прав	Возможности: • Изменять список пользователей, имеющих доступ к управлению программой. • изменять права доступа пользователей к функциям Kaspersky Industrial CyberSecurity for Nodes.

О правах на управление регистрируемыми службами

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

Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Если программа Kaspersky Industrial CyberSecurity for Nodes установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

kaspersky

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, имеющие доступ уровня Изменение прав (см. раздел "Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля" на стр. 992), могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Служба Kaspersky Security Management

Для управления программой через Консоль программы, установленную на другом защищаемом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Industrial CyberSecurity for Nodes, 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.

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

Служба Kaspersky Security Exploit Prevention

По умолчанию доступ к управлению службой Kaspersky Security Exploit Prevention имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, а также в группу SYSTEM с правами на чтение и исполнение.

О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Industrial CyberSecurity for Nodes.

При установке Kaspersky Industrial CyberSecurity for Nodes регистрирует службу Kaspersky Security Management (KAVFSGT). Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, используемая для подключения к Kaspersky Industrial CyberSecurity for Nodes, 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, KICS Administrators созданной на защищаемом компьютере при установке Kaspersky Industrial CyberSecurity for Nodes.

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

Вы не можете разрешать или запрещать пользователям доступ к службе Kaspersky Security Management, настраивая параметры Kaspersky Industrial CyberSecurity for Nodes.

Вы можете подключиться к Kaspersky Industrial CyberSecurity for Nodes с локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с такими же именем пользователя и паролем.

kaspersky

О правах на управление службой Kaspersky Security

При установке Kaspersky Industrial CyberSecurity for Nodes регистрирует в Windows службу Kaspersky Security (KAVFS), так как программа включает в себя функциональные компоненты, запускаемые при старте операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности защищаемого компьютера через управление службой Kaspersky Security, вы можете ограничить права на управление службой Kaspersky Security с помощью Консоли программы или Плагина управления.

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.

Нельзя удалить или изменять права для учетной записи SYSTEM. Если права учетной записи SYSTEM были изменены, при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ к функциям уровня Изменение прав, могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Industrial CyberSecurity for Nodes один из следующих стандартных уровней доступа для управления службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security, а также запускать и останавливать службу Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security.
- **Исполнение** – возможность запускать и останавливать службу Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Industrial CyberSecurity for Nodes (см. таблицу ниже).

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

Таблица 137. Разграничение прав доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

Функция	Описание
Просмотр параметров службы	Возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения службы Kaspersky Security у Диспетчера управления службами Microsoft Windows.
Запрос статуса у службы	Возможность запрашивать статус службы у службы Kaspersky Security.
Перечисление зависимых служб	Возможность просматривать список служб, от которых зависит служба Kaspersky Security, а также служб, зависимых от службы Kaspersky Security.
Изменение параметров службы	Возможность просматривать и изменять общие параметры работы и права пользователей для служб Kaspersky Security.
Запуск службы	Возможность запускать выполнение службы Kaspersky Security.
Остановка службы	Возможность останавливать выполнение службы Kaspersky Security.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение службы Kaspersky Security.
Чтение прав	Возможность просматривать список пользователей службы Kaspersky Security и права доступа каждого пользователя.
Изменение прав	Возможности: • добавлять и удалять пользователей службы Kaspersky Security; • изменять права доступа пользователей к службе Kaspersky Security.
Удаление службы	Возможность отмены регистрации службы Kaspersky Security в диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.

Управление правами доступа с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка прав доступа для одного или всех защищаемых устройств сети.

В этом разделе

kaspersky

Настройка прав доступа к Kaspersky Industrial CyberSecurity for Nodes и службе Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Industrial CyberSecurity for Nodes и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).
4. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Industrial CyberSecurity for Nodes 3.2**.
5. 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**.
6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых компьютеров, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 385).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого компьютера, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 389).

4. В разделе **Дополнительные возможности** выполните одно из следующих действий:

   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Industrial CyberSecurity for Nodes**.

5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.

6. В разделе **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:

   - **Полный контроль**: полный набор прав на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Security.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Industrial CyberSecurity for Nodes: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Права на чтение**.
     - Следующие права на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Права на чтение**.
   - **Изменение**:
     - Все права на управление Kaspersky Industrial CyberSecurity for Nodes, кроме **Права на изменение**.
     - Следующие права на управление службой Kaspersky Security: **Настройка параметров службы**, **Права на чтение**.
   - **Особые разрешения**: следующие права на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Права на чтение**, **Пользовательские запросы к KAVFS**.

7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.

   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Industrial CyberSecurity for Nodes** 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 выбранной группе.

e. Нажмите на кнопку **OK**.

f. В окне **Дополнительные параметры безопасности для службы Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **OK**.

8. В окне **Разрешения для службы Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **Применить**.

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

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

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- изменение компонентов Kaspersky Industrial CyberSecurity for Nodes;
- выполнение команд командной строки.

Интерфейс Kaspersky Industrial CyberSecurity for Nodes скрывает вводимый пароль на экране. Kaspersky Industrial CyberSecurity for Nodes хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Industrial CyberSecurity for Nodes не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Выберите группу администрирования, содержащую защищаемые компьютеры, для которых вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры политики для группы защищаемых компьютеров, выберите закладку **Политики** и с помощью контекстного меню перейдите к свойствам **<Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого компьютера, откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 389) в Kaspersky Security Center.
3. На закладке **Безопасность и надежность** в разделе **Параметры программы** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В разделе **Самозащита** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Industrial CyberSecurity for Nodes будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

kaspersky

Управление правами доступа с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка прав доступа для защищаемого устройства.

В этом разделе

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

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 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 программы 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.
   - 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 Kaspersky Industrial CyberSecurity for Nodes**.
2. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу и нажмите на кнопку **Удалить**.
3. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:*

1. В дереве Консоли программы 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.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите настроить права доступа к службе Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Industrial CyberSecurity for Nodes**.
2. В открывшемся окне в списке **Имена групп и пользователей** 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:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Industrial CyberSecurity for Nodes**.
4. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
5. В разделе **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Industrial CyberSecurity for Nodes или службой Kaspersky Security.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Industrial CyberSecurity for Nodes: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Права на чтение**.
     - Следующие права на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Права на чтение**.
   - **Изменение**:
     - Все права на управление Kaspersky Industrial CyberSecurity for Nodes, кроме **Права на изменение**.
     - Следующие права на управление службой Kaspersky Security: **Настройка параметров службы**, **Права на чтение**.
   - **Особые разрешения**: следующие права на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Права на чтение**, **Пользовательские запросы к KAVFS**.

6. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Industrial CyberSecurity for Nodes** 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 выбранной группе.
   e. Нажмите на кнопку **ОК**.
   f. В окне **Дополнительные параметры безопасности для службы Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **ОК**.
7. В окне **Разрешения для службы Kaspersky Industrial CyberSecurity for Nodes** нажмите на кнопку **Применить**.

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

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

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- изменение компонентов Kaspersky Industrial CyberSecurity for Nodes;
- выполнение команд командной строки.

Интерфейс Kaspersky Industrial CyberSecurity for Nodes скрывает вводимый пароль на экране. Kaspersky Industrial CyberSecurity for Nodes хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Industrial CyberSecurity for Nodes не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);

- цифры (0-9);
- символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

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

1. В дереве Консоли программы 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 разделе **Самозащита** установите флажок **Использовать защиту паролем**.

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

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

Управление правами доступа с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка прав доступа для защищаемых устройств сети.

В этом разделе

Настройка прав доступа к Kaspersky Industrial CyberSecurity for Nodes и службе Kaspersky Security

Чтобы настроить права доступа для пользователя или группы, необходимо указать строку дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL). Дополнительная информация о строке дескриптора безопасности приведена на веб-сайте Microsoft.

► *Чтобы настроить права доступа для пользователя или группы, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства → Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Выполните одно из следующих действий:
   - Нажмите на кнопку **Параметры** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes.
   - Нажмите на кнопку **Параметры** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.
6. Добавьте пользователя или группу, указав строку дескриптора безопасности в окне **Права пользователей на управление программой** или **Права пользователей на управление службой Kaspersky Security Service**.
7. Нажмите на кнопку **OK**.

kaspersky

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

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Industrial CyberSecurity for Nodes запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- изменение компонентов Kaspersky Industrial CyberSecurity for Nodes;
- выполнение команд командной строки.

Интерфейс Kaspersky Industrial CyberSecurity for Nodes скрывает вводимый пароль на экране. Kaspersky Industrial CyberSecurity for Nodes хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Industrial CyberSecurity for Nodes не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.

3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. В разделе **Безопасность и надежность** нажмите на кнопку **Параметры**.
6. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.
7. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Industrial CyberSecurity for Nodes будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

kaspersky

Работа с Kaspersky Industrial CyberSecurity for Nodes из командной строки

Этот раздел содержит описание работы с Kaspersky Industrial CyberSecurity for Nodes из командной строки.

В этом разделе

Команды

Вы можете выполнять основные команды управления Kaspersky Industrial CyberSecurity for Nodes из командной строки защищаемого компьютера с помощью компонента Утилита командной строки, входящего в группу программных компонентов Kaspersky Industrial CyberSecurity for Nodes.

С помощью командной строки можно управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Industrial CyberSecurity for Nodes.

Некоторые из команд Kaspersky Industrial CyberSecurity for Nodes выполняются в следующих режимах:

- Синхронный режим: управление возвращается на Консоль только после завершения выполнения команды.
- Асинхронный режим: управление возвращается на Консоль сразу после запуска команды.

► *Чтобы прервать выполнение команды в синхронном режиме,*

нажмите комбинацию клавиш **CTRL+C**.

При вводе команд Kaspersky Industrial CyberSecurity for Nodes применяйте следующие правила:

- Вводите ключи и команды символами верхнего или нижнего регистра.
- Разделяйте ключи символом пробела.
- Если имя файла или папки содержит пробел, заключите путь к файлу или папке в кавычки, например: `"C:\TEST\test cpp.exe"`.
- При необходимости можно использовать подстановочные символы в масках имен файлов или путей, например: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

С помощью командной строки можно выполнять все операции по управлению и администрированию Kaspersky Industrial CyberSecurity for Nodes (см. таблицу ниже).

Таблица 138. Команды Kaspersky Industrial CyberSecurity for Nodes

Команда	Описание
KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL" на стр. 1013)	Обновляет список правил в соответствии с выбранным правилом импорта.
KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачей Контроль запуска программ: KAVSHELL APPCONTROL /CONFIG" на стр. 1010)	Задает режим работы задачи Контроль запуска программ.
KAVSHELL APPCONTROL /GENERATE (см. раздел "Формирование правил контроля запуска программ: KAVSHELL APPCONTROL /GENERATE" на стр. 1011)	Запускает задачу Формирование правил контроля запуска программ.
KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала Kaspersky Industrial CyberSecurity for Nodes. KAVSHELL VACUUM" на стр. 1024)	Дефрагментирует файлы журналов Kaspersky Industrial CyberSecurity for Nodes.
KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Industrial CyberSecurity for Nodes. KAVSHELL HELP" на стр. 1000)	Отображает справку о командах Kaspersky Industrial CyberSecurity for Nodes.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP" на стр. 1001)	Запускает службу Kaspersky Security.
KAVSHELL STOP (см. раздел "Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP" на стр. 1001)	Останавливает службу Kaspersky Security.
KAVSHELL SCAN (см. раздел "Проверка указанной области: KAVSHELL SCAN" на стр. 1001)	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами командной строки.

Команда	Описание
KAVSHELL SCANCRITICAL (см. раздел "Запуск задачи Проверка важных областей: KAVSHELL SCANCRITICAL" на стр. 1005)	Запускает локальную системную задачу Проверка важных областей.
KAVSHELL TASK (см. раздел "Управление задачей в асинхронном режиме: KAVSHELL TASK" на стр. 1006)	Запускает, приостанавливает, возобновляет, останавливает указанную задачу в асинхронном режиме. Возвращает текущее состояние задачи / статистику задачи.
KAVSHELL RTP (см. раздел "Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP" на стр. 1009)	Запускает или останавливает все задачи постоянной защиты компьютера.
KAVSHELL UPDATE (см. раздел "Запуск задачи Обновление баз программы: KAVSHELL UPDATE" на стр. 1015)	Запускает задачу Обновление баз программы с параметрами, заданными ключами командной строки.
KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes: KAVSHELL ROLLBACK" на стр. 1019)	Откатывает базы программы до предыдущей версии.
KAVSHELL LICENSE (см. раздел "Активация программы. KAVSHELL LICENSE" на стр. 1020)	Добавляет или удаляет ключи. Отображает информацию о добавленных ключах.
KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE" на стр. 1021)	Включает или выключает трассировку. Управляет параметрами трассировки.
KAVSHELL DUMP (см. раздел "Включение и выключение создания файла дампа. KAVSHELL DUMP" на стр. 1025)	Включает и выключает создание файлов дампов процессов Kaspersky Industrial CyberSecurity for Nodes при их аварийном завершении.
KAVSHELL IMPORT (см. раздел "Импорт параметров. KAVSHELL IMPORT" на стр. 1027)	Импортирует общие параметры Kaspersky Industrial CyberSecurity for Nodes, а также параметры функций и задач из конфигурационного файла.

Команда	Описание
KAVSHELL EXPORT (см. раздел "Экспорт параметров. KAVSHELL EXPORT" на стр. 1027)	Экспортирует все параметры Kaspersky Industrial CyberSecurity for Nodes и существующих задач в конфигурационный файл.
KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL" на стр. 1014)	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

Вызов справки о командах Kaspersky Industrial CyberSecurity for Nodes. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Industrial CyberSecurity for Nodes, выполните одну из следующих команд:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Чтобы получить описание команды и ее синтаксис, выполните одну из следующих команд:

```
KAVSHELL HELP <команда>

KAVSHELL <команда> /?
```

Примеры команды KAVSHELL HELP

Чтобы просмотреть подробную информацию о команде KAVSHELL SCAN, выполните следующую команду:

```
KAVSHELL HELP SCAN
```

Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP

Чтобы запустить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускается Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Проверка указанной области: KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого компьютера, используйте команду `KAVSHELL SCAN`. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная с помощью команды `KAVSHELL SCAN`, является временной. Она отображается в Консоли программы только во время выполнения (в Консоли программы не отображаются ее параметры). Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи.

При указании путей в задачах проверки отдельных областей можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду `KAVSHELL SCAN` с правами этого пользователя.

Команда `KAVSHELL SCAN` выполняется в синхронном режиме.

Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду KAVSHELL TASK (см. раздел "Управление задачей в асинхронном режиме: KAVSHELL TASK" на стр. 1006).

Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<путь к файлу со
списком областей проверки>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"маски">] [/ES:<размер>] [/ET:<количество секунд>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<дни>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<путь к файлу
журнала выполнения задачи>] [/ANSI] [/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL SCAN есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

Пример команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\
C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED
/AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info"
/NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Таблица 139. Ключи / параметры команды KAVSHELL SCAN

Ключ / параметр	Описание
Область проверки. Обязательный параметр.	
<файлы>	Область проверки – список файлов, папок, сетевых путей и стандартных областей. Указывайте сетевые пути к формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней. Это значит, что она находится в папке, из которой вы запускаете команду KAVSHELL. KAVSHELL SCAN Folder4 Если имя объекта, который вы хотите проверить, содержит пробелы, заключайте его в кавычки. Kaspersky Industrial CyberSecurity for Nodes проверит также все вложенные папки в выбранной папке. Для проверки группы файлов вы можете использовать символы * или ?.
<папки>	
<сетевой путь>	
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на защищаемом компьютере.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.

Ключ / параметр	Описание
/MYCOMP	Проверять все области защищаемого компьютера.
/L: <путь к файлу со списком областей проверки>	Полный путь к файлу со списком областей проверки. Разделяйте области проверки в файле символом перевода строки. Вы можете указывать стандартные области проверки, как показано в следующем примере файла со списком областей проверки: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Проверка объектов (типы файлов). Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Industrial CyberSecurity for Nodes проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Industrial CyberSecurity for Nodes проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	Проверять только новые и измененные файлы. Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes будет проверять все объекты.
Действия над зараженными и другими обнаруженными объектами. Если вы не зададите никаких значений этого ключа, Kaspersky Industrial CyberSecurity for Nodes будет выполнять действие **Пропускать**.	
DISINFECT	Лечить; если лечение невозможно, пропускать Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Industrial CyberSecurity for Nodes для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Industrial CyberSecurity for Nodes не будет обрабатывать возможно зараженные объекты.
DISINFDEL	Лечить; если лечение невозможно, удалять
DELETE	Удалять Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Industrial CyberSecurity for Nodes для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Industrial CyberSecurity for Nodes не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие

Ключ / параметр	Описание
/AS: **Действия над возможно зараженными объектами** Если вы не укажете этот параметр, Kaspersky Industrial CyberSecurity for Nodes будет выполнять действие **Пропускать**.	
QUARANTINE	Карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
Исключения	
/E:ABMSPO	Исключать составные объекты следующих типов: A – SFX-архивы; B – почтовые базы; M – файлы почтовых форматов; S – архивы (включая SFX-архивы); P – упакованные объекты; O – вложенные OLE-объекты.
/EM:<"маски">	Исключать файлы по маске Вы можете задать несколько масок, например: `EM:"*.txt; *.png; C\Videos\*.avi"`.
/ET:<количество секунд>	Прекращать обработку объекта, если она продолжается дольше указанного количества секунд. По умолчанию ограничений продолжительности нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанное значение. По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет объекты любого размера.
/TZOFF	Отменить исключения доверенной зоны.
Дополнительные параметры (опции)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ANALYZERLEVEL:<уровень эвристического анализа>	Включить использование эвристического анализатора, настроить уровень анализа. Доступны следующие уровни эвристического анализа: 1 – поверхностный; 2 – средний; 3 – глубокий. Если вы опустите этот параметр, Kaspersky Industrial CyberSecurity for Nodes не будет использовать эвристический анализатор.

Ключ / параметр	Описание
/ALIAS:<альтернативное название задачи>	Присваивает задаче проверки по требованию временное название, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Industrial CyberSecurity for Nodes. Если этот параметр не задан, задаче присваивается временное название вида scan_<kavshell_pid>, например, scan_1234. В Консоли программы задаче присваивается название "Проверка объектов <дата и время>", например, "Проверка объектов 16.08.2007 17:13:14".
Параметры журнала выполнения задачи	
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Industrial CyberSecurity for Nodes сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли программы. Если Kaspersky Industrial CyberSecurity for Nodes не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.
/ANSI	Этот параметр позволяет записывать события в журнал выполнения задачи в кодировке ANSI. Параметр ANSI не будет применяться, если не задан параметр W. Если параметр ANSI не указан, то журнал выполнения задачи формируется в кодировке UNICODE.

Запуск задачи Проверка важных областей: KAVSHELL SCANCRITICAL

Используйте команду `KAVSHELL SCANCRITICAL`, чтобы запустить задачу Проверка важных областей с параметрами, заданными в Консоли программы.

Синтаксис команды KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<имя файла журнала выполнения задачи>]
```

Примеры команды KAVSHELL SCANCRITICAL

Чтобы запустить задачу Проверка важных областей и сохранить журнал выполнения задачи в файле с именем scancritical.log в текущей папке, выполните следующую команду:

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

С помощью параметра /W можно настроить местоположение файла журнала выполнения задачи (см. таблицу ниже).

Таблица 140. Синтаксис параметра /W команды KAVSHELL SCANCRITICAL

Ключ / параметр	Описание
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Industrial CyberSecurity for Nodes сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** в Консоли программы. Если Kaspersky Industrial CyberSecurity for Nodes не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.

Управление задачей в асинхронном режиме: KAVSHELL TASK

Команда `KAVSHELL TASK` позволяет управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное название задачи> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS>]
```

Пример команды KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

Команда `KAVSHELL TASK` может быть выполнена как без ключей/параметров, так и с использованием одного либо нескольких ключей/параметров (см. таблицу ниже).

Таблица 141. Ключи / параметры команды KAVSHELL TASK

Ключ / параметр	Описание
Без параметров	Возвращает список всех существующих задач Kaspersky Industrial CyberSecurity for Nodes. Список содержит следующие поля: альтернативное название задачи, категория задачи (системная или пользовательская) и текущий статус задачи.
<альтернативное название задачи>	Вместо названия задачи в команде SCAN TASK используйте ее альтернативное название – дополнительное сокращенное название, которое Kaspersky Industrial CyberSecurity for Nodes присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Industrial CyberSecurity for Nodes, введите команду KAVSHELL TASK без параметров.
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/PAUSE	Приостановить указанную задачу
/RESUME	Возобновить указанную задачу в асинхронном режиме
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*).
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи

Обратите внимание, что не все задачи Kaspersky Industrial CyberSecurity for Nodes поддерживают ключи /PAUSE, /RESUME и /STATE.

Коды возврата команды KAVSHELL TASK (на стр. 1034).

kaspersky

Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG

Команда `KAVSHELL CONFIG` позволяет удалить атрибут защищенного процесса (Protected Process Light) у службы Kaspersky Security с помощью драйвера ELAM, установленного во время установки программы.

Синтаксис команды KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

Таблица 142. Ключи / параметры команды KAVSHELL CONFIG

Ключ / параметр	Описание
/PPL:OFF	Снять атрибут PPL со службы Kaspersky Security.

Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP

Команда `KAVSHELL RTP` позволяет запустить или остановить все задачи постоянной защиты компьютера.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Пример команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты компьютера, выполните следующую команду:

```
KAVSHELL RTP /START
```

Команда `KAVSHELL RTP` должна включать один из двух параметров (см. таблицу ниже).

Таблица 143. Параметры команды KAVSHELL RTP

Ключ / параметр	Описание
/START	Запустить все задачи постоянной защиты компьютера: Постоянная защита файлов и Использование KSN.
/STOP	Остановить все задачи постоянной защиты компьютера.

kaspersky

Управление задачей Контроль запуска программ: KAVSHELL APPCONTROL /CONFIG

Команда `KAVSHELL APPCONTROL /CONFIG` позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

Синтаксис команды KAVSHELL APPCONTROL /CONFIG

```
 /config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<полный путь к XML файлу>
```

Примеры команды KAVSHELL APPCONTROL /CONFIG

► *Чтобы запустить задачу Контроль запуска программ в режиме **Активный** без контроля загрузки DLL-модулей и сохранить параметры задачи по завершении, выполните следующую команду:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Таблица 144. `KAVSHELL APPCONTROL /CONFIG` command-line parameters/options

Ключ / параметр	Описание
`/mode:<applyrules|statistics>`	Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: • active - применяются правила контроля запуска программ; • statistics - только формировать статистику.
`/dll:<no|yes>`	Выключить или включить контроль загрузки DLL-модулей.
`/savetofile: <полный путь к XML файлу>`	Экспортировать заданные правила в указанный файл в формате XML.
`/savetofile: <полное имя xml-файла>`	Сохранить список правил в файл.
`/savetofile: <полное имя xml-файла> /sdc`	Сохранить список правил контроля распространения программного обеспечения в файл.
`/clearsdc`	Удалить все правила контроля распространения программного обеспечения.

kaspersky

Формирование правил контроля запуска программ: KAVSHELL APPCONTROL /GENERATE

Команда `KAVSHELL APPCONTROL /GENERATE` позволяет формировать списки правил контроля запуска программ.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <путь к папке> | /source:<путь к файлу со списком папок> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<пользователь или группа пользователей>] [/export:<полный путь к XML файлу>] [/import:<a|r|m>] [/prefix:<префикс для названий правил>] [/unique]
```

Примеры команды KAVSHELL APPCONTROL /GENERATE

- *Чтобы сформировать правила для файлов из указанных папок, выполните команду:*

  ```
  KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
  /export:c:\rules\appctrlrules.xml
  ```

- *Чтобы сформировать правила для исполняемых файлов с любыми расширениями, хранящихся в указанной папке, и по завершении задачи сохранить сформированные правила в указанный XML-файл, выполните следующую команду:*

  ```
  KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
  /export:c\rules\appctrlrules.xml
  ```

Вы можете использовать ключи/параметры для настройки автоматического формирования правил задачи Контроль запуска программ (см. таблицу ниже).

Таблица 145. Ключи / параметры команды KAVSHELL APPCONTROL /GENERATE

Ключ / параметр	Описание
Область применения разрешающих правил	
<путь к папке>	Указать путь к папке с исполняемыми файлами, для которых будут автоматически формироваться разрешающие правила.
/source: <путь к файлу со списком папок>	Указать путь к TXT-файлу со списком папок, содержащих исполняемые файлы, для которых будут автоматически формироваться разрешающие правила.
/masks: <edms>	Указать расширения исполняемых файлов, для которых будут автоматически формироваться разрешающие правила. В область применения правил можно включить файлы со следующими расширениями: • e - файлы с расширением exe; • d - файлы с расширением dll; • m - файлы с расширением msi; • s - скрипты.
/runapp	Учитывать при формировании разрешающих правил программы, запущенные на защищаемом компьютере в текущий момент.
Действия при автоматическом формировании разрешающих правил	
/rules: <ch|cp|h>	Указать действия при формировании разрешающих правил для задачи Контроль запуска программ: • ch – использовать цифровой сертификат. Если сертификат отсутствует, использовать SHA256-хеш. • cp — использовать цифровой сертификат. Если сертификат отсутствует, использовать путь к исполняемому файлу. • h – использовать SHA256-хеш.
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании разрешающих правил для задачи Контроль запуска программ. Команда выполняется, если задано значение ключа /rules: <ch|cp>.
/user: <пользователь или группа пользователей>	Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или группой.

Ключ / параметр	Описание
Действия по завершении выполнения задачи Формирование правил контроля запуска программ	
/export: <полный путь к XML файлу>	Сохранить сформированные правила в XML-файл.
/unique	Добавлять информацию о защищаемом компьютере, по программам которого формируются разрешающие правила контроля запуска программ.
/prefix: <префикс для названий правил>	Указать префикс названий разрешающих правил контроля запуска программ.
/import: <a|r|m>	Импортировать сформированные правила в указанный список правил контроля запуска программ в соответствии с выбранным принципом добавления новых правил: • a – **Добавить правила к существующим** (одинаковые правила дублируются); • r – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален); • m – **Объединить правила с существующими** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).

Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL

Команда `KAVSHELL APPCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль запуска программ в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL APPCONTROL

► *Чтобы добавить к имеющимся правилам контроля запуска программ правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля запуска программ (см. таблицу ниже).

Таблица 146. Ключи / параметры команды KAVSHELL APPCONTROL

Ключ / параметр	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).
/merge <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила).
/clear	Очистить список правил контроля запуска программ.

Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL

Команда `KAVSHELL DEVCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль устройств в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL DEVCONTROL

► *Чтобы добавить к имеющимся правилам контроля устройств правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля устройств (см. таблицу ниже).

Таблица 147. Ключи / параметры команды KAVSHELL DEVCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).
/merge <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила).
/clear	Очистить список правил контроля устройств.

Запуск задачи Обновление баз программы: KAVSHELL UPDATE

Команда `KAVSHELL UPDATE` позволяет запускать задачу обновления баз Kaspersky Industrial CyberSecurity for Nodes в синхронном режиме.

Задача Обновление баз программы, запущенная с помощью команды `KAVSHELL UPDATE`, является временной. Она отображается в Консоли программы только во время ее выполнения. Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи. К задачам обновления, созданным и запущенным с помощью команды `KAVSHELL UPDATE`, и к задачам обновления, созданным в Консоли программы, могут применяться политики Kaspersky Security Center. Сведения об использовании Kaspersky Security Center для управления Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах приведены в разделе "Управление Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center".

Чтобы указать путь к источнику обновлений в этой задаче, можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду `KAVSHELL UPDATE` с правами этого пользователя.

Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE < Путь к источнику обновления | /AK | /KL > [/NOUSEKL]
[/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>]
[/PROXYPWD:<пароль>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
[/REG:<код iso3166>] [/W:<имя файла журнала выполнения задачи>]
[/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL UPDATE есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

Пример команды KAVSHELL UPDATE

- *Чтобы запустить пользовательскую задачу Обновление баз программы, выполните следующую команду:*

```
KAVSHELL UPDATE
```

- *Чтобы запустить задачу Обновление баз программы, файлы обновлений для которой хранятся в сетевой папке \\server\databases, выполните следующую команду:*

```
KAVSHELL UPDATE \\server\bases
```

- *Чтобы запустить задачу Обновление баз программы с FTP-сервера ftp://dnl-ru1.kaspersky-labs.com/ и записать все события задачи в файл c:\update_report.log, выполните следующую команду:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- *Чтобы загрузить обновления баз Kaspersky Industrial CyberSecurity for Nodes с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений с помощью прокси-сервера (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к защищаемому компьютеру с помощью встроенной в Windows проверки подлинности NTLM с именем пользователя netuser и паролем 123456, выполните следующую команду:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Таблица 148. Ключи / параметры команды KAVSHELL UPDATE

Ключ / параметр	Описание
Источник обновлений (обязательный параметр). Укажите один или несколько источников. Kaspersky Industrial CyberSecurity for Nodes будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC.
<URL>	Пользовательские источники обновления. Адрес HTTP- или FTP-сервера, на котором располагается папка с обновлениями.
<Локальная папка>	Пользовательские источники обновления. Папка на защищаемом компьютере.
/AK	Использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
/KL	Использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.
/NOUSEKL	Не использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны (по умолчанию).
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот параметр, Kaspersky Industrial CyberSecurity for Nodes будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	Этот параметр задает метод аутентификации для доступа к прокси-серверу. Он может принимать следующие значения: **0** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Industrial CyberSecurity for Nodes обращается к прокси-серверу с использованием учетной записи **Локальная система** (**SYSTEM**). **1** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Industrial CyberSecurity for Nodes обращается к прокси-серверу с использованием учетной записи, имя пользователя и пароль которой заданы параметрами /PROXYUSER и /PROXYPWD. **2** – обычная проверка подлинности по имени пользователя и паролю, заданным параметрами /PROXYUSER и /PROXYPWD. Если для доступа к прокси-серверу не требуется аутентификация, можно не указывать этот параметр.
/PROXYUSER:<имя пользователя>	Имя пользователя, используемое для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.

Ключ / параметр	Описание
/PROXYPWD:<пароль>	Пароль пользователя, используемый для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если указан параметр /PROXYUSER, но не указан параметр /PROXYPWD, считается, что задан пустой пароль.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию).
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используется).
/USEPROXYFORLOCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать прокси-сервер для локальных адресов**.
Общие параметры FTP- и HTTP-сервера	
/NOFTPPASSIVE	Если указан этот ключ, Kaspersky Industrial CyberSecurity for Nodes использует активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes использует пассивный режим FTP-сервера, при возможности.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот параметр, Kaspersky Industrial CyberSecurity for Nodes использует значение по умолчанию: 10 секунд. Значение параметра должно быть целым числом.
/REG:<код iso3166>	Региональные параметры. Этот параметр используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Industrial CyberSecurity for Nodes минимизирует нагрузку на защищаемый компьютер, выбирая ближайший к нему сервер обновлений. Значение этого параметра должно быть двухбуквенным кодом страны, в которой расположен защищаемый компьютер, в стандарте ISO 3166-1, например: /REG: gr или /REG:US. Если ключ не указан или указан недопустимый код страны, Kaspersky Industrial CyberSecurity for Nodes распознает местоположение защищаемого компьютера в соответствии с региональными параметрами защищаемого устройства, на котором установлена Консоль программы.
/ALIAS:<альтернативное название задачи>	Этот параметр позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Industrial CyberSecurity for Nodes. Если этот ключ не задан, задаче присваивается временное название вида update_<kavshell_pid>, например, update_1234. В Консоли программы задаче присваивается название "Обновление баз программы <дата и время>", например: "Обновление баз программы 16.08.2007 17:41:02".

Ключ / параметр	Описание
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Industrial CyberSecurity for Nodes сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** в Консоли программы. Если Kaspersky Industrial CyberSecurity for Nodes не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.

Коды возврата команды KAVSHELL UPDATE (на стр. 1035).

Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes: KAVSHELL ROLLBACK

Команда `KAVSHELL ROLLBACK` позволяет выполнить локальную системную задачу Откат обновления баз программы – откатить базы Kaspersky Industrial CyberSecurity for Nodes до предыдущей установленной версии. Команда выполняется синхронно.

Синтаксис команды

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK (на стр. 1035).

Управление анализом журналов: KAVSHELL TASK LOG-INSPECTOR

Команда `KAVSHELL TASK LOG-INSPECTOR` позволяет осуществлять контроль целостности среды, основываясь на анализе журнала событий Windows.

Синтаксис команды

```
KAVSHELL TASK LOG-INSPECTOR
```

Пример команды

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Таблица 149. Ключи / параметры команды KAVSHELL TASK LOG-INSPECTOR

Ключ / параметр	Описание
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи.

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR (на стр. 1033).

Активация программы. KAVSHELL LICENSE

Команда `KAVSHELL LICENSE` позволяет управлять ключами и кодами активации Kaspersky Industrial CyberSecurity for Nodes.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<файл ключа | код активации> [/R] | /DEL:<ключ | код активации>]
```

Примеры команды KAVSHELL LICENSE

► *Чтобы активировать программу, выполните команду:*

```
KAVSHELL.EXE LICENSE / ADD: <код активации или файл ключа>
```

► *Чтобы получить информацию о добавленных ключах, выполните команду:*

```
KAVSHELL LICENSE
```

► *Чтобы удалить добавленный ключ с номером 0000-000000-00000001, выполните команду:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Команда `KAVSHELL LICENSE` может быть выполнена как без ключей, так и с их использованием (см. таблицу ниже).

Таблица 150. Ключи / параметры команды KAVSHELL LICENSE

Параметр	Описание
Без ключей	Команда возвращает следующую информацию о добавленных ключах: • Ключ. • Тип лицензии (коммерческая). • Срок действия связанной с ключом лицензии. • Статус ключа (активный или дополнительный). Если значение статуса *, ключ добавлен в качестве дополнительного.
/ADD:<имя файла ключа или код активации>	Добавить ключ с помощью указанного файла или кода активации. Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/R	Код активации или ключ /R является дополнительным к коду активации или ключу /ADD и указывает, что код активации или ключ добавляется в качестве дополнительного.
/DEL:<ключ или код активации>	Удалить указанный ключ или код активации.

Коды возврата команды KAVSHELL LICENSE (на стр. 1036).

Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE

Команда `KAVSHELL TRACE` позволяет включать или выключать ведение журнала трассировки всех подсистем Kaspersky Industrial CyberSecurity for Nodes, а также устанавливать уровень детализации информации в журнале.

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<путь к папке с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] [/r:<максимальное количество файлов трассировки для ротации>] | /OFF>
```

Если ведется журнал трассировки и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом /ON и с помощью ключей /S и /LVL задайте параметры журнала трассировки (см. таблицу ниже).

Таблица 151. Ключи / параметры команды KAVSHELL TRACE

Ключ	Описание
/ON	Включить ведение журнала трассировки.
/F:<папка с файлами журнала трассировки>	Этот параметр указывает полный путь к папке, в которую будут сохранены файлы журнала трассировки (обязательный). Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Пути к папкам на сетевых дисках других защищаемых компьютерах указывать нельзя. Если указанный параметром путь содержит пробел, заключите его в кавычки, например: /F:"C:\Trace Folder". Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/S: <максимальный размер файла журнала в мегабайтах>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Industrial CyberSecurity for Nodes начнет записывать информацию в новый файл; предыдущий файл журнала сохранится. Если значение этого параметра не указано, максимальный размер одного файла журнала составит 50 МБ.
/LVL:debug|info|warning|error|critical	Этот параметр устанавливает уровень детализации журнала от максимального (**Вся отладочная информация**), при котором в журнал записываются все события, до минимального (**Критические события**), при котором в журнал записываются только критические события. Если значение этого параметра не указано, в журнал трассировки будут записываться все события с уровнем детализации **Вся отладочная информация**.

Ключ	Описание
/r:<максимальное количество файлов трассировки для ротации>	Этот параметр включает ротацию файлов трассировки. Если включена ротация файлов трассировки и достигнуто <максимальное количество файлов трассировки для ротации>, перед созданием нового файла самый старый файл удаляется. Доступные значения: от 1 до 999. Если значение не указано, ротация файлов трассировки не включается и программа возвращает ошибку.
/OFF	Этот параметр выключает ведение журнала трассировки.

Пример команды KAVSHELL TRACE

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Вся отладочная информация** и максимальным размером файла журнала 200 МБ и сохранить файл журнала в папке C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Важные события** и сохранить файл журнала в папку C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Чтобы включить журнал трассировки с использованием уровня детализации **Важные события**, сохранить файл журнала в папку C:\Trace Folder и включить ротацию файлов трассировки при достижении предельного количества 50 файлов, выполните следующую команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

► *Чтобы выключить ведение журнала трассировки, выполните команду:*

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE (на стр. 1036).

kaspersky

Дефрагментация файлов журнала Kaspersky Industrial CyberSecurity for Nodes. KAVSHELL VACUUM

Команда `KAVSHELL VACUUM` позволяет выполнить дефрагментацию файлов журнала программы. Это помогает избежать системных ошибок и ошибок программы из-за хранения большого количества файлов журнала, сформированных на основе событий программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Рекомендуется применять команду `KAVSHELL VACUUM` для оптимизации хранения файлов журналов в случае частых запусков задач проверки по требованию и задач обновления. При выполнении команды Kaspersky Industrial CyberSecurity for Nodes обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом компьютере по указанному пути.

По умолчанию файлы журнала программы сохраняются в папку C:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\3.2\Reports. Если вы вручную указали другой путь для хранения файлов журнала, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журнала Kaspersky Industrial CyberSecurity for Nodes.

Файлы большого размера увеличивают время, необходимое команде `KAVSHELL VACUUM` на выполнение дефрагментации.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля компьютера. Процедура дефрагментации блокирует доступ к журналу Kaspersky Industrial CyberSecurity for Nodes и запрещает запись событий в журнал. Чтобы избежать снижения защиты, рекомендуется планировать запуск команды `KAVSHELL VACUUM`.

► *Чтобы выполнить дефрагментацию файлов журнала Kaspersky Industrial CyberSecurity for Nodes, выполните команду:*

```
KAVSHELL VACUUM
```

Для выполнения команды необходимы права учетной записи Локальная система (Local System).

kaspersky

Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Industrial CyberSecurity for Nodes использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Industrial CyberSecurity for Nodes создает файлы klamfb.dat и klamfb2.dat в папке %SYSTEMDRIVE%\System Volume Information. Эти файлы содержат информацию о проверенных незараженных объектах. Размер файла klamfb.dat (klamfb2.dat) увеличивается пропорционально количеству файлов, проверенных Kaspersky Industrial CyberSecurity for Nodes. В этом файле хранится только актуальная информация о существующих в системе файлах: если файл был удален, то Kaspersky Industrial CyberSecurity for Nodes удаляет информацию о нем из файла klamfb.dat.

Для очистки данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла klamfb.dat с помощью команды KAVSHELL FBRESET, Kaspersky Industrial CyberSecurity for Nodes не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Industrial CyberSecurity for Nodes может увеличить нагрузку на защищаемый компьютер. При этом после очистки файла klamfb.dat Kaspersky Industrial CyberSecurity for Nodes проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Industrial CyberSecurity for Nodes заново добавляет информацию о каждом проверенном объекте в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не проверять файл повторно, если он не был изменен.

Для выполнения команды `KAVSHELL FBRESET` нужно запускать интерпретатор командной строки с правами учетной записи SYSTEM.

Включение и выключение создания файла дампа. KAVSHELL DUMP

Команда `KAVSHELL DUMP` позволяет включать и выключать создание образов памяти (файлов дампов) процессов Kaspersky Industrial CyberSecurity for Nodes при их аварийном завершении (см. таблицу ниже). Кроме того, можно в любой момент создать файл дампа для выполняющихся процессов Kaspersky Industrial CyberSecurity for Nodes.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена с правами учетной записи локальной системы (SYSTEM).

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.
Команда KAVSHELL DUMP не используется для 64-разрядных процессов.

Синтаксис команды KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом
дампа> / P:<pid> | /OFF>
```

Таблица 152. Ключи / параметры команды KAVSHELL DUMP

Ключ	Описание
/ON	Включить создание файла дампа при аварийном завершении процесса.
/F:<папка с файлами дампов>	Это обязательный параметр. Указывает путь к папке, в которой будет сохранен файл дампа. Нельзя указывать пути к папкам на сетевых дисках других незащищенных устройств. При указании пути к папке с файлом дампа можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя.
/SNAPSHOT	Снимает образ памяти выполняющегося процесса с указанным идентификатором и сохраняет файл дампа в папку, указанную параметром /F.
/P	Идентификатор процесса (PID); отображается в Диспетчере задач Microsoft Windows.
/OFF	Выключить создание файла дампа при аварийном завершении процесса.

Коды возврата команды KAVSHELL DUMP (на стр. 1037).

Пример команды KAVSHELL DUMP

► *Чтобы включить создание файла дампа и сохранить файл дампа в папку C:\Dump Folder, выполните команду:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Чтобы снять образ памяти процесса с идентификатором 1234 в папку C:/Dumps, выполните команду:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

► *Чтобы выключить создание файлов дампа, выполните команду:*

```
KAVSHELL DUMP /OFF
```

kaspersky

Импорт параметров. KAVSHELL IMPORT

Команда `KAVSHELL IMPORT` позволяет импортировать параметры Kaspersky Industrial CyberSecurity for Nodes и текущих задач программы из конфигурационного файла в Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве. Вы можете создать конфигурационный файл с помощью команды `KAVSHELL EXPORT`.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL IMPORT

```
KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Таблица 153. Параметр команды KAVSHELL IMPORT

Параметр	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL IMPORT (на стр. 1038).

Экспорт параметров. KAVSHELL EXPORT

Команда `KAVSHELL EXPORT` позволяет экспортировать все параметры Kaspersky Industrial CyberSecurity for Nodes и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Industrial CyberSecurity for Nodes на других защищаемых компьютерах.

Синтаксис команды KAVSHELL EXPORT

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Таблица 154. Параметр команды KAVSHELL EXPORT

Параметр	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Конфигурационному файлу можно присвоить любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL EXPORT (на стр. 1038).

Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

Команда KAVSHELL OMSINFO позволяет просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами. Информация об угрозах поступает из доступных журналов событий.

Синтаксис команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <полный путь к сформированному файлу с именем файла>
```

Пример команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Таблица 155. Параметр команды KAVSHELL OMSINFO

Параметр	Описание
<путь к сформированному файлу с именем файла>	Имя сформированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах.

kaspersky

Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE

Команда `KAVSHELL FIM /BASELINE` позволяет настраивать режим работы задачи Мониторинг целостности файлов на основе эталона и контролировать загрузку DLL-модулей.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<область мониторинга> | /L:<путь к TXT-файлу со списком областей мониторинга>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/EXPORT:<путь к TXT-файлу> [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SHOW [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SCAN [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/PWD:<пароль>]
```

Примеры команды KAVSHELL FIM /BASELINE

► *Чтобы удалить эталон, выполните следующую команду:*

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<идентификатор эталона>
```

Вы можете настраивать параметры задачи Мониторинг целостности файлов на основе эталона с помощью параметров командной строки (см. таблицу ниже).

Таблица 156. Ключи / параметры команды KAVSHELL FIM/ BASELINE

Ключ / параметр	Описание
`/CREATE`	Создать задачу Мониторинг целостности файлов на основе эталона. Kaspersky Industrial CyberSecurity for Nodes запустит новую задачу Мониторинг целостности файлов на основе эталона, чтобы создать эталон.
`/L`	Укажите путь к TXT-файлу, содержащему список областей мониторинга.
`/MD5`	Укажите алгоритм MD5 для расчета контрольной суммы (необязательный параметр). Параметр `/MD5` не используется совместно с параметром `/SHA256`. Алгоритм MD5 используется по умолчанию.

Ключ / параметр	Описание
/SHA256	Укажите алгоритм SHA256 для расчета контрольной суммы (необязательный параметр). Параметр /SHA256 не используется совместно с параметром /MD5. Алгоритм MD5 используется по умолчанию.
/SF	Включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона (необязательный параметр). По умолчанию вложенные папки не входят в область задачи Мониторинг целостности файлов на основе эталона.
/CLEAR	Удалить эталон с указанным <идентификатором эталона> или эталон задачи с указанным <существующим названием>. Удалить все эталоны, если не указан ни один из параметров <идентификатор эталона> или <существующее название>. Необязательный параметр.
/BL	Укажите уникальный идентификатор эталона (необязательный параметр).
/EXPORT	Экспортировать данные всех эталонов в TXT-файл.
/SHOW	Показать данные всех эталонов.
/SCAN	Запустить новую задачу Мониторинг целостности файлов на основе эталона с указанным <идентификатором эталона> или <существующим названием>.
/ALIAS	Укажите название новой или существующей задачи.
<область мониторинга>	Укажите файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона. Этот параметр позволяет указать только одну область.
<путь к TXT-файлу со списком областей мониторинга>	Укажите путь к TXT-файлу, содержащему список областей мониторинга. Файл должен быть в кодировке UTF-8, а путь к каждой области мониторинга необходимо указывать на отдельной строке.
<путь к TXT-файлу>	Укажите путь к файлу, в который вы хотите экспортировать данные всех эталонов.

Ключ / параметр	Описание
<идентификатор эталона>	Укажите уникальный идентификатор эталона. Чтобы просмотреть идентификатор эталона, используйте параметр /SHOW.
<существующее название>	Укажите название существующей задачи.
<новое название>	Укажите название новой задачи.

Коды возврата команд

В этом разделе

kaspersky

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Таблица 157. Коды возврата команд KAVSHELL START и KAVSHELL STOP

Код возврата	Описание
0	Операция выполнена успешно
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-6	Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена)
-7	Служба не зарегистрирована
-8	Автоматический запуск службы отключен
-9	Неудачная попытка запустить управляемое устройство под другой учетной записью (по умолчанию служба Kaspersky Security работает под учетной записью Локальная система).
-99	Неизвестная ошибка

kaspersky

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Таблица 158. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден файл со списком областей проверки)
-5	Неверный синтаксис команды или не определена область проверки
-80	Зараженных и других обнаруживаемых объектов
-81	Возможно зараженных объектов
-82	Обнаружены ошибки обработки
-83	Обнаружены непроверенные объекты
-84	Обнаружены поврежденные объекты
-85	Не удалось создать журнал выполнения задачи
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Таблица 159. Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Код возврата	Описание
0	Операция выполнена успешно
-6	Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена)
402	Задача уже запущена (для параметра /STATE)

Коды возврата команды KAVSHELL TASK

Таблица 160. Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для параметра /STATE)
402	Задача уже запущена (для параметра /STATE)
403	Задача уже приостановлена (для параметра /STATE)
-404	Сбой выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL RTP

Таблица 161. Коды возврата команды KAVSHELL RTP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найдена одна или все задачи постоянной защиты компьютера)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача уже запущена или уже остановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL UPDATE

Таблица 162. Коды возврата команды KAVSHELL UPDATE

Код возврата	Описание
0	Операция выполнена успешно
200	Все объекты актуальны (базы или программные компоненты в актуальном состоянии)
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Ошибка аутентификации при подключении к прокси-серверу
-234	Ошибка подключения к программе Kaspersky Security Center
-235	Kaspersky Industrial CyberSecurity for Nodes не прошел проверку подлинности при соединении с источником обновлений
-236	Базы программы повреждены
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Таблица 163. Коды возврата команды KAVSHELL ROLLBACK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-99	Неизвестная ошибка
-221	Резервная копия баз не найдена
-222	Резервная копия баз повреждена

Коды возврата команды KAVSHELL LICENSE

Таблица 164. Коды возврата команды KAVSHELL LICENSE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Недостаточно прав для управления ключами
-4	Ключ с указанным номером не найден
-5	Неверный синтаксис команды
-6	Неверная операция (ключ уже добавлен)
-99	Неизвестная ошибка
-301	Недействительный ключ
-303	Лицензия распространяется на другую программу

Коды возврата команды KAVSHELL TRACE

Таблица 165. Коды возврата команды KAVSHELL TRACE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь к папке с файлами журнала трассировки)
-5	Неверный синтаксис команды
-6	Недопустимая операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL FBRESET

Таблица 166. Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL DUMP

Таблица 167. Коды возврата команды KAVSHELL DUMP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь к папке с файлом дампа; не найден процесс с указанным идентификатором)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения команды KAVSHELL DUMP /OFF, если создание файла дампа уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL IMPORT

Таблица 168. Коды возврата команды KAVSHELL IMPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не удается найти конфигурационный файл для импорта)
-5	Неверный синтаксис
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Industrial CyberSecurity for Nodes не импортировала параметры некоторых функциональных компонентов)
-502	Файл импорта отсутствует или имеет неизвестный формат
-503	Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Industrial CyberSecurity for Nodes более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Таблица 169. Коды возврата команды KAVSHELL EXPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Industrial CyberSecurity for Nodes не экспортировала параметры некоторых функциональных компонентов)

kaspersky

Коды возврата команды KAVSHELL FIM /BASELINE

Таблица 170. Коды возврата команды KAVSHELL FIM /BASELINE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, эталон был удален)
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-12	Неверный пароль
-80	Не соответствует удаленным эталонным объектам
-85	Не удалось создать журнал выполнения задачи
-99	Внутренняя ошибка
-303	Недопустимый лицензионный ключ
-502	Задача не запущена
200	Все объекты соответствуют эталону
501	Задача завершена успешно с ошибкой / комментарием

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В приложении Kaspersky Security Center, находящемся 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 приложениями, 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, приложения еще раз проведут контроль целостности загружаемых обновлений.

kaspersky

Устранение уязвимостей и установка критических обновлений в приложении

"Лаборатория Касперского" может выпускать обновления приложения, 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 приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения 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.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки.

kaspersky

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.

Поддержка программы предоставляется в течение ее жизненного цикла (см. страницу жизненного цикла программ https://support.kaspersky.com/corporate/lifecycle).
Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки, отправив запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

kaspersky

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Дополнительная информация о Kaspersky CompanyAccount приведена на веб-сайте Службы технической поддержки http://support.kaspersky.ru/faq/companyaccount_help.

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Industrial CyberSecurity for Nodes и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять защищаемое устройство на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки системы.

kaspersky

Источники информации о Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

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

В этом разделе

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Industrial CyberSecurity for Nodes:

- страница Kaspersky Industrial CyberSecurity for Nodes на веб-сайте "Лаборатории Касперского";
- страница программы на веб-сайте Службы технической поддержки (База знаний).

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/.

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Industrial CyberSecurity for Nodes на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Industrial CyberSecurity for Nodes https://www.kaspersky.ru/enterprise-security/industrial можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Для приобретения программы или продления лицензии вы можете обратиться к нашим партнерам и представителям.

Страница Kaspersky Industrial CyberSecurity for Nodes в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Industrial CyberSecurity for Nodes в Базе знаний https://support.kaspersky.ru/kics вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний содержат информацию, относящуюся не только к Kaspersky Industrial CyberSecurity for Nodes, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний могут также включать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" на форуме

Вы можете обсудить вопросы, связанные с программами "Лаборатории Касперского", с другими пользователями и специалистами "Лаборатории Касперского" на нашем форуме https://community.kaspersky.com/.

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает приложения, 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 приложениями "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com (https://community.kaspersky.com/)

kaspersky

Глоссарий

E

End User License Agreement

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков) с помощью различных технологий безопасности. Пример Endpoint Protection Platform – решение Kaspersky Endpoint Security для бизнеса.

EPP-приложение

Приложение, входящее в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP). EPP-приложения устанавливаются на конечные устройства внутри IT-инфраструктуры организации (например, мобильные устройства, компьютеры или ноутбуки). Примером EPP-приложения является Kaspersky Endpoint Security for Windows в составе EPP-решения Kaspersky Endpoint Security for Business.

I

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми приложение считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

K

Kaspersky Endpoint Agent

Kaspersky Industrial CyberSecurity for Nodes - приложение, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Kaspersky Industrial CyberSecurity for Nodes взаимодействует с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории

Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

Объект, который присоединен к другому файлу или встроен в другой файл с использованием технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel, встроенная в документ Microsoft Office Word.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

OVAL-правила

OVAL (Open Vulnerability and Assessment Language) – открытый язык описания и оценки уязвимостей. OVAL стандартизирует следующие компоненты процесса оценки:

- Представление конфигурационной информации для системы.
- Анализ системы на предмет наличия состояний: уязвимости, обновления, патчи и т.п.
- Представление отчетов по оценке системы.

Для выполнения задачи Аудит безопасности Kaspersky Industrial CyberSecurity for Nodes использует файлы с OVAL-правилами в формате .xml. По результатам проверки приложение формирует отчет.

S

SIEM

Аббревиатура от Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

T

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Y

YARA-файл

YARA-файлы – это файлы с расширением `yara` или `yar`, которые содержат YARA-правила.

YARA-правила представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру

организации. По этим правилам Kaspersky Industrial CyberSecurity for Nodes производит проверку объектов. Если правило выполняется, анализатор выносит заключение о заражении с соответствующими подробностями в журнале.

А

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

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 в проверяемых объектах вредоносный код. Антивирусные базы формируются 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 приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

К

Карантин

Папка, в которую приложение "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.

kaspersky

Ложное срабатывание

Ситуация, когда незараженный объект определяется приложением "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

М

Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

Н

Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор приложений, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и 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

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

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, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

С

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сервер сбора телеметрии

Тип сервера, с которым Kaspersky Industrial CyberSecurity for Nodes поддерживает интеграцию. В рамках интеграции Kaspersky Industrial CyberSecurity for Nodes отправляет *телеметрию* на сервер, получает задачи от сервера, а также готовит отчеты о выполнении этих задач.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Т

Телеметрия

Данные, которые Kaspersky Industrial CyberSecurity for Nodes анализирует на защищаемом устройстве и отправляет на *Сервер сбора телеметрии*. Телеметрия представляет собой список событий, которые произошли на защищаемом устройстве.

Точки автозапуска

Список процессов, которые автоматически запускаются в фоновом режиме на конечных устройствах (например, мобильных устройствах, компьютерах или ноутбуках) при возникновении определённых условий (например, загрузка операционной системы, вход в систему, запуск файлового проводника, запланированные задачи). Файлы автозапущенных программ могут быть скрытыми, что может быть причиной неявного замедления работы устройства или наличия на устройстве вредоносных программ.

Трассировка

Отладочное выполнение приложения, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

Уровень важности события

Характеристика события, зафиксированного в работе приложения "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Отказ функционирования.
- 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 приложении, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или приложение 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 приложений.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

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).

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Domino, Lotus Notes – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Forefront, Excel, Hyper-V, Internet Explorer, JScript, Lync, Outlook, PowerShell, SharePoint, SQL Server, Surface, Windows, Windows Server и Windows Vista являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

NetApp – товарный знак или зарегистрированный в США и/или других странах товарный знак NetApp, Inc.

Schneider Electric – товарный знак компании Schneider Electric.

Siemens, Simatic и WinCC – зарегистрированные товарные знаки Siemens AG.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 171. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа, ПО	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 программы, базы доверенных/недоверенных сертификатов, облачные базы KSN	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь
уведомления о критических событиях пользователей и администратора	сигналы тревоги

kaspersky

Приложение. Значения параметров программы в сертифицированной конфигурации

В сертифицированной версии программы Kaspersky Industrial CyberSecurity for Nodes допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния программы.

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 172. 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 Контроль устройств	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Использование KSN	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Проверка по требованию	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Постоянная защита	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Защита от шифрования	Выбор компонентов для установки на защищаемый сервер.	Установлен (по умолчанию)
Компонент Значок в области уведомлений	Выбор компонентов для установки на защищаемый сервер.	Установлен (по умолчанию)

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройки прав доступа и функциональных компонентов		
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 3.2. • Запущена • Остановлена	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 3.2: • 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.
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 3.2. • Запущена • Остановлена	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 3.2: • 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

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Лицензирование	Активация программы с помощью ключа.	Добавлен файл ключа. По окончании срока действия ключа программа выходит из сертифицированного состояния.
Задача Обновление баз программы	Копирует базы из источника обновлений на устройство и сразу переходит к их использованию в выполняющейся задаче Постоянная защита компьютера: • Не выполняется. • Ежечасно. • Ежесуточно. • Еженедельно. • При запуске программы.	Одно из следующих значений: • Ежечасно. • Ежесуточно. • Еженедельно. • При запуске программы.
Задача Обновление модулей программы	Проверяет доступность обновлений модулей программы в источнике обновлений: • Не выполняется. • Ежечасно. • Ежесуточно. • Еженедельно. • При запуске программы.	Не выполняется. Включение обновления модулей программы приводит к выходу программы из сертифицированного состояния.
Использовать 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.
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).

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
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.	Область защиты включает в себя все съемные диски, все жесткие диски, все общие сетевые папки. Исключение папок из области защиты, установленной по умолчанию, может привести к выходу программы 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	Применяется (флажок установлен) как минимум для следующих объектов: • Все архивы. • Все SFX-архивы. • Все упакованные объекты. • Все вложенные OLE-объекты.
Действия над заражёнными и другими обнаруженными объектами	Действие по умолчанию, которое выполняет программа при обнаружении заражённых и других обнаруженных объектов. Один из следующих вариантов: • Лечить. • Лечить, Удалять если не удалось. • Удалять • Выполнять рекомендуемое действие. • Только сообщать.	Одно из следующих значений: • Лечить. • Лечить, Удалять если не удалось. • Удалять. • Выполнять рекомендуемое действие.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Действия над возможно заражёнными объектами	Действие по умолчанию, которое выполняет программа при обнаружении возможно заражённых объектов. Один из следующих вариантов: • Перемещать на карантин. • Удалять. • Выполнять рекомендуемое действие. • Только сообщать.	Одно из следующих значений: • Перемещать на карантин. • Удалять. • Выполнять рекомендуемое действие.
Действия над составными файлами, недоступными для изменения	Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменён программой: • Не удалять файл (флажок снят). • Удалять файл (флажок установлен).	Удалять файл (флажок установлен).
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). Исключение обнаруживаемых объектов из проверки допускается только для подтвержденных ложноположительных срабатываний для исключения влияния программы на технологические процессы АСУ ТП.
Параметр остановки проверки, если она занимает более указанного времени	Если проверка объекта занимает более указанного настройкой времени в секундах, то проверка объекта прерывается, и программа переходит к следующим объектам. Значения: • Не применяется (флажок снят). • Применяется (флажок установлен и указано время интервала).	Не применяется (флажок снят).

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметр пропуска составных объектов, превышающих определенный размер	Если размер составного объекта более указанного в настройке в мегабайтах, то программа не проверяет такой объект и переходит к следующих объектам. Значения: • Не применяется (флажок снят). • Применяется (флажок установлен и указан максимальный размер).	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.
Настройка параметров аудита		
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 может привести 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 может привести 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 может привести к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройка сигналов тревоги		
Уведомление администраторов	Способы уведомления администраторов: • Средствами службы сообщений; • Путем запуска исполняемого файла; • По электронной почте.	Выбран способ Средствами службы сообщений. Другие способы оповещения могут быть включены.
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.