

Kaspersky Industrial CyberSecurity for Nodes

643.46856491.00093-02 90 01

Руководство администратора

Версия программы: 2.5.0.235

Уважаемый пользователь!

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

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

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

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

Документ может быть изменен без предварительного уведомления.

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

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

Дата редакции документа: 26.06.2018

Обозначение документа: 643.46856491.00093-02 90 01

© АО "Лаборатория Касперского", 2018.

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

Содержание

Об этом документе	10
О программе	11
Требования	12
Аппаратные и программные требования	12
Указания по эксплуатации и требования к среде	15
Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA	17
Типовые схемы развертывания	18
Подготовка к установке программы	20
Установка и удаление программы	22
Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer	22
Компоненты программы Kaspersky Industrial CyberSecurity for Nodes 2.5	23
Программные компоненты набора "Средства администрирования"	25
Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	26
Процессы Kaspersky Industrial CyberSecurity for Nodes 2.5	29
Параметры установки и удаления и их ключи для службы Windows Installer	30
Журнал установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5	37
Планирование установки	38
Выбор средств администрирования	38
Выбор способа установки	39
Установка и удаление программы с помощью мастера	41
Установка с помощью мастера установки	41
Установка Kaspersky Industrial CyberSecurity for Nodes 2.5	42
Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5	44
Дополнительная настройка после установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере	45
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	47
Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes 2.5	50
Удаление с помощью мастера установки	51
Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5	52
Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5	53
Установка и удаление программы из командной строки	53
Об установке и удалении Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки	54
Примеры команд установки Kaspersky Industrial CyberSecurity for Nodes 2.5	54
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	56
Добавление и удаление компонентов. Примеры команд	57
Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 Примеры команд	58
Коды возврата	58
Установка и удаление программы через Kaspersky Security Center	59

Общие сведения об установке через Kaspersky Security Center	60
Права для установки или удаления Kaspersky Industrial CyberSecurity for Nodes 2.5	60
Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center	61
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	63
Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center	63
Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center	64
Установка и удаление программы через групповые политики Active Directory	64
Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory	65
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	66
Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory	66
Подготовка программы к работе	67
Процедура приемки	68
Безопасное состояние	68
Настройка прав доступа	68
Сигналы тревоги	70
События аудита	71
Постоянная защита файлов	72
Проверка по требованию	72
Настройка обновлений баз программы	73
Проверка работоспособности. Тестовый файл EICAR	74
Разделение доступа к функциям программы по пользовательским ролям	77
О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5	77
О правах на управление службой Kaspersky Security	79
О правах доступа к службе Kaspersky Security Management	81
Настройка прав доступа для Kaspersky Industrial CyberSecurity for Nodes 2.5 и службы Kaspersky Security	81
Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля	84
Разрешение сетевых соединений для службы Kaspersky Security Management	85
Интерфейсы управления программой	87
Создание и настройка политик	88
О политиках	88
Создание политики	89
Настройка политики	90
Настройка запуска по расписанию локальных системных задач	96
Создание и настройка задач в Kaspersky Security Center	98
О создании задач в Kaspersky Security Center	98
Создание задачи в Kaspersky Security Center	99
Настройка локальных задач в окне Параметры программы в Kaspersky Security Center	103
Контроль проектов ПЛК	104

О Проверке целостности проектов ПЛК	105
О Реестре Конфигураций ПЛК	106
Настройка реестра ПЛК	106
Настройка Проверки целостности проектов ПЛК	108
Настройка Проверки целостности проектов ПЛК	109
Включение и выключение Проверки целостности проектов ПЛК	110
Импорт и экспорт данных для задачи Получение данных о проектах ПЛК	111
Настройка групповых задач в Kaspersky Security Center	111
Задачи формирования правил контроля устройств и контроля запуска программ	120
Задача Активация программы	122
Задачи обновления	123
Задача Проверка целостности модулей программы	124
Создание задачи проверки по требованию	125
Настройка задач проверки по требованию	128
Присвоение задаче проверки по требованию статуса Задача проверки важных областей	129
Настройка параметров диагностики сбоев в Kaspersky Security Center	130
Работа с расписанием задач	132
Настройка параметров расписания запуска задач	133
Включение и выключение запуска по расписанию	134
Управление параметрами программы	136
Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center	136
О настройке общих параметров программы в Kaspersky Security Center	137
Настройка масштабируемости и интерфейса в Kaspersky Security Center	137
Настройка параметров безопасности в Kaspersky Security Center	139
Настройка параметров соединения в Kaspersky Security Center	141
О настройке дополнительных возможностей программы	142
Настройка параметров доверенной зоны в Kaspersky Security Center	143
Добавление доверенных процессов	145
Использование маски not-a-virus	147
Проверка съёмных дисков	148
Настройка прав доступа в Kaspersky Security Center	150
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center	151
Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы	152
О блокировании доступа к сетевым файловым ресурсам	152
Включение блокирования доступа к сетевым файловым ресурсам	153
Настройка параметров хранилища заблокированных узлов	154
О настройке журналов и уведомлений	155
Настройка параметров журналов	156
Журнал безопасности	157
Настройка параметров интеграции с SIEM	157
Настройка параметров уведомлений	161

Настройка формирования инцидентов и взаимодействия с Сервером администрирования	162
Постоянная защита компьютера	165
Постоянная защита файлов	165
О задаче Постоянная защита файлов	165
Настройка задачи Постоянная защита файлов	166
Применение эвристического анализатора	168
Выбор режима защиты объектов	169
Область защиты в задаче Постоянная защита файлов	170
Предопределенные области защиты	170
Выбор предустановленных уровней безопасности	171
Настройка параметров безопасности вручную	173
Настройка общих параметров задачи	175
Настройка действий	177
Настройка производительности	179
Использование KSN	181
О задаче Использование KSN	181
Настройка параметров задачи Использование KSN	183
Настройка обработки данных	186
Настройка передачи дополнительных данных	188
Защита от эксплойтов	188
О защите от эксплойтов	189
Настройка параметров защиты памяти процессов	190
Добавление защищаемого процесса	192
Техники защиты от эксплойтов	193
Контроль активности на компьютерах	195
Управление запуском программ из Kaspersky Security Center	195
Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center	195
Настройка параметров задачи Контроль запуска программ	196
О Контроле пакетов установки	201
Настройка контроля пакетов установки	203
Переход в режим разрешения по умолчанию	206
О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center	207
Создание разрешающих правил из событий Kaspersky Security Center	209
Импорт правил контроля запуска программ из файла формата XML	210
Импорт правил из файла отчета Kaspersky Security Center о заблокированных запусках программ	212
Контроль Wi-Fi	214
О задаче Контроль Wi-Fi	214
Настройка параметров задачи Контроль Wi-Fi	215
О списке доверенных сетей Wi-Fi	217

Добавление доверенной сети Wi-Fi вручную.....	217
Добавление доверенной сети Wi-Fi с помощью списка доступных сетей Wi-Fi.....	219
Удаление исключения для сети Wi-Fi.....	220
Контроль активности в сети	222
Защита от шифрования.....	222
О задаче Защита от шифрования.....	222
Настройка параметров задачи Защита от шифрования.....	223
Общие параметры задачи	224
Формирование области защиты.....	225
Добавление исключений.....	227
Диагностика системы.....	228
Мониторинг файловых операций.....	228
О задаче Мониторинг файловых операций.....	228
О правилах мониторинга файловых операций.....	229
Настройка параметров задачи Мониторинг файловых операций.....	231
Настройка правил мониторинга	233
Анализ журналов	236
О задаче Анализ журналов.....	236
Настройка параметров предзаданных правил задачи.....	238
Настройка правил анализа журналов.....	240
Контроль производительности. Счетчики Kaspersky Industrial CyberSecurity for Nodes 2.5	242
Счетчики производительности для программы Системный монитор.....	242
О счетчиках производительности Kaspersky Industrial CyberSecurity for Nodes 2.5	242
Общее количество отвергнутых запросов.....	243
Общее количество пропущенных запросов	244
Количество запросов, не обработанных из-за нехватки системных ресурсов	245
Количество запросов, отданных на обработку	245
Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).	246
Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).	246
Количество элементов в очереди зараженных объектов	247
Количество объектов, обрабатываемых за секунду.....	248
Счетчики и ловушки SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5	249
О счетчиках и ловушках SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.....	249
Счетчики SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.....	249
Счетчики производительности	250
Счетчики карантина.....	250
Счетчики резервного хранилища	250
Общие счетчики	251
Счетчик обновления.....	251
Счетчики постоянной защиты.....	251

Ловушки SNMP	252
Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки.....	260
Команды командной строки	260
Отображение справки о командах Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL HELP	262
Запуск и остановка службы Kaspersky Security KAVSHELL START, KAVSHELL STOP	263
Проверка указанной области. KAVSHELL SCAN	263
Запуск задачи Проверка важных областей. KAVSHELL SCANCritical	267
Управление указанной задачей в асинхронном режиме. KAVSHELL TASK	268
Запуск и остановка задач постоянной защиты. KAVSHELL RTP	269
Управление задачами Контроль запуска программ KAVSHELL APPCONTROL /CONFIG	270
Автоматическое формирование разрешающих правил KAVSHELL APPCONTROL /GENERATE ...	271
Заполнение списка правил задачи Контроль запуска программ KAVSHELL APPCONTROL.....	273
Запуск задачи обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL UPDATE	274
Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL ROLLBACK	277
Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR.....	278
Активация программы KAVSHELL LICENSE	278
Включение, настройка и выключение создания журнала трассировки. KAVSHELL TRACE	280
Дефрагментация файлов журнала Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL VACUUM	281
Очищение базы iSwift. KAVSHELL FBRESET	282
Включение и выключение создания файла дампа. KAVSHELL DUMP	283
Импорт параметров. KAVSHELL IMPORT	284
Экспорт параметров. KAVSHELL EXPORT	285
Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO	285
Коды возврата командной строки.....	286
Коды возврата команд KAVSHELL START и KAVSHELL STOP	286
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical	287
Коды возврата команды KAVSHELL TASK LOG-INSPECTOR.....	287
Коды возврата команды KAVSHELL TASK.....	288
Коды возврата команды KAVSHELL RTP.....	288
Коды возврата команды KAVSHELL UPDATE.....	289
Коды возврата команды KAVSHELL ROLLBACK.....	289
Коды возврата команды KAVSHELL LICENSE.....	290
Коды возврата команды KAVSHELL TRACE	290
Коды возврата команды KAVSHELL FBRESET	291
Коды возврата команды KAVSHELL DUMP.....	291
Коды возврата команды KAVSHELL IMPORT	291
Коды возврата команды KAVSHELL EXPORT	292

Обновление антивирусных баз в ручном режиме	293
Устранение уязвимостей и установка критических обновлений в программе	294
Действия после сбоя или неустранимой ошибки в работе программы	295
Способы получения технической поддержки	296
Техническая поддержка по телефону	296
Техническая поддержка через Kaspersky CompanyAccount	296
АО "Лаборатория Касперского"	298
Информация о стороннем коде	300
Уведомления о товарных знаках	301
Соответствие терминов.....	302
Глоссарий	303
Приложение. Значения параметров программы в сертифицированной конфигурации	308

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия " Kaspersky Industrial CyberSecurity for Nodes 2.5.0.235" (далее также " Kaspersky Industrial CyberSecurity for Nodes 2.5", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Industrial CyberSecurity for Nodes 2.5, а также поддержка организаций, использующих Kaspersky Industrial CyberSecurity for Nodes 2.5.

О программе

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

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

В программе реализованы следующие функции безопасности:

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

Требования

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

В этом разделе

Аппаратные и программные требования.....	12
Указания по эксплуатации и требования к среде	15

Аппаратные и программные требования

Этот раздел содержит перечень аппаратных и программных требований Kaspersky Industrial CyberSecurity for Nodes 2.5.

Аппаратные требования к защищаемым устройствам

Общие требования:

- x86-совместимые системы в однопроцессорной и многопроцессорной конфигурации;
- x64-совместимые системы в однопроцессорной и многопроцессорной конфигурации;

Объем дискового пространства для установки:

- Для установки компонента Контроль запуска программ – 50 МБ;
- Для установки всех компонентов Kaspersky Industrial CyberSecurity for Nodes – 500 МБ.

Объем оперативной памяти:

- 256 МБ при установке компонента Контроль запуска программ на устройстве под управлением 32-разрядных операционных систем Microsoft Windows XP Embedded / Windows XP / Windows Embedded POSReady 2009;
- 512 МБ при установке всех компонентов программы на устройстве под управлением 32-разрядных операционных систем Microsoft Windows XP Embedded / Windows XP / Windows Embedded POSReady 2009;
- 1 ГБ при установке всех компонентов программы на устройстве под управлением других 32-разрядных операционных систем Microsoft Windows;
- 2 ГБ при установке всех компонентов программы на устройстве под управлением 64-разрядных операционных систем Microsoft Windows.

Минимальные требования к процессору:

- для 32-разрядных операционных систем Microsoft Windows – Intel® Pentium® III
- для 64-разрядных операционных систем Microsoft Windows – Intel Pentium IV.

Программные требования к защищаемым устройствам

Настольные операционные системы:

- Windows XP Professional SP2 x86
- Windows XP Professional SP2 x64
- Windows XP Professional SP3 x86
- Windows Vista® SP2 x86
- Windows Vista SP2 x64
- Семейство Windows 7:
 - Windows 7 Professional x86
 - Windows 7 Professional x64
 - Windows 7 Enterprise x86
 - Windows 7 Enterprise x64
 - Windows 7 Ultimate x86
 - Windows 7 Ultimate x64
 - Windows 7 Professional SP1 x86
 - Windows 7 Professional SP1 x64
 - Windows 7 Ultimate SP1 x86
 - Windows 7 Ultimate SP1 x64
 - Windows 7 Enterprise SP1 x86
 - Windows 7 Enterprise SP1 x64
- Семейство Windows 8:
 - Windows 8 Pro x86
 - Windows 8 Pro x64
 - Windows 8 Enterprise x86
 - Windows 8 Enterprise x64
- Семейство Windows 8.1:
 - Windows 8.1 Pro x86
 - Windows 8.1 Pro x64
 - Windows 8.1 Enterprise x86
 - Windows 8.1 Enterprise x64
- Семейство Windows 10:
 - Windows 10 Pro x86
 - Windows 10 Pro x64
 - Windows 10 Enterprise x86
 - Windows 10 Enterprise x64

- Windows 10 RS1 x86
- Windows 10 RS1 x64
- Windows 10 RS2 x86
- Windows 10 RS2 x64
- Windows 10 RS3 x64
- Windows 10 RS3 x64

Серверные операционные системы:

- Семейство Windows Server 2003:
 - Windows Server 2003 Standard SP1 x86
 - Windows Server 2003 Standard SP1 x64
 - Windows Server 2003 Enterprise SP1 x86
 - Windows Server 2003 Enterprise SP1 x64
 - Windows Server 2003 Standard SP2 x86
 - Windows Server 2003 Standard SP2 x64
 - Windows Server 2003 Enterprise SP2 x86
 - Windows Server 2003 Enterprise SP2 x64
- Семейство Windows Server 2008:
 - Windows Server 2008 Standard SP1 x86
 - Windows Server 2008 Standard SP1 x64
 - Windows Server 2008 Enterprise SP1 x86
 - Windows Server 2008 Enterprise SP1 x64
 - Windows Server 2008 R2 Standard
 - Windows Server 2008 R2 Enterprise
 - Windows Server 2008 R2 Enterprise with SP1
- Семейство Windows 2012:
 - Windows Server 2012 Essentials x64
 - Windows Server 2012 Standard x64
 - Windows Server 2012 Foundation x64
 - Windows Server 2012 Datacenter x64
 - Windows Server 2012 R2 Essentials x64
 - Windows Server 2012 R2 Standard x64
 - Windows Server 2012 R2 Foundation x64
 - Windows Server 2012 R2 Datacenter x64
- Windows Server 2016.

Встраиваемые системы:

- Windows XP Embedded x86
- Windows Embedded Standard 7 x86
- Windows Embedded Standard 7 x64
- Windows Embedded 8.1 Industry Pro x86
- Windows Embedded 8.1 Industry Pro x64
- Windows Embedded 8.0 Standard x86
- Windows Embedded 8.0 Standard x64

Поддерживаемые промышленные системы

Kaspersky Industrial CyberSecurity for Nodes 2.5 защищает следующие программируемые логические контроллеры:

- Siemens™ SIMATIC™ series S7-300
- Siemens SIMATIC series S7-400
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580

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 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 попыток 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.

Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA

Kaspersky Industrial CyberSecurity for Nodes 2.5 может передавать состояние безопасности автоматизированной системы управления технологическим процессом (далее "АСУ ТП") (сведения об обнаружении угроз) в Kaspersky Security Center. Если настроена передача сведений об угрозах в Kaspersky Security Center, вы можете настроить в SCADA-системе 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 установлен Kaspersky Industrial CyberSecurity for Nodes 2.5.

Информация о состоянии безопасности отобразится в панели результатов справа.

Статус компьютера с Kaspersky Industrial CyberSecurity for Nodes 2.5 отображает состояние безопасности АСУ ТП. Цвет значка компьютера соответствует одному из двух возможных состояний безопасности АСУ ТП:

- Зеленый: ОК. На компьютере с Kaspersky Industrial CyberSecurity for Nodes 2.5 нет неподтвержденных событий с критическим уровнем важности (инцидентов Kaspersky Security Center).
- Красный: критический. На компьютере с Kaspersky Industrial CyberSecurity for Nodes 2.5 есть неподтвержденные события с критическим уровнем важности (инциденты Kaspersky Security Center).

Просмотр состояния безопасности АСУ ТП через SCADA-систему

► Чтобы настроить получение и отображение состояния безопасности АСУ ТП в SCADA-систему, выполните следующие действия:

1. На компьютере с Kaspersky Security Center установите Kaspersky Security Gateway.

Вы можете найти подробную информацию об установке и настройке Kaspersky Security Gateway в документе *Руководство Администратора Kaspersky Security Gateway*.

2. В SCADA-системе создайте элемент управления, отображающий состояние компьютера с Kaspersky Industrial CyberSecurity for Nodes 2.5.

Способ настройки элемента управления описан в документе *Руководство Администратора Kaspersky Security Gateway*. В качестве протокола передачи данных укажите протокол OPC 2.0 DA.

Типовые схемы развертывания

Kaspersky Industrial CyberSecurity for Nodes 2.5 – это средство защиты узлов промышленной сети от угроз компьютерной безопасности, входящее в состав решения Kaspersky Industrial CyberSecurity.

Решение Kaspersky Industrial CyberSecurity включает в себя следующие программы:

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

Программы Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes 2.5 работают на разных уровнях *выделенной сети*. Выделенная сеть Kaspersky Industrial CyberSecurity - это часть промышленной сети, которая включает в себя компьютеры, предназначенные для работы программ защиты промышленных систем Kaspersky Industrial CyberSecurity и вспомогательного оборудования (например, коммутаторов). Программа Kaspersky Industrial CyberSecurity for Networks выполняет мониторинг и анализ трафика промышленной сети.

В ходе мониторинга трафика промышленной сети программа Kaspersky Industrial CyberSecurity for Networks учитывает обращения Kaspersky Industrial CyberSecurity for Nodes 2.5 к защищаемым программируемым логическим контроллерам (далее ПЛК), если эти ПЛК включены в область защиты Kaspersky Industrial CyberSecurity for Networks. Чтобы избежать ложных срабатываний при совместной работе Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes 2.5 в одной выделенной сети, выполните развертывание и настройку параметров Kaspersky Industrial CyberSecurity for Networks в соответствии с инструкциями Руководства пользователя Kaspersky Industrial CyberSecurity for Networks.

Вы можете управлять программами Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes 2.5, 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 2.5, из Kaspersky Security Center в SCADA-систему с помощью программы Kaspersky Security Gateway.

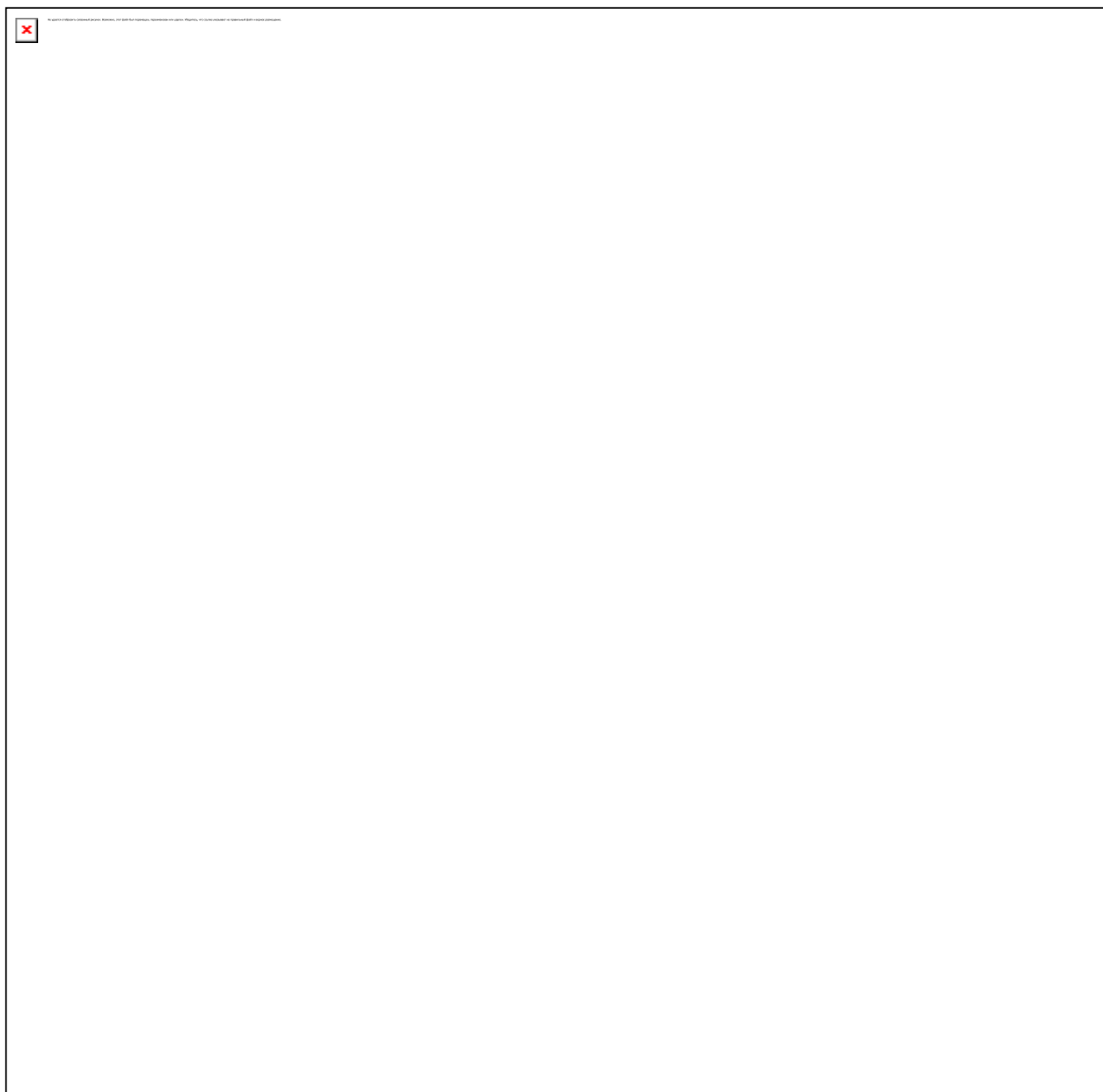
- Kaspersky Industrial CyberSecurity for Nodes 2.5 включает в себя следующие компоненты:
- *Функциональный модуль*. Этот компонент фиксирует информацию о состоянии узлов промышленной сети, а также выполняет защиту узлов от информационных угроз.
- *Консоль*. Этот компонент является локальным графическим интерфейсом пользователя. С помощью Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете управлять работой программы на узлах промышленной сети. Консоль может устанавливаться на компьютере с установленной программой Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5, с помощью одной Консоли.

Компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 разворачиваются как часть выделенной сети решения Kaspersky Industrial CyberSecurity.

Программа Kaspersky Industrial CyberSecurity for Nodes 2.5, установленная на узле промышленной сети, защищает компьютер от известных угроз компьютерной безопасности и контролирует целостность проектов ПЛК, включенных в область проверки. Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 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.



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.

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 Kaspersky Industrial CyberSecurity for Nodes 2.5 и управления им. В качестве средств администрирования Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете использовать Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, 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 2.5, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Industrial CyberSecurity for Nodes 2.5.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 входит в набор компонентов "Средства администрирования".

Утилита командной строки

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5.

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 2.5 через Консоль администрирования Kaspersky Security Center.

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 2.5. Он обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5, 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 2.5.** Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Industrial CyberSecurity for Nodes 2.5 через Сервер администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки плагина, \server\klcfginst.exe, входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes 2.5.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer.....	22
Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	26
Процессы Kaspersky Industrial CyberSecurity for Nodes 2.5	29
Параметры установки и удаления и их ключи для службы Windows Installer	30
Журнал установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5.....	37
Планирование установки	38
Установка и удаление программы с помощью мастера.....	41
Установка и удаление программы из командной строки.....	53
Установка и удаление программы через Kaspersky Security Center	59
Установка и удаление программы через групповые политики Active Directory.....	64
Проверка функций Kaspersky Industrial CyberSecurity for Nodes 2.5. Использование тестового вируса EICAR	67
Интерфейс программы	67

Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer

По умолчанию файлы \server\kics_x86(x64).msi устанавливают все программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете включить установку данного компонента при выборочной установке программы.

Файлы \client\kicstools_x86(x64).msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приводятся коды компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 для службы Windows Installer. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки.

В этом разделе

Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5.....	23
Программные компоненты набора "Средства администрирования"	25

Компоненты программы Kaspersky Industrial CyberSecurity for Nodes 2.5

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5.

Таблица 1. Описание программных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5

Компонент	Код	Выполняет функции
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.
Антивирусная защита	AVProtection	Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: <ul style="list-style-type: none"> Проверка по требованию Постоянная защита файлов
Проверка по требованию	Ods	Этот компонент устанавливает системные файлы Kaspersky Industrial CyberSecurity for Nodes 2.5 и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого компьютера, выполняемая по требованию).
Постоянная защита файлов	Oas	Этот компонент обеспечивает антивирусную проверку файлов на защищаемом компьютере при обращении к этим файлам. Компонент реализует задачу Постоянная защита файлов.
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 фиксировать операции, производимые над файлами в выбранной области мониторинга. Компонент реализуется в задаче Мониторинг файловых операций.
Защита от эксплойтов	AntiExploit	Этот компонент обеспечивает управление параметрами защиты процессов в памяти защищаемого компьютера.

Компонент	Код	Выполняет функции
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes 2.5 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	LogInspector	Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.
Защита от шифрования	AntiCryptor	Компонент защищает от вредоносного шифрования папки общего доступа на защищаемом компьютере.
Контроль Wi-Fi	WiFiControl	Этот компонент позволяет контролировать подключение защищаемого компьютера к сетям Wi-Fi.
Получение данных о проектах ПЛК	Plc	Этот компонент позволяет получать данные о проектах ПЛК, используемых в промышленной сети.
Проверка целостности проектов ПЛК	Plc	Этот компонент позволяет проверять целостность проектов ПЛК, используемых в промышленной сети.
Набор счетчиков производительности программы "Системный монитор"	PerfMonCounters	Компонент устанавливает набор счетчиков производительности программы "Системный монитор". Эти счетчики позволяют измерять производительность Kaspersky Industrial CyberSecurity for Nodes 2.5 и находить возможные узкие места при совместной работе Kaspersky Industrial CyberSecurity for Nodes 2.5 с другими программами.
Поддержка SNMP-протокола	SnmpSupport	Компонент публикует счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes 2.5 через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Вы можете установить этот компонент на защищаемом компьютере только в случае, если служба Microsoft SNMP установлена на этом компьютере.
Значок Kaspersky Industrial CyberSecurity for Nodes 2.5 в области уведомлений	TrayApp	Компонент отображает значок Kaspersky Industrial CyberSecurity for Nodes 2.5 в области уведомлений панели задач защищаемого компьютера. Значок Kaspersky Industrial CyberSecurity for Nodes 2.5 показывает состояние защиты компьютера, позволяет открыть Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 (если она установлена) и окно О программе.

Компонент	Код	Выполняет функции
Утилита командной строки	Shell	Позволяет управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки защищаемого компьютера.

Программные компоненты набора "Средства администрирования"

В следующей таблице содержатся коды и описание программных компонентов набора "Средства администрирования".

Таблица 2. Описание программных компонентов набора "Средства администрирования"

Компонент	Код	Функции компонента
Оснастка Kaspersky Industrial CyberSecurity for Nodes 2.5	MmcSnapin	Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5. Если, устанавливая набор "Средства администрирования" из командной строки, вы укажете другие компоненты набора, не указывая компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически.
Справка	Help	Chm-файл справки; сохраняется в папке с файлами средств администрирования Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете открыть файл справки из меню Пуск или по клавише F1 на открытом окне Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.
Документация	Help	Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет Руководство администратора и Руководство пользователя в формате PDF на защищаемом компьютере. Вы можете открыть Руководство администратора из меню Пуск .

Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes 2.5

При установке Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 (набора "Средства администрирования") служба Windows Installer выполняет на компьютере следующие изменения:

- создает папки Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере и компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5;
- регистрирует службы Kaspersky Industrial CyberSecurity for Nodes 2.5;
- создает группу пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5;
- регистрирует ключи Kaspersky Industrial CyberSecurity for Nodes 2.5 в системном реестре.

Эти изменения описаны в таблице ниже.

Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Таблица 3. Папки Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере

Папка	Документация Kaspersky Industrial CyberSecurity for Nodes 2.5
Папка %Kaspersky Industrial CyberSecurity for Nodes%; по умолчанию: в Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\ В Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Industrial CyberSecurity for Nodes\	Исполняемые файлы Kaspersky Industrial CyberSecurity for Nodes 2.5 (папка назначения, указанная при установке).
Папка %Kaspersky Industrial CyberSecurity for Nodes%\mibs	Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Kaspersky Industrial CyberSecurity for Nodes 2.5 по протоколу SNMP.
Папка %Kaspersky Industrial CyberSecurity for Nodes%\x64	64-разрядные версии исполняемых файлов Kaspersky Industrial CyberSecurity for Nodes 2.5 (папка создается только при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 в Microsoft Windows 64-разрядной версии).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Industrial CyberSecurity for Nodes\2.5\Dskm\	Служебные файлы Kaspersky Industrial CyberSecurity for Nodes 2.5.

Папка	Документация Kaspersky Industrial CyberSecurity for Nodes 2.5
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Update\	Файлы с параметрами источников обновлений.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Update\Distribution\	Обновления баз и программных модулей, полученные с помощью задачи Копирование обновлений (папка создается при первом получении обновлений с помощью задачи Копирование обновлений).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Reports\	Журналы выполнения задач и журнал системного аудита.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Bases\Current\	Набор баз, используемых в текущий момент.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Bases\Backup\	Резервная копия баз; перезаписывается при каждом обновлении баз.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Bases\Temp\	Временные файлы, создаваемые во время выполнения задач обновления.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Quarantine\	Объекты на карантине (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Backup\	Объекты в резервном хранилище (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Restored\	Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию).

Таблица 4. Папки, создаваемые при установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Папка	Документация Kaspersky Industrial CyberSecurity for Nodes 2.5
<p>Папка %Kaspersky Industrial CyberSecurity for Nodes 2.5%; по умолчанию:</p> <ul style="list-style-type: none"> 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\; 	Файлы набора "Средства администрирования" (папка назначения, указанная при установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5).

Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Службы Kaspersky Industrial CyberSecurity for Nodes 2.5 запускаются под системной учетной записью "Локальная система" (SYSTEM).

Таблица 5. Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Служба	Назначение
Служба Kaspersky Security (KAVFS)	Основная служба Kaspersky Industrial CyberSecurity for Nodes 2.5, которая управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5.
Служба Kaspersky Security Management (KAVFSGT)	Служба, предназначенная для управления программой через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Таблица 6. Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Группа	Назначение
KICS Administrators	Группа на защищаемом компьютере, пользователи которой имеют полный доступ к службе Kaspersky Security Management, а также доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

Ключи системного реестра

Таблица 7. Ключи системного реестра

Ключ	Назначение
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Параметры службы управления Kaspersky Industrial CyberSecurity for Nodes 2.5.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Параметры журнала событий Kaspersky Industrial CyberSecurity for Nodes 2.5 (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Параметры службы управления Kaspersky Industrial CyberSecurity for Nodes 2.5.
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]	Параметры счетчиков производительности.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Ключ	Назначение
В Microsoft Windows 64-разрядной версии: [[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\2.5\SnmpAgent] В Microsoft Windows 64-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.5\SnmpAgent]	Параметры компонента "Поддержка SNMP-протокола".
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KICS\2.5\CrashDump\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KICS\2.5\Crash Dump\ Dump\	Параметры записи файла дампа.
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KICS\2.5\Trace\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KICS\2.5\Trace \	Параметры журнала трассировки.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KICS\2.5\Environment]	Параметры задач и функций программы.

Процессы Kaspersky Industrial CyberSecurity for Nodes 2.5

Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает процессы, описанные в таблице ниже.

Таблица 8. Процессы Kaspersky Industrial CyberSecurity for Nodes 2.5

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Industrial CyberSecurity for Nodes 2.5
kavtray.exe	Процесс значка области уведомлений
kavshell.exe	Процесс утилиты командной строки
kavfsrpn.exe	Процесс удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5
kavfs.exe	Процесс службы Kaspersky Security
kavfsgt.exe	Процесс службы управления Kaspersky Security Management
kavfswh.exe	Процесс службы Kaspersky Security Exploit Prevention

Параметры установки и удаления и их ключи для службы Windows Installer

В следующих таблицах описаны параметры установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 и их значения по умолчанию, указаны ключи для изменения значений параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды msixexec службы Windows Installer при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки.

Таблица 9. Параметры установки и их ключи в Windows Installer

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Принятие условий Лицензионного соглашения	Отклонить условия Лицензионного соглашения	EULA=<значение> 0 – вы отклоняете условия Лицензионного соглашения. 1 – вы принимаете условия Лицензионного соглашения.	Вам нужно принять условия Лицензионного соглашения для установки Kaspersky Industrial CyberSecurity for Nodes 2.5.
Принятие Политики конфиденциальности	Отклонение Политики конфиденциальности	PRIVACYPOLICY=<значение> 0 – вы отклоняете условия Политики конфиденциальности. 1 – вы принимаете условия Политики конфиденциальности.	Вам нужно принять условия Политики конфиденциальности и для установки Kaspersky Industrial CyberSecurity for Nodes 2.5.
Папка назначения	Kaspersky Industrial CyberSecurity for Nodes 2.5: %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)%.	INSTALLDIR=<полный путь к папке>	Папка, в которой будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes 2.5 при его установке. Вы можете указать другую папку.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Запуск постоянной защиты файлов при запуске Kaspersky Industrial CyberSecurity for Nodes 2.5 (Включить постоянную защиту после установки программы)	Запустить	RUNRTP=<значение> 1 – запустить; 0 – не запускать.	Включите этот параметр, чтобы запустить постоянную защиту файлов при запуске Kaspersky Industrial CyberSecurity for Nodes 2.5 (рекомендуется).
Исключения из проверки, рекомендуемые корпорацией Microsoft (Добавить к исключениям файлы, рекомендованные Microsoft)	Исключать	ADDMSEXCLUSION=<значение> 1 – исключать; 0 – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на компьютере, которые рекомендует исключать корпорация Microsoft. Некоторые программы на компьютере могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, к которым эти программы обращаются. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Исключения из проверки, рекомендуемые "Лабораторией Касперского" (Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского")	Исключать	ADDKLEXCLUSION=<значение> 1 – исключать; 0 – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на компьютере, которые рекомендует исключать "Лаборатория Касперского".
Разрешить удаленное соединение для Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.	Не разрешать	ALLOWREMOTECON=<значение> 1 – разрешать; 0 – не разрешать.	По умолчанию удаленное подключение к Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной на защищаемом компьютере, не разрешено. Во время установки вы можете разрешить подключение. Kaspersky Industrial CyberSecurity for Nodes 2.5 создаст разрешающие правила для процесса kavfsgr.exe по протоколу TCP для всех портов.
Путь к файлу ключа (Ключ)	Папка комплекта поставки \server	LICENSEKEYPATH=<имя файла ключа>	По умолчанию программа установки пытается найти файл с расширением .key в папке \server комплекта поставки.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
			<p>Если в папке \server хранится несколько файлов ключа, программа установки выбирает файл ключа с самым поздней датой истечения срока действия.</p> <p>Вы можете предварительно сохранить файл ключа в папке \server или указать другой путь к файлу ключа с помощью параметра Добавление ключа.</p> <p>Вы можете добавить ключ после установки Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью выбранного вами средства администрирования, например, через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5. Если вы не добавите ключ программы во время его установки, после установки Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет функционировать.</p>

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Путь к конфигурационному файлу	Не указан	CONFIGPATH=<имя конфигурационного файла>	<p>Kaspersky Industrial CyberSecurity for Nodes 2.5 импортирует параметры из указанного конфигурационного файла, созданного в программе.</p> <p>Kaspersky Industrial CyberSecurity for Nodes 2.5 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.</p> <p>Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.</p>
Разрешение сетевых соединений для Консоли	Выключено	ADDWFEXCLUSION=<значение> 1 – разрешать; 0 – не разрешать.	<p>Используйте этот параметр, если вы устанавливаете Kaspersky Industrial CyberSecurity for Nodes 2.5 не на защищаемом компьютере. Вы можете удаленно управлять защитой компьютера с другого устройства, на котором установлена</p>

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
			<p>Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.</p> <p>В брандмауэре Microsoft Windows компьютера будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5 kavfsrcn.exe и открыт доступ к программам DCOM.</p> <p>После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу KICS Administrators на компьютере и разрешите на нем сетевые соединения для службы Kaspersky Security Managment (файл kavfsgt.exe).</p>

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
			Вы можете подробнее прочитать о дополнительной настройке при установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере (см. раздел "Дополнительная настройка после установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере" на стр. 45).
Отключение проверки на наличие несовместимого программного обеспечения	Проверка выполняется	SKIPINCOMPATIBLESW = <значение> 0 - выполняется проверка на несовместимое программное обеспечение 1 - проверка на наличие несовместимого программного обеспечения не выполняется	<p>Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на устройство в фоновом режиме.</p> <p>Независимо от значения данного параметра, при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 программа всегда предупреждает о других версиях программы, установленных на этом же устройстве.</p>

Таблица 10. Параметры удаления и их ключи в Windows Installer

Параметр	Значение по умолчанию	Описание, ключи Windows Installer и их значения
Восстановление содержимого карантина	Удалить	RESTOREQTN =<значение> 0 – удалить содержимое карантина; 1 – восстановить содержимое карантина в папку, указанную параметром RESTOREPATH.
Восстановление содержимого резервного хранилища	Удалить	RESTOREBCK =<значение> 0 – удалить содержимое резервного хранилища; 1 – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH.
Ввод текущего пароля для подтверждения операции удаления (при активной функции применения пароля)	Не указан	UNLOCK_PASSWORD=<заданный пароль>
Папка для восстановленных объектов	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Restored	RESTOREPATH=<полный путь к папке> Восстановленные объекты будут сохранены в папке, указанной этим параметром: Объекты из карантина будут сохранены во вложенной папке \Quarantine. Объекты из резервного хранилища – во вложенной папке \Backup.

Журнал установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5

Если вы выполняете установку или удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью мастера установки (удаления), служба Windows Installer создает журнал установки (удаления). Файл журнала с именем kics_install_<uid>.log (где <uid> – уникальный восьмизначный идентификатор журнала) сохраняется в папке %temp% пользователя, с правами которого был запущен мастер установки.

Если вы выполняете установку или удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки, по умолчанию журнал установки не создается.

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с созданием файла журнала *kics.log* на диске C:\, выполните одну из следующих команд:

- `msiexec /i kics_x86.msi /l*v C:\log.txt /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i kics_x64.msi /l*v C:\log.txt /qn EULA=1 PRIVACYPOLICY=1`

Планирование установки

Этот раздел содержит описание средств администрирования Kaspersky Industrial CyberSecurity for Nodes 2.5, особенностей установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. [41](#)), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. [53](#)), через Kaspersky Security Center (см. раздел "Установка и удаление программы через Kaspersky Security Center" на стр. [59](#)) и через групповые политики Active Directory® (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. [64](#)).

Перед тем как начать установку Kaspersky Industrial CyberSecurity for Nodes 2.5, спланируйте основные этапы ее проведения:

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Industrial CyberSecurity for Nodes 2.5 и его настройки.
2. Определите, какие программные компоненты требуется установить (см. раздел "Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer" на стр. [22](#)).
3. Выберите способ установки.

В этом разделе

Выбор средств администрирования	38
Выбор способа установки	39

Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров Kaspersky Industrial CyberSecurity for Nodes 2.5 и управления им. В качестве средств администрирования Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете использовать Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на защищаемом компьютере или на другом компьютере в сети организации.

В одну Консоль Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток Kaspersky Industrial CyberSecurity for Nodes 2.5, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Industrial CyberSecurity for Nodes 2.5.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 входит в набор компонентов "Средства администрирования".

Утилита командной строки

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5.

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 2.5 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 2.5. Он обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5, 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 2.5.** Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Industrial CyberSecurity for Nodes 2.5 через Сервер администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки плагина управления \server\klcginst.exe входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes 2.5.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer" на стр. [22](#)) вам нужно 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 2.5 или вы будете использовать параметры установки по умолчанию (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [30](#));
- будут ли параметры установки едиными для всех компьютеров или индивидуальными для каждого компьютера.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5 как с помощью мастера установки, так и в режиме без взаимодействия с пользователем, указав параметры установки в командной строке. Вы можете выполнить централизованную удаленную установку Kaspersky Industrial CyberSecurity for Nodes 2.5: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5 на одном компьютере, настроить его для работы и сохранить его параметры в конфигурационном файле, чтобы затем использовать созданный файл для установки Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере (эта возможность не применяется при установке через групповые политики Active Directory).

Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 23) на защищаемом компьютере из файла `\server\setup.exe` включены в комплект поставки.
- Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 44) из файла `\client\setup.exe`, входящего в комплект поставки на защищаемом компьютере или другом компьютере в локальной сети.

Запуск из командной строки файла инсталляционного пакета с параметрами установки

Запустив файл инсталляционного пакета без ключей, вы установите Kaspersky Industrial CyberSecurity for Nodes 2.5 с параметрами установки по умолчанию. С помощью ключей Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете изменять параметры установки.

Вы можете установить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере и (или) на рабочем месте администратора.

Примеры команд для установки Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 приведены в разделе "Установка и удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки" (см. раздел "Установка и удаление программы из командной строки" на стр. 53).

Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой компьютеров сети, вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5 на нескольких компьютерах с помощью задачи удаленной установки Kaspersky Security Center.

Компьютеры, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. 59), могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене или вообще не принадлежать ни одному домену.

Централизованная установка через групповые политики Active Directory

С помощью групповых политик Active Directory вы можете устанавливать Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере. Вы также можете устанавливать Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере или рабочем месте администратора.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5, используя лишь параметры установки по умолчанию.

Компьютеры, на которых Kaspersky Industrial CyberSecurity for Nodes 2.5 установлен с помощью групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 64), должны быть расположены в том же домене и в том же подразделении организации. Установка выполняется при запуске компьютера, перед входом в Microsoft Windows.

Установка и удаление программы с помощью мастера

Этот раздел содержит описание процедуры установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоли программы на защищаемом компьютере с помощью мастера установки, а также информацию о дополнительной настройке Kaspersky Industrial CyberSecurity for Nodes 2.5 и действиях после установки программы.

В этом разделе

Установка с помощью мастера установки	41
Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes 2.5	50
Удаление с помощью мастера установки.....	51

Установка с помощью мастера установки

В следующих разделах содержится информация о том, как установить Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

► *Чтобы установить и приступить к использованию Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

3. Установите Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере.
4. На компьютерах, с которых вы планируете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5, установите Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
5. Если вы установили Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку, чтобы пользователи Консоли могли через нее удаленно управлять Kaspersky Industrial CyberSecurity for Nodes 2.5.
6. Выполните действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5	42
Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5	44
Дополнительная настройка после установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере	45

Установка Kaspersky Industrial CyberSecurity for Nodes 2.5

Перед установкой Kaspersky Industrial CyberSecurity for Nodes 2.5 выполните следующие действия:

- Убедитесь, что на компьютере не установлены другие антивирусные программы.
- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, зарегистрирована в группе 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 2.5. Вы можете прервать установку Kaspersky Industrial CyberSecurity for Nodes 2.5 на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Вы можете прочитать подробнее о параметрах установки (удаления) (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [30](#)).

► Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью мастера установки, выполните следующие действия:

1. На компьютере запустите файл программы-приветствия setup.exe.
2. В открывшемся окне в блоке Установка перейдите по ссылке **Установить Kaspersky Industrial CyberSecurity for Nodes 2.5**.
3. В открывшемся окне приветствия мастера установки Kaspersky Industrial CyberSecurity for Nodes 2.5 нажмите на кнопку **Далее**.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы прочли Лицензионное соглашение и Политику конфиденциальности, для продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения и Политику конфиденциальности, которая описывает обработку данных**.

Если вы не принимаете Лицензионное соглашение и Политику конфиденциальности, установка будет прервана.

6. Нажмите на кнопку **Далее**.
Откроется окно **Быстрая проверка перед началом установки**.
7. В окне **Быстрая проверка перед началом установки** установите флажок **Проверить компьютер на вирусы**, чтобы проверить на наличие угроз загрузочные секторы локальных дисков компьютера и системную память. Затем нажмите на кнопку **Далее**. По окончании проверки откроется окно с результатами проверки.

Вы можете просмотреть информацию о проверенных объектах на компьютере: общее количество проверенных объектов, количество обнаруженных типов угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или подозрительных процессов,

которые Kaspersky Industrial CyberSecurity for Nodes 2.5 удалил из памяти, и количество опасных или подозрительных процессов, которые программе не удалось удалить.

Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

8. В окне **Быстрая проверка перед началом установки** нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

9. Выберите компоненты, которые вы хотите установить.

По умолчанию в список устанавливаемых объектов включены все компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5, за исключением компонента Управление сетевым экраном.

Для установки программы в сертифицированной конфигурации снимите флажки для компонентов Контроль устройств и Управление сетевым экраном

Компонент Поддержка SNMP-протокола Kaspersky Industrial CyberSecurity for Nodes 2.5 отображается в списке устанавливаемых компонентов только в случае, если на компьютере установлена Служба SNMP Microsoft Windows.

10. Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.

11. В открывшемся окне **Выбор папки назначения** выполните следующие действия:

- Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes 2.5.
- Если требуется, просмотрите информацию о доступном пространстве на локальных жестких дисках по кнопке **Диск**.

Нажмите на кнопку **Далее**.

12. В открывшемся окне **Дополнительные параметры установки** настройте следующие параметры установки:

- **Включить постоянную защиту после установки программы.**
- **Добавить к исключениям файлы, рекомендованные Microsoft.**
- **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского".**

Нажмите на кнопку **Далее**.

13. В открывшемся окне **Импорт параметров из конфигурационного файла** выполните следующие действия:

- a. Если вы хотите импортировать параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.
- b. Затем нажмите на кнопку **Далее**.

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

- Если вы хотите активировать программу, укажите файл ключа Kaspersky Industrial CyberSecurity for Nodes 2.5 для активации программы.

- Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
- Если вы предварительно сохранили файл ключа в папке \server комплекта поставки, имя этого файла отобразится в поле **Ключ**.

Если вы хотите добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

После добавления файла ключа в окне отобразится информация о лицензии. Kaspersky Industrial CyberSecurity for Nodes 2.5 отображает расчетную дату окончания срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, но истекает не позднее истечения срока годности файла ключа.

Нажмите на кнопку **Далее**, чтобы применить ключ в программе.

15. В открывшемся окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5.
16. По завершении установки откроется окно **Установка завершена**.
17. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о выпуске после завершения работы мастера установки.
18. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. По завершении установки Kaspersky Industrial CyberSecurity for Nodes 2.5 будет готов к работе, если вы добавили ключ для активации программы.

Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Следуя инструкциям мастера установки, задайте параметры установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

► Чтобы установить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на компьютере.
2. Запустите файл приветствия setup.exe на компьютере.
Откроется окно программы-приветствия.
3. Нажмите на ссылку **Установить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5**.
Откроется окно приветствия мастера установки. Нажмите на кнопку **Далее**.
4. Просмотрите условия Лицензионного соглашения и Политики конфиденциальности в открывшемся окне и для продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения и Политику конфиденциальности, которая описывает обработку данных**. Нажмите на кнопку **Далее**.
Откроется окно **Дополнительные параметры установки**.
5. В открывшемся окне **Дополнительные параметры установки** выполните следующие действия:

- Если вы планируете с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 управлять Kaspersky Industrial CyberSecurity for Nodes 2.5, установленным на удаленном компьютере, установите флажок **Разрешить удаленный доступ**.
- Чтобы открыть окно **Пользовательская установка** и выбрать компоненты, выполните следующие действия:
 - a. Нажмите на кнопку **Дополнительно**.
Откроется окно **Выборочная установка**.
 - b. Выберите компоненты набора средств администрирования из списка.
По умолчанию устанавливаются все компоненты.
 - c. Нажмите на кнопку **Далее**.

Вы можете прочитать подробнее о компонентах Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Программные компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5 и их коды для службы Windows Installer" на стр. [22](#)).

6. В открывшемся окне **Выбор папки назначения** выполните следующие действия:
 - a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
 - b. Нажмите на кнопку **Далее**.
7. В открывшемся окне **Готовность к установке** нажмите на кнопку **Установить**.
Мастер приступит к установке выбранных компонентов.
8. Нажмите на кнопку **ОК**.
Окно мастера установки будет закрыто. Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 будет установлена на защищаемый компьютер.

Если вы установили набор "Средства администрирования" не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере" на стр. [45](#)).

Дополнительная настройка после установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере

Если вы установили Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 не на защищаемом компьютере, а на другом компьютере сети, выполните описанные ниже действия для того, чтобы пользователи могли удаленно управлять Kaspersky Industrial CyberSecurity for Nodes 2.5:

- На защищаемом компьютере добавьте пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5 в группу KICS Administrators.
- Разрешать сетевые соединения для службы Kaspersky Security Management (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. [81](#)), если на защищаемом компьютере используется сетевой экран Windows или сетевой экран стороннего поставщика.
- Если при установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютере под управлением Microsoft Windows вы не установили флажок **Разрешить удаленный доступ**, разрешите сетевые соединения для Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вручную через брандмауэр на этом компьютере.

Разрешение сетевых соединений для Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Названия параметров могут отличаться в разных операционных системах Windows.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на удаленном компьютере использует протокол DCOM, чтобы получать информацию о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5, например о проверенных объектах или завершении задач, от службы Kaspersky Security Management на защищаемом компьютере. Вам нужно разрешить сетевые соединения в настройках брандмауэра Windows для Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, чтобы устанавливать соединения между Консолью Kaspersky Industrial CyberSecurity for Nodes 2.5 и службой Kaspersky Security Management.

Выполните следующие действия:

- убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск или активация программ COM);
- в брандмауэре Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5 kavfsrcn.exe.

Через порт TCP 135 клиентский компьютер, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, обменивается информацией с защищаемым компьютером.

Если Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 открыта во время настройки параметров соединения между защищаемым компьютером и компьютером, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, вам нужно закрыть Консоль программы, дождаться завершения процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5 kavfsrcn.exe и снова запустить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5. Новые параметры соединения будут применены.

► Чтобы разрешить анонимный удаленный доступ к программам COM, выполните следующие действия:

1. На компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, откройте консоль Службы компонентов.
2. Выберите **Пуск > Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **ОК**.
5. В консоли **Службы компонентов** компьютера разверните узел **Компьютеры**.
6. Откройте контекстное меню на узле **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в группе параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

10. Нажмите на кнопку **ОК**.

► Чтобы открыть в брандмауэре Windows TCP-порт 135 и разрешить сетевые соединения для процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. На удаленном компьютере закройте Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
2. Выполните одно из следующих действий:
 - В Microsoft Windows XP или Microsoft Windows Vista:
 - a. В Microsoft Windows XP с пакетом обновлений 2 или выше выберите **Пуск > Брандмауэр Windows**.
В Microsoft Windows Vista выберите **Пуск > Панель управления > Брандмауэр Windows** и в окне **Брандмауэр Windows** выберите пункт **Изменить параметры**.
 - b. В окне Брандмауэр Windows (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 2.5, в поле **Номер порта** укажите номер порта: 135.
 - d. Выберите протокол **TCP**.
 - e. Нажмите на кнопку **ОК**.
 - f. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
 - В Microsoft Windows 7 и выше:
 - a. Выберите пункт **Пуск > Панель управления > Брандмауэр Windows**. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
 - b. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.
3. В окне **Добавление программы** укажите файл kavfsrqn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью консоли Microsoft Management Console.
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5

Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Industrial CyberSecurity for Nodes 2.5 был выбран пункт **Включить постоянную защиту после установки программы** (настройка по умолчанию), Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет задачу Проверка важных областей.

После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты с использованием баз, которые входили в состав программы при поставке.

Рекомендуется сразу же обновить базы Kaspersky Industrial CyberSecurity for Nodes 2.5, так как базы могли устареть.

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

- Выполнить проверку важных областей компьютера, если перед установкой Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Запуск и настройка задачи обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5.....	48
Проверка важных областей	50

Запуск и настройка задачи обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5

► Чтобы обновить базы программы после установки, выполните следующие действия:

1. В свойствах задачи Обновление баз программы настройте соединение с источником обновлений – HTTP- или FTP-серверами обновлений "Лаборатории Касперского".
2. Запустите задачу Обновление баз программы.

► Чтобы настроить соединение с серверами обновлений "Лаборатории Касперского" в задаче Обновление баз программы, выполните следующие действия:

1. Запустите Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 одним из следующих способов:
 - Откройте Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере. Для этого выберите **Пуск > Все Программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Средства администрирования > Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5**.
 - Если вы запустили Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 не на защищаемом компьютере, подключитесь к защищаемому компьютеру:
 - с. Откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes 2.5** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.
 - d. Выберите пункт **Подключиться к другому компьютеру**.
 - e. В диалоговом окне **Выбор компьютера** выберите вариант **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого компьютера.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

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. 81), укажите учетную запись, которая обладает этими правами.

Откроется окно Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

2. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
3. Выберите вложенный узел **Обновление баз программы**.
4. В панели результатов перейдите по ссылке **Свойства**.
5. В открывшемся окне **Параметры задачи** откройте закладку **Параметры соединения**.
6. Выполните следующие действия:
 - a. Если в вашей сети не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети, укажите параметры прокси-сервера: в блоке **Параметры прокси-сервера** установите флажок **Использовать параметры указанного прокси-сервера**, в поле **Адрес** введите адрес, а в поле **Порт** – номер порта прокси-сервера.
 - b. Если в вашей сети требуется проверка подлинности при доступе к прокси-серверу, выберите нужный метод проверки подлинности в раскрывающемся списке блока **Параметры аутентификации на прокси-сервере**:
 - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows (NTLM authentication). Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи (по умолчанию задача выполнится под учетной записью **Локальная система {SYSTEM}**).
 - **Использовать NTLM-аутентификацию с именем и паролем**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать для доступа к прокси-серверу учетную запись, указанную вами. Введите имя и пароль пользователя или выберите пользователя в списке.
 - **Использовать имя и пароль пользователя**, чтобы выбрать обычную проверку подлинности (Basic authentication). Введите имя и пароль пользователя или выберите пользователя в списке.

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

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 Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5**.

Проверка важных областей

После того как вы обновили базы Kaspersky Industrial CyberSecurity for Nodes 2.5, проверьте компьютер на наличие вредоносных программ с помощью задачи "Проверка важных областей".

► Чтобы запустить задачу Проверка важных областей, выполните следующие действия:

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. В контекстном меню вложенного узла **Проверка важных областей** выберите команду **Запустить**.

Задача будет запущена; в рабочей области 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 2.5

Вы можете добавлять или удалять компоненты Kaspersky Industrial CyberSecurity for Nodes 2.5. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу постоянной защиты или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге мастера.

► Чтобы изменить состав компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Изменение или удаление**.

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

2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

3. В окне **Выборочная установка** в списке компонентов, доступных для использования, выберите компоненты, которые вы хотите добавить в Kaspersky Industrial CyberSecurity for Nodes 2.5 или удалить. Для этого выполните следующие действия:

- Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента и в контекстном меню выберите:
 - пункт **Компонент будет установлен на локальный жесткий диск**, если хотите установить один компонент;

- пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если хотите установить группу компонентов.
- Чтобы удалить ранее установленные компоненты, нажмите на кнопку рядом с названием выбранного компонента и в контекстном меню выберите пункт **Компонент будет недоступен**.

Нажмите на кнопку **Установить**.

4. В окне **Готовность к установке** подтвердите операцию изменения 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 2.5 будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Industrial CyberSecurity for Nodes 2.5 возникли проблемы (Kaspersky Industrial CyberSecurity for Nodes 2.5 завершается аварийно; задачи завершаются аварийно или не запускаются), вы можете попробовать восстановить Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете выполнить восстановление, сохранив текущие значения параметров Kaspersky Industrial CyberSecurity for Nodes 2.5, или выбрать режим, при котором все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Industrial CyberSecurity for Nodes 2.5 после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Изменение или удаление**.

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

2. Выберите пункт **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

Откроется окно **Восстановление установленных компонентов**.

3. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если хотите сбросить настроенные параметры программы и восстановить Kaspersky Industrial CyberSecurity for Nodes 2.5 с предустановленными параметрами по умолчанию. Нажмите на кнопку **Установить**.
4. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
5. В окне, открывшемся по завершении восстановления, нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет восстановлен в соответствии с заданными параметрами.

Удаление с помощью мастера установки

Этот раздел содержит инструкции для удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 с защищаемого компьютера с помощью мастера установки.

В этом разделе

Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 [52](#)

Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5	53
---	----

Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 с защищаемого компьютера с помощью мастера установки / удаления.

После удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 может потребоваться перезагрузка компьютера. Вы можете отложить перезагрузку.

Удаление, восстановление и добавление программы через панель управления Windows невозможны, если операционная система использует функцию Контроль учетных записей пользователя (User Account Control), или доступ к управлению программой защищен паролем.

Если доступ к управлению программой защищен паролем, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге мастера.

► Чтобы удалить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Изменение или удаление**.

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

2. Выберите пункт **Удаление компонентов программы**. Нажмите на кнопку **Далее**.

Откроется окно **Дополнительные параметры удаления программы**.

3. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:
 - a. Установите флажок **Экспортировать объекты на карантин**, чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 экспортировал объекты, помещенные на карантин. По умолчанию флажок снят.
 - b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 экспортировал объекты из резервного хранилища. По умолчанию флажок снят.
 - c. Нажмите на кнопку **Сохранить** и укажите папку, в которую вы хотите экспортировать восстановленные объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Uninstall.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Нажмите на кнопку **Далее**.

4. В окне **Готовность к удалению** подтвердите операцию удаления, нажав на кнопку **Удалить**.
5. В окне, открывшемся по завершении удаления, нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет удален с защищаемого компьютера.

Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с компьютера с помощью мастера установки / удаления.

После удаления Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 перезагрузка компьютера не требуется.

► Чтобы удалить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Средства администрирования > Изменение или удаление**.
2. Откроется окно мастера **Изменение, восстановление или удаление**.
Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.
3. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.
Откроется окно **Удаление завершено**.
4. Нажмите на кнопку **ОК**.

Операция удаления будет завершена; окно мастера будет закрыто.

Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки, примеры команд для установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки.

В этом разделе

Об установке и удалении Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки	54
Примеры команд для установки Kaspersky Industrial CyberSecurity for Nodes 2.5	54
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	56

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Добавление и удаление компонентов.Примеры команд.....	57
Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5. Примеры команд	58
Коды возврата	58

Об установке и удалении Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки

Вы можете устанавливать и удалять Kaspersky Industrial CyberSecurity for Nodes 2.5, добавлять или удалять его компоненты, запустив из командной строки файлы инсталляционного пакета `\product\kics_x86(x64).msi`, указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом компьютере или другом компьютере в сети, чтобы работать с Консолью Kaspersky Industrial CyberSecurity for Nodes 2.5 локально или удаленно. Для этого используйте инсталляционный пакет `\client\kicstools.msi`.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на компьютере, на котором вы выполняете установку.

Если вы запустите на защищаемом компьютере один из файлов `\product\kics_x86(x64).msi` без дополнительных ключей, Kaspersky Industrial CyberSecurity for Nodes 2.5 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.

Примеры команд установки Kaspersky Industrial CyberSecurity for Nodes 2.5

В этом разделе приводятся примеры команд для установки Kaspersky Industrial CyberSecurity for Nodes 2.5.

На компьютере под управлением Microsoft Windows 32-разрядной версии запускайте файлы с суффиксом `x86` комплекта поставки. На компьютере под управлением Microsoft Windows 64-разрядной версии запускайте файлы с суффиксом `x64` комплекта поставки.

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

Примеры установки Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью файла setup.exe

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с параметрами установки по умолчанию в режиме без взаимодействия с пользователем, выполните следующую команду:

```
\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 со следующими параметрами:

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать постоянную защиту при запуске Kaspersky Industrial CyberSecurity for Nodes 2.5;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

выполните следующую команду:

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Примеры команд для установки: запуск msi-файла инсталляционного пакета

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с параметрами установки по умолчанию в режиме без взаимодействия с пользователем, выполните следующую команду:

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

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с параметрами установки по умолчанию; показать интерфейс установки, выполните следующую команду:

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

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с активацией с помощью файла ключа C:\0000000A.key:

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

- Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 с предварительной проверкой активных процессов и загрузочных секторов локальных дисков компьютера, выполните следующую команду:

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


- Чтобы установить *Kaspersky Industrial CyberSecurity for Nodes 2.5*, сохранив его файлы в папке назначения *C:\KICS*, выполните следующую команду:

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

- Чтобы установить *Kaspersky Industrial CyberSecurity for Nodes 2.5*; сохранить файл журнала установки с именем *kics.log* в папке, в которой хранится *msi*-файл инсталляционного пакета *Kaspersky Industrial CyberSecurity for Nodes 2.5*, выполните следующую команду:

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

- Чтобы установить Консоль *Kaspersky Industrial CyberSecurity for Nodes 2.5*, выполните следующую команду:

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

- Чтобы установить *Kaspersky Industrial CyberSecurity for Nodes 2.5* с активацией с помощью файла ключа *C:\0000000A.key*; настроить *Kaspersky Industrial CyberSecurity for Nodes 2.5* в соответствии с параметрами, описанными 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 программы, когда *Kaspersky Industrial CyberSecurity for Nodes 2.5* защищен паролем, выполните следующую команду:

```
msiexec /p "<msp путь к имени файла>" UNLOCK_PASSWORD=<пароль>
```

Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5

Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Industrial CyberSecurity for Nodes 2.5 вы выбрали пункт **Включить постоянную защиту после установки программы**, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет задачу "Проверка важных областей".

После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Industrial CyberSecurity for Nodes 2.5. 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:

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.


```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

При этом обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 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 проверки подлинности Microsoft Windows (NTLM-authentication) под учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить проверку важных областей компьютера, если перед установкой Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере не было установлено антивирусной программы 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 2.5.

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 2.5.

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

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

или

```
\server\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Если вы укажете не только компоненты, которые хотите установить, но и уже установленные компоненты, Kaspersky Industrial CyberSecurity for Nodes 2.5 переустановит указанные установленные компоненты.

► *Чтобы удалить установленные компоненты, выполните следующую команду:*

```
msiexec /i kics_x64.msi "ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,
Firewall,AntiCryptor,Plc,Fim,LogInspector,AKIntegration,PerfMonCounters,Sn
mpSupport,Shell,TrayApp,AVProtection,RamDisk REMOVE=AppCtrl,WiFiControl"
/qn
```

Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Примеры команд

- Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 с защищаемого компьютера, выполните следующую команду:

```
msiexec /x kics.msi /qn
```

или

- Для x32-разрядной операционной системы:

```
msiexec /x {98973F3A-3B19-431E-A1FF-FEF92FD2DD3E} /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {1946CA6C-94EF-427B-8210-AF3E84E18E03} /qn
```

- Чтобы удалить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующую команду:

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

или

- Для x32-разрядной операционной системы:

```
msiexec /x {AEC4DA78-ED59-496D-9B10-67C0334545CC} /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {A81A10C2-AD3E-4069-8C1F-D95F4B7B258F} /qn
```

- Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 с защищаемого компьютера, на котором установлен пароль, выполните следующую команду:

- Для x32-разрядной операционной системы:

```
msiexec /x {98973F3A-3B19-431E-A1FF-FEF92FD2DD3E} UNLOCK_PASSWORD=*** /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {1946CA6C-94EF-427B-8210-AF3E84E18E03} UNLOCK_PASSWORD=*** /qn
```

- Чтобы удалить Плагин управления Kaspersky Industrial CyberSecurity for Nodes 2.5 с защищаемого компьютера, выполните следующую команду:

```
msiexec.exe /x {5479FADB-700D-49EA-980D-40B8F603E7CB} /qn
```

Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

Таблица 11. Коды возврата

Код	Описание
1324	Имя папки назначения содержит недопустимые символы.
25001	Недостаточно прав для установки Kaspersky Industrial CyberSecurity for Nodes 2.5. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Kaspersky Industrial CyberSecurity for Nodes 2.5 не может быть установлен на компьютер 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 и удаление программы через Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center, а также описание действий после установки Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Общие сведения об установке через Kaspersky Security Center	60
Права для установки или удаления Kaspersky Industrial CyberSecurity for Nodes 2.5	60
Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center	61
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	63
Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center	63

Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки Kaspersky Industrial CyberSecurity for Nodes 2.5 будет установлен с одинаковыми параметрами на нескольких компьютерах.

Вы можете объединить все компьютеры в одну группу администрирования и создать групповую задачу для установки Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютеры этой группы.

Вы можете создать задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes 2.5 для набора компьютеров, не объединенных в одну группу администрирования. При ее создании вам нужно сформировать список отдельных компьютеров, на которые требуется установить Kaspersky Industrial CyberSecurity for Nodes 2.5.

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

Права для установки или удаления Kaspersky Industrial CyberSecurity for Nodes 2.5

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

- На компьютерах, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes 2.5, уже установлен Агент администрирования Kaspersky Security Center (независимо от того, в каком домене находятся компьютеры и принадлежат ли они к какому-либо домену).

Если Агент администрирования еще не установлен на компьютерах, вы можете установить его вместе с Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом из компьютеров.

- Все компьютеры, на которые вы хотите установить Kaspersky Industrial CyberSecurity for Nodes 2.5, находятся в одном домене с Сервером администрирования, и Сервер администрирования зарегистрирован под учетной записью "Администратор домена" (**Domain Admin**) (если эта учетная запись обладает правами администратора на компьютерах домена).

По умолчанию задача удаленной установки методом **Форсированная установка** выполняется под учетной записью, с правами которой работает Сервер администрирования.

В групповых задачах, а также в тех задачах для набора компьютеров, в которых был выбран метод форсированной установки (удаления), учетная запись должна обладать следующими правами на клиентском компьютере:

- правом на удаленный запуск программ;
- правами на ресурс **Admin\$**;

- правом **Вход в качестве службы**.

Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center

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

Если вы планируете в дальнейшем управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На компьютере с установленным Сервером администрирования Kaspersky Security Center также установлен плагин управления Kaspersky Industrial CyberSecurity for Nodes 2.5 (файл `server\klcfginst.exe` комплекта поставки Kaspersky Industrial CyberSecurity for Nodes 2.5).
- 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 2.5 в задаче удаленной установки.

Вы также можете предварительно объединить компьютеры 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 2.5 с помощью задачи удаленной установки, выполните следующие действия:

1. запустить утилиту Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
3. Введите имя инсталляционного пакета.
4. Выберите файл `kics.kud` из комплекта поставки Kaspersky Industrial CyberSecurity for Nodes 2.5 в качестве файла инсталляционного пакета.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

5. Если вы прочли Лицензионное соглашение и Политику конфиденциальности, для продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения и Политику конфиденциальности, которая описывает обработку данных**.

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

6. Чтобы изменить набор устанавливаемых компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 (см.раздел "Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. [50](#)) и настройки установки по умолчанию (см.раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [30](#)) в установочном пакете, выполните следующие действия:
 - a. В Kaspersky Security Center разверните узел **Удаленная установка**.
 - b. Во вложенном узле **Инсталляционные пакеты** в рабочей области откройте контекстное меню созданного установочного пакета Kaspersky Industrial CyberSecurity for Nodes 2.5 и выберите команду **Свойства**.
 - c. В окне **Свойства: <название инсталляционного пакета>** в разделе **Настройка** выполните следующие действия:
 - a. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5, которые вы хотите установить.

Для установки программы в сертифицированной конфигурации снимите флажки для компонентов **Контроль устройств** и **Управление сетевым экраном**

 - b. 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 компьютере, она будет создана.
 - c. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:
 - Выполнить антивирусную проверку компьютера перед началом установки.
 - Включить постоянную защиту после установки программы.
 - Добавить к исключениям файлы, рекомендованные Microsoft.
 - d. Учесть исключения, рекомендованные «Лабораторией Касперского».
 - d. В окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.
7. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes 2.5 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.
 Подробная информация о создании и настройке задачи удаленной установки содержится в *справке Kaspersky Security Center*.
8. Запустите созданную задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes 2.5. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет установлен на указанные в задаче компьютеры.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5

После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 рекомендуется обновить базы Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах, а также выполнить проверку важных областей компьютеров, если до установки Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если компьютеры, на которых вы установили Kaspersky Industrial CyberSecurity for Nodes 2.5, объединены в одной группе администрирования Kaspersky Security Center, вы можете выполнить эти задачи следующими способами:

1. Создать задачу обновления баз программы для группы компьютеров, на которых вы установили Kaspersky Industrial CyberSecurity for Nodes 2.5. Установить в качестве источника обновлений Сервер администрирования Kaspersky Security Center.
2. Создать групповую задачу проверки по требованию со статусом Задача проверки важных областей. Программа Kaspersky Security Center будет оценивать состояние безопасности каждого компьютера группы по результатам выполнения этой задачи, а не по результатам системной задачи Проверка важных областей.
3. Создать новую политику для группы компьютеров. В свойствах созданной политики на закладке **Системные задачи** отключить запуск по расписанию системных задач проверки по требованию и задач обновления баз программы на компьютерах группы администрирования.

Вы можете также настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5.

Установка Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью задачи удаленной установки, выполните следующие действия:

4. В Консоли администрирования Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** создайте новый инсталляционный пакет на основе файла client\setup.exe. Создавая новый инсталляционный пакет:
 - В окне **Выбор дистрибутива программы для установки** укажите файл client\setup.exe из папки комплекта поставки Kaspersky Industrial CyberSecurity for Nodes 2.5 и установите флажок **Копировать обновления из репозитория в инсталляционный пакет**.
 - Если требуется, в поле **Параметры запуска исполняемого файла (необязательно)** измените состав устанавливаемых компонентов набора с помощью ключа ADDLOCAL и измените папку назначения.

Например, чтобы установить в папке C:\KasperskyConsole только Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, не устанавливая файла справки и документации, выполните следующую команду:

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

- В узле "Инсталляционные пакеты" создайте задачу удаленной установки Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

Подробная информация о создании и настройке задачи удаленной установки содержится в справке *Kaspersky Security Center*.

- Запустите созданную задачу удаленной установки.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 будет установлена на указанных в задаче компьютерах.

Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Kaspersky Security Center

Если доступ к управлению Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах сети защищен паролем, введите пароль при создании задачи группового удаления программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет успешно удален на компьютерах, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Kaspersky Industrial CyberSecurity for Nodes 2.5 на других компьютерах удален не будет.

- Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоли администрирования Kaspersky Security Center, выполните следующие действия:

- В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программ.
- В задаче выберите метод удаления (аналогично выбору метода установки; см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к компьютерам. Вы можете удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [30](#)).

Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory, а также информацию о действиях после установки Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

В этом разделе

Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory.....	65
Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5	66
Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory.....	66

Установка Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes 2.5 на нескольких компьютерах через групповую политику Active Directory. Таким же образом вы можете установить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

Компьютеры, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes 2.5 или Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, должны быть в одном домене и в одной организационной единице.

Операционные системы на компьютерах, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5, используйте инсталляционные пакеты kics_x86(x64).msi. Чтобы установить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, используйте инсталляционные пакеты kicstools.msi.

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

► Чтобы установить Kaspersky Industrial CyberSecurity for Nodes 2.5 (Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5), выполните следующие действия:

1. Сохраните msi-файл инсталляционного пакета, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папке общего доступа на контроллере домена.
2. На контроллере домена создайте новую политику для группы, в которую объединены компьютеры.
3. С помощью **редактора объектов групповой политики** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes 2.5 (Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5) в формате UNC (Universal Naming Convention).
4. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
5. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет установлен на компьютерах группы после их перезагрузки, перед входом в Microsoft Windows.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5

После установки Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемых компьютерах рекомендуется сразу обновить базы программы и выполнить проверку важных областей компьютера. Вы можете выполнить эти действия из Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Действия после установки Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 47).

Вы можете также настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5.

Удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory

Если вы устанавливали Kaspersky Industrial CyberSecurity for Nodes 2.5 или Консоль программы на компьютерах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 и Консоль программы.

Вы можете выполнить удаление только с параметрами удаления по умолчанию.

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

Если доступ к управлению программой защищен паролем, удаление Kaspersky Industrial CyberSecurity for Nodes 2.5 через групповые политики Active Directory невозможно.

► Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 (Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5), выполните следующие действия:

1. На контроллере домена выберите организационную единицу, с компьютеров которой вы хотите удалить Kaspersky Industrial CyberSecurity for Nodes 2.5 или Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
2. Выберите политику, созданную для установки Kaspersky Industrial CyberSecurity for Nodes 2.5, и в **Редакторе объектов групповых политик** в узле Установка программ (**Конфигурация компьютеров > Параметры программ > Установка программ**) откройте контекстное меню инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes 2.5 (Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5) и выберите команду **Все задачи > Удалить**.
3. Выберите метод удаления **Немедленно удалить программы из учетных записей пользователей и с компьютеров**.
4. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет удален с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

Подготовка программы к работе

Процедура приемки

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

В этом разделе

Безопасное состояние	68
Проверка работоспособности. Тестовый файл EICAR	74

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированной конфигурации" на стр. [308](#)).

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 2.5, 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 компьютере при установке Kaspersky Industrial CyberSecurity for Nodes 2.5, а также системная группа «SYSTEM».

Пользователи-администраторы, осуществляющие контроль за безопасностью должны быть добавлены в группу «KICS Administrators» с правами полного доступа к управлению службами и функциями программы.

► Чтобы добавить пользователя, выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Изменить права пользователей на управление программой**.
Откроется окно **Разрешения для группы «Kaspersky Industrial CyberSecurity for Nodes»**.
3. В открывшемся окне в списке **Группы или пользователи** выберите группу «KICS Administrators» и нажмите кнопку **Добавить**.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

4. В открывшемся окне введите название учетной записи, которую необходимо добавить.
5. 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 2.5 или службой Kaspersky Security.
 - **Чтение:**
 - следующие права на управление Kaspersky Industrial CyberSecurity for Nodes 2.5: **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 2.5, 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. В окне **Разрешения для группы «Kaspersky Industrial CyberSecurity for Nodes»** нажмите на кнопку **Применить**.

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

Для настройки доступа к службам Kaspersky Industrial CyberSecurity for Nodes 2.5, в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Изменить права пользователей на управление Kaspersky Security Service** и выполните шаги 3-6.

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 2.5 откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

Откроется окно **Параметры журналов**.

2. 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.

3. Нажмите на кнопку **Настройка**.

Откроется окно **Дополнительные параметры**.

4. 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**.

5. На закладке **Уведомления** нажмите на кнопку **Текст сообщения**.

6. В открывшемся окне укажите информацию, которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет передавать в составе сигнала тревоги.

Убедитесь, что в тексте сообщения присутствуют следующие 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.

7. Нажмите на кнопку **ОК**.

Настройки уведомлений администраторов будут сохранены.

Сообщение сигнала тревоги не содержит данных о действиях по обработке. Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 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.

События аудита

Kaspersky Industrial CyberSecurity for Nodes 2.5 ведет системный 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 для данных компонентов выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

Откроется окно **Параметры Журналов**.

2. На закладке **Общие**, установите флажок **Все события** для следующих компонентов:
 - Постоянная защита файлов;
 - Проверка по требованию;

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- Контроль запуска программ.
3. Нажмите на кнопку **ОК**.

Постоянная защита файлов

Для приведения программы в сертифицируемое состояние, требуется произвести донастройку 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 2.5 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 измененных файлов**.

6. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes будет 2.5 выполнять проверку архивов ZIP, CAB, RAR, ARJ и других форматов.

Проверка по требованию

В соответствии с требованиями сертификации, необходимо создать новую пользовательскую задачу Проверки по требованию и запустить ее с предзаданными параметрами.

Подробная инструкция по созданию задач проверки по требованию содержится в разделе [Создание задачи проверки по требованию](#).

Настройка обновлений баз программы

► Чтобы настроить обновление антивирусных баз через один из защищаемых компьютеров, который выполняет функцию компьютера-ретранслятора, выполните следующие действия:

1. На компьютере-ретрансляторе остановите выполнение задач Обновление баз программы и Обновление модулей программы.
2. Настройте параметры задачи Копирование обновлений:
 - На закладке **Общие**:
 - В блоке **Источник обновлений** выберите **Серверы обновлений «Лаборатории Касперского»**.
 - В блоке **Параметры копирования обновлений** выберите **Копировать обновления баз программы**.
 - В поле **Папка локального источника обновлений** укажите путь к общей сетевой папке, в которую программа будет сохранять скопированный файл баз. Программа не распаковывает и не применяет обновления, загруженные с помощью задачи копирования баз.
 - На закладке **Параметры соединения** установите флажок **Использовать параметры прокси-сервера для соединения с серверами «Лаборатории Касперского»**.
 - На закладке **Расписание** установите флажок **Запускать задачу по расписанию** с частотой запуска **Ежечасно**.
3. На компьютере-ретрансляторе запустите задачу Копирование обновлений.
4. На компьютерах-ресиверах настройте параметры задачи Обновление баз программы, выполнив следующие действия:
 - a. На закладке **Общие** укажите в качестве источника обновлений **Другие HTTP-, FTP-серверы или сетевые ресурсы**. В качестве источника укажите сетевую папку, настроенную в качестве папки локального источника обновлений в задаче Копирование обновлений на сервере-ретрансляторе.
 - b. Снимите флажок **Использовать серверы обновлений «Лаборатории Касперского»**, если серверы, указанные пользователем, недоступны.
 - c. Настройте расписание запуска задачи Обновление баз программы на компьютерах-ресиверах таким образом, чтобы:
 - Задача выполнялась ежечасно.

- Запуск задачи выполнялся с шагом 30 минут после запуска задачи Копирование обновлений на сервере-ретрансляторе.

Обновления баз программы, загруженные из локальной папки обновлений на компьютеры-ресиверы, будут немедленно применены и распакованы.

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 2.5 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 2.5, в журнале выполнения задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 обработал файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задач Kaspersky Industrial CyberSecurity for Nodes 2.5 "Постоянная защита файлов и задач проверки по требованию".

Таблица 12. Префиксы в файлах EICAR

Префикс	Статус файла после проверки и действие Kaspersky Industrial CyberSecurity for Nodes 2.5
Без префикса	Kaspersky Industrial CyberSecurity for Nodes 2.5 присваивает объекту статус Зараженный и удаляет его.
SUSP–	Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 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 2.5 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](https://www.eicar.com/). 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.

2. 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.
3. Откройте Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
4. 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 диска защищаемого компьютера.
- В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 журнал выполнения задачи получил статус **Критический**. В журнале появилась строка с информацией об угрозе в файле eicar.com. (Чтобы просмотреть журнал выполнения задачи, в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**, выберите задачу "Постоянная защита файлов" и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.)

- Появилось сообщение Службы сообщений Microsoft Windows на компьютере, с которого вы скопировали файл, следующего содержания: Kaspersky Industrial CyberSecurity for Nodes 2.5 заблокировал доступ к <путь к файлу eicar.com на компьютере>\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 проверить функцию Проверка по требованию, выполните следующие действия:

1. Загрузите файл eicar.com со страницы сайта [EICAR](#). 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.

2. Откройте Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
3. Выполните следующие действия:
 - a. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
 - b. Выберите вложенный узел **Проверка важных областей**.
 - c. На закладке **Настройка области проверки** откройте контекстное меню на узле **Сетевое окружение** и выберите **Добавить сетевой файл**.
 - d. Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention).
 - e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.
 - f. 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 2.5 журнал выполнения задачи получил статус **Критический**; в журнале выполнения задачи "Проверка важных областей" появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**, выберите задачу Проверка важных областей и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

Разделение доступа к функциям программы по пользовательским ролям

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

В этом разделе

О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5	77
О правах на управление службой Kaspersky Security	79
О правах доступа к службе Kaspersky Security Management	81
Настройка прав доступа для Kaspersky Industrial CyberSecurity for Nodes 2.5 и службы Kaspersky Security	81
Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля	84
Разрешение сетевых соединений для службы Kaspersky Security Management	85

О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5

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

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

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

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

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

Также вы можете выполнять расширенную настройку прав доступа (см. раздел "Настройка прав доступа для Kaspersky Industrial CyberSecurity for Nodes 2.5 и службы Kaspersky Security" на стр. [81](#)): разрешать или запрещать доступ к отдельным функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

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

Таблица 13. Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Industrial CyberSecurity for Nodes 2.5.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: <ul style="list-style-type: none"> • Импортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5. • Редактировать настройки программы.
Чтение параметров	Возможности: <ul style="list-style-type: none"> • просматривать общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: <ul style="list-style-type: none"> • 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.

Права доступа	Описание
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Industrial CyberSecurity for Nodes 2.5.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Industrial CyberSecurity for Nodes 2.5.
Удаление программы	Возможность удалить Kaspersky Industrial CyberSecurity for Nodes 2.5.
Чтение прав	Возможность просматривать список пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5 и права доступа каждого пользователя.
Изменение прав	Возможности: <ul style="list-style-type: none"> • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

О правах на управление службой Kaspersky Security

При установке Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 или плагина управления Kaspersky Industrial CyberSecurity for Nodes 2.5.

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 удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи пользователя SYSTEM были изменены, при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, которые имеют доступ с правом на изменение к функциям (см. раздел "О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 77), могут предоставлять доступ к управлению 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 2.5 один из следующих предустановленных уровней доступа на управление службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security, а также запускать и останавливать работу службы Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры работы 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 работу службы Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: давать или ограничивать права на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 (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 14. Разграничение прав доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5

Функция	Описание
Чтение настроек службы	Возможность просматривать общие параметры работы 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 выполнения службы у 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: <ul style="list-style-type: none"> • добавлять и удалять пользователей службы Kaspersky Security; • изменять права доступа пользователей к службе Kaspersky Security.
Удаление службы	Возможность разрегистрации службы Kaspersky Security в Диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.

О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Industrial CyberSecurity for Nodes 2.5.

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

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

Вы можете управлять 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 2.5.

Вы можете соединиться с Kaspersky Industrial CyberSecurity for Nodes 2.5 с 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 2.5 и службы Kaspersky Security

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

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

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 2.5.
- Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению службой Kaspersky Security.

Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes 2.5"**.

4. В открывшемся окне выполните следующие действия:

- Чтобы добавить пользователя или группу в список, нажмите 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 кнопку **Удалить**.

5. Нажмите кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► Чтобы изменить права пользователя или группы на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 или службой Kaspersky Security, 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:
 1. Если вы хотите настроить параметры политики для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. [90](#)).

- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 2.5.
 - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению службой Kaspersky Security.

Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes 2.5"**.
4. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.
5. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
 - **Полный контроль**: полный набор прав на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 или службой Kaspersky Security.
 - **Чтение**:
 - Следующие разрешения на управление Kaspersky Industrial CyberSecurity for Nodes 2.5: **Чтение статистики, Чтение параметров, Чтение журналов и Чтение прав**.
 - следующие 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 2.5, 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, Определенные пользователем запросы к службе**.
6. Если вы хотите выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
 - a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Industrial CyberSecurity for Nodes 2.5** выберите нужного пользователя или группу.
 - b. Нажмите на кнопку **Изменить**.

- с. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить** или **Запретить**).
 - d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
 - e. Нажмите на кнопку **ОК**.
 - f. В окне **Дополнительные параметры безопасности для Kaspersky Industrial CyberSecurity for Nodes 2.5** 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 2.5 или службой Kaspersky Security будут сохранены.

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

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

Kaspersky Industrial CyberSecurity for Nodes 2.5 запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к локальной Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5;
- удаление Kaspersky Industrial CyberSecurity for Nodes 2.5;
- изменение компонентного состава Kaspersky Industrial CyberSecurity for Nodes 2.5.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Industrial CyberSecurity for Nodes 2.5 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.

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 защитить доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).
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 Kaspersky Industrial CyberSecurity for Nodes 2.5.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет запрашивать пароль при доступе к защищаемым операциям.

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

Вы можете изменить или сбросить заданный пароль в параметрах программы в любой момент.

► Чтобы сбросить пароль,

Снимите флажок **Использовать защиту паролем** в настройках политики или свойствах программы.

Защита паролем будет отключена. Kaspersky Industrial CyberSecurity for Nodes 2.5 удалит контрольную сумму старого пароля из параметров программы.

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 **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 2.5.
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.

Интерфейсы управления программой

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 через локальную Консоль и Плагин управления Kaspersky Industrial CyberSecurity for Nodes 2.5. Действия с локальной Консолью описаны в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*. Действия с Плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center содержится в *Справочной системе Kaspersky Security Center*.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления задачами Kaspersky Industrial CyberSecurity for Nodes 2.5 на нескольких компьютерах.

В этом разделе

О политиках	88
Настройка запуска по расписанию локальных системных задач	96



О политиках



Вы можете создавать единые политики Kaspersky Security Center для управления защитой нескольких компьютеров, на которых установлен Kaspersky Industrial CyberSecurity for Nodes 2.5.


Политика применяет указанные в ней значения параметров Kaspersky Industrial CyberSecurity for Nodes 2.5, его функций и задач 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, в Консоли администрирования имеет статус *активна*.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете просмотреть ее в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на локальных компьютерах: *Запретить изменение параметров*. После применения политики Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет на локальных компьютерах значения параметров, рядом с которыми в свойствах политики вы установили значок , вместо значений этих параметров, установленных локально до применения политики. Kaspersky Industrial CyberSecurity for Nodes 2.5 не применяет значения параметров активной политики, рядом с которыми в свойствах политики установлен значок .

Если политика активна, то в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 значения параметров, помеченные в политике значком , отображаются, но недоступны для редактирования. Значения остальных параметров (которые в политике помечены значком ) доступны для редактирования в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

Параметры, настроенные в активной политике и помеченные значком , также блокируют изменение параметров в Kaspersky Security Center для одного компьютера из окна **Свойства: <имя компьютера>**.

Параметры, настроенные и переданные на локальный компьютер с помощью активной политики, сохраняются в параметрах локальных задач после снятия активной политики.

Если политика определяет параметры какой-либо из задач постоянной защиты и эта задача выполняется, параметры, определенные политикой, изменяются сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

Создание политики

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 задачи постоянной защиты, общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры карантина и резервного хранилища, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5.


► Чтобы создать политику для группы компьютеров, на которых установлен Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:

1. В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства**, а затем выберите группу администрирования, для компьютеров которой вы хотите создать политику.
2. В панели результатов выбранной группы администрирования выберите закладку **Политики** и откройте окно мастера 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 2.5 и нажмите **Далее**.
4. **Введите название политики в поле Имя.**

Имя политики не может содержать символы " * < : > ? \ | .

5. Чтобы применить настройки политики, использованные в предыдущей версии программы, выполните следующие действия:
 - a. Установите флажок **Использовать параметры политики для предыдущей версии программы**.
 - b. Нажмите на кнопку **Выбрать** и выберите политику, которую вы хотите применить.
 - c. Нажмите на кнопку **Далее**.
6. В окне **Выбор типа операции** выберите один из следующих вариантов:
 - **Создать**, чтобы создать новую политику с настройками по умолчанию.
 - **Импортировать политику, созданную с помощью Kaspersky Industrial CyberSecurity for Nodes 2.0**, чтобы использовать данную политику в качестве шаблона.
 - Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в котором вы сохранили параметры ранее созданной политики.
7. В окне **Постоянная защита компьютера** настройте параметры задач Постоянная защита файлов, Использование KSN и функциональности Защита от эксплойтов, согласно вашим требованиям. Разрешите или запретите применение настроенных задач политики на локальных компьютерах сети:
 - Нажмите на кнопку , чтобы разблокировать настройку параметров задачи на компьютерах сети и запретить применение настроенных в политике параметров задачи.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- Нажмите кнопку , чтобы заблокировать настройку параметров задачи на компьютерах сети и разрешить применение настроенных в политике параметров задачи.

Во вновь созданной политике параметры задач постоянной защиты установлены по умолчанию.

- Если вы хотите изменить параметры задачи Постоянная защита файлов, настроенные по умолчанию, нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**. В открывшемся окне настройте задачу в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.
- Если вы хотите изменить параметры задачи Использование KSN, настроенные по умолчанию, нажмите на кнопку **Настройка** в блоке **Использование KSN**. В открывшемся окне настройте задачу в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.

Для запуска задачи Использование KSN необходимо принять Положение о KSN в окне Обработка данных (см. Раздел "Настройка обработки данных" на стр. [186](#)).

- Если вы хотите изменить параметры Защиты от эксплойтов, настроенные по умолчанию, нажмите на кнопку **Настройка** в блоке **Защита от эксплойтов**. В открывшемся окне настройте функциональность в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.
8. В окне **Создание групповой политики для программ** выберите одно из следующих состояний политики:
- **Активная политика**, если вы хотите, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, она становится неактивной, а новая политика применяется.
 - **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. 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**.
9. В окне мастера **Завершение работы** 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 2.5.

Настройка политики

В окне **Свойства: <Имя политики>** существующей политики вы можете настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты, параметры контроля активности на компьютерах, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5, права доступа к управлению программой и службой Kaspersky Security, параметры применения профилей 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, затем 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.
 - В панели результатов выбранного узла перейдите по ссылке **настроить параметры политики**.
 - Дважды щелкните выбранную политику.
4. На закладке **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
 - **Активная политика**, если хотите, чтобы политика применялась на всех компьютерах, входящих в выбранную группу администрирования.
 - **Неактивная политика**, если не хотите, чтобы политика применялась на всех компьютерах, входящих в выбранную группу.

Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Industrial CyberSecurity for Nodes 2.5.

5. В разделах **Оповещение о событиях**, **Параметры программы**, **Журналы и уведомления**, **Дополнительные возможности**, **История ревизий** настройте общие параметры работы программы (см. таблицу ниже).
6. В блоках **Постоянная защита компьютера**, **Контроль активности на компьютерах**, **Контроль активности в сети**, **Мониторинг целостности системы** настройте параметры выполнения задач программы, а также параметры их запуска (см. таблицу ниже).

Вы можете включать и выключать выполнение любой задачи на всех компьютерах, входящих в группу администрирования, с помощью политики Kaspersky Security Center. Вы можете настроить применение параметров, заданных в политике, на всех компьютерах сети для каждого отдельного компонента программы.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут применены в политике.

Процедура настройки функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

Разделы параметров политики Kaspersky Industrial CyberSecurity for Nodes 2.5

Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров от родительских политик и для дочерних политик.

Уведомления о событиях

В разделе **Оповещение о событиях** вы можете настроить параметры для следующих категорий событий:

- *Критические события;*
- *Отказ функционирования;*
- *Предупреждение;*
- *Информационные события.*

По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:

- указать место хранения и срок хранения информации о зарегистрированном событии;
- выбрать способ уведомления о регистрируемых событиях.

Параметры программы

Таблица 15. Параметры в разделе Параметры программы

Блок	Параметры
Масштабируемость и интерфейс	В блоке Масштабируемость и интерфейс по кнопке Настройка вы можете настроить следующие параметры: <ul style="list-style-type: none"> • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
Безопасность	В блоке Безопасность , нажав на кнопку Настройка , вы можете настроить следующие параметры: <ul style="list-style-type: none"> • настроить параметры запуска задачи; • указать действия программы при переходе на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.
Параметры соединения	В блоке Параметры соединения по кнопке Настройка вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: <ul style="list-style-type: none"> • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск системных задач	В блоке Запуск системных задач , нажав на кнопку Настройка , вы можете разрешить или запретить запуск следующих системных задач по расписанию, настроенному на локальных компьютерах: <ul style="list-style-type: none"> • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Таблица 16. Параметры в разделе *Дополнительные возможности*

Блок	Параметры
Доверенная зона	В блоке Доверенная зона по кнопке Настройка вы можете настроить следующие параметры применения доверенной зоны: <ul style="list-style-type: none"> сформировать список исключений доверенной зоны; включить или выключить проверку операций резервного копирования файлов; сформировать список доверенных процессов.
Проверка съёмных дисков	В блоке Менеджер устройств по кнопке Настройка вы можете настроить параметры проверки съёмных дисков, подключаемых по USB.
Права пользователей на управление программой	В блоке Права пользователей на управление программой вы можете настроить параметры доступа пользователей и групп пользователей к управлению Kaspersky Industrial CyberSecurity for Nodes 2.5
Права пользователей на управление службой	В блоке Права пользователей на управление службой вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.
Хранилища	В блоке Хранилища по кнопке Настройка вы можете настроить следующие параметры карантина и резервного хранилища: <ul style="list-style-type: none"> 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 резервного хранилища и карантина на Сервер администрирования. настроить период блокирования компьютеров.

Постоянная защита компьютераТаблица 17. Параметры в разделе *Постоянная защита компьютера*

Блок	Параметры
Постоянная защита файлов	В блоке Постоянная защита файлов по кнопке Настройка вы можете настроить следующие параметры выполнения задачи: <ul style="list-style-type: none"> 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 предустановленный уровень безопасности или настроить параметры безопасности вручную; настроить параметры запуска задачи.
Использование KSN	В блоке Использование KSN по кнопке Настройка или Обработка данных вы можете настроить следующие параметры выполнения задачи:

	<ul style="list-style-type: none"> указать действия над объектами, недоверенными в KSN; настроить производительность задачи; настроить параметры использования Kaspersky Security Center в качестве прокси-сервера KSN; принять Положение о KSN; настроить параметры запуска задачи.
Защита от эксплойтов	<p>В блоке Защита от эксплойтов по кнопке Настройка вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"> выбрать режим защиты памяти процессов; указать действия для снижения рисков эксплуатации уязвимостей; дополнить и изменить список защищаемых процессов.

Контроль активности на компьютерах

Таблица 18. Параметры в разделе Контроль активности на компьютерах

Блок	Параметры
Контроль запуска программ	<p>В блоке Контроль запуска программ с помощью кнопки Настройка вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"> 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 Wi-Fi	<p>В блоке Контроль Wi-Fi по кнопке Настройка вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"> управлять режимами работы компонента; настроить правила контроля Wi-Fi сетей.

Контроль активности в сети

Таблица 19. Параметры в разделе Контроль активности в сети

Блок	Параметры
Защита от шифрования	<p>В блоке Защита от шифрования по кнопке Настройка вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"> выбрать режим работы задачи; настроить область защиты от вредоносного шифрования; настроить параметры запуска задачи.

Диагностика системы

Таблица 20. Параметры в разделе Диагностика системы

Блок	Параметры
Мониторинг файловых операций	<p>В блоке Мониторинг файловых операций можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере.</p>

Анализ журналов	В блоке Анализ журналов можно настроить контроль целостности защищаемого компьютера на основе результатов анализа журналов событий Windows.
------------------------	--

Журналы и уведомления

Таблица 21. Параметры в разделе Журналы и уведомления

Блок	Параметры
Журналы выполнения задач	В блоке Журналы выполнения задач по кнопке Настройка вы можете настроить следующие параметры: <ul style="list-style-type: none"> указать уровень важности регистрируемых событий для выбранных компонентов программы; указать параметры хранения журналов выполнения задач.
Уведомления о событиях	В блоке Уведомления о событиях по кнопке Настройка вы можете настроить следующие параметры: <ul style="list-style-type: none"> указать параметры уведомления пользователя для события <i>Обнаружен объект</i>; указать параметры уведомления администратора для любого выбранного события из списка событий в блоке Настройка уведомлений.
Взаимодействие с Сервером администрирования	В блоке Информировать Сервер администрирования по кнопке Настройка вы можете выбрать типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет передавать на Сервер администрирования.
Инциденты	В блоке Инциденты по кнопке Настройка вы можете выбрать уведомления, на основе которых программа будет формировать инциденты на стороне Kaspersky Security Center.

История ревизий

В разделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Настройка запуска по расписанию локальных системных задач

С помощью политик вы можете разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, установленному локально на каждом компьютере группы администрирования:

- Если запуск по расписанию для локальных системных задач указанного типа запрещен в политике, такие задачи не будут выполняться на локальном 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 2.5 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 модулей программы.
- Задачи обновления: Обновление баз программы, Обновление модулей программы и Копирование обновлений.

Если вы исключите защищаемый компьютер из группы администрирования, расписание системных задач будет автоматически включено.

► Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Industrial CyberSecurity for Nodes 2.5, 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, с помощью которой вы хотите настроить запуск по расписанию системных задач Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах группы, выберите команду **Свойства**.
3. В окне **Свойства: <Имя политики>** откройте блок **Свойства программы**. В блоке **Запуск системных задач** нажмите кнопку **Настройка** и выполните одно из следующих действий:

- Установите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
- Снимите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы запретить запуск по расписанию указанных задач.

Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.

4. Убедитесь, что политика (см. раздел "О политиках" на стр. [88](#)), которую вы настраиваете, активна и применена к группе компьютеров администрирования.
5. Нажмите на кнопку **ОК**.

Настроенные параметры запуска по расписанию для выбранных задач будут применены.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Industrial CyberSecurity for Nodes 2.5, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

О создании задач в Kaspersky Security Center	98
Создание задачи в Kaspersky Security Center	99
Настройка локальных задач в окне "Параметры программы" в Kaspersky Security Center	103
Настройка групповых задач в Kaspersky Security Center	111
Создание задачи проверки по требованию	125
Настройка параметров диагностики сбоев в Kaspersky Security Center	130
Работа с расписанием задач	132

О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов компьютеров. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для одного компьютера: в окне **Свойства <Имя компьютера>** в блоке **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы компьютеров на закладке **Задачи**;
- для набора компьютеров: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 96) на всех защищаемых компьютерах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center содержится в справке *Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes*.

► 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:
 - В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый компьютер.
 - В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом компьютере и выберите пункт **Свойства**.
 - В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
- Для создания групповой задачи:
 - В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, для которой вы хотите создать задачу.
 - В панели результатов откройте контекстное меню на закладке **Задачи** и выберите пункт **Создать > Задачу**.
- Для создания задачи для произвольного набора компьютеров в дереве Консоли администрирования Kaspersky Security Center в узле **Выборки устройств** выберите пункт **Создать** задачу.

Откроется окно мастера создания задачи.


2. В окне **Определение названия задачи** введите имя задачи (не более 100 символов, не может содержать символы " * < > ? \ | : . Рекомендуется включить в имя задачи ее тип (например, "Проверка по требованию папок общего доступа").
3. В окне **Выбор типа задачи** под заголовком **Kaspersky Industrial CyberSecurity for Nodes 2.5** выберите тип создаваемой задачи.
4. Если вы выбрали любой тип задачи, кроме типа Откат обновлений баз или Активация программы, откроется окно **Параметры задачи**. В зависимости от типа создаваемой задачи выполните одно из следующих действий:

- Если вы создаете задачу проверки по требованию:

- a. В окне **Область проверки** сформируйте область проверки.

По умолчанию область проверки включает критические области компьютера. Проверяемые области отображаются в таблице помеченными значком .

Вы можете изменять область проверки: включать в нее отдельные предопределенные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

- Чтобы исключить из проверки все области проверки, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
 - Чтобы включить в область проверки предопределенную область, диск, папку, сетевой объект или файл, нажмите правой клавишей мыши в таблице **Область проверки** и выберите **Добавить область**. В окне **Добавление в область проверки** выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом компьютере или другом компьютере в сети и нажмите на кнопку **ОК**.
 - Чтобы исключить из проверки вложенные папки или файлы, выберите добавленную папку (диск) в окне **Область проверки** мастера, откройте контекстное меню и выберите **Настроить**, затем в окне **Уровень безопасности** нажмите кнопку **Настройка** и в окне **Настройка проверки по требованию** на закладке **Общие** снимите флажок **Вложенные папки и файлы**.
 - Чтобы изменить параметры безопасности области проверки, откройте контекстное меню на области, параметры которой вы хотите изменить, и выберите **Настроить**. В окне **Настройка проверки по требованию** выберите один из предустановленных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную. Настройка параметров безопасности выполняется так же, как в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.
 - Чтобы исключить из добавленной области проверки вложенные объекты, откройте контекстное меню в таблице **Область проверки**, выберите **Добавить исключение** и укажите объекты, которые вы хотите исключить: выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом компьютере или другом компьютере в сети, а затем нажмите кнопку **ОК**.
 - Области, являющиеся исключениями из проверки, отображаются в таблице помеченными значком .
- b. В окне **Параметры** выполните следующие действия.

Установите флажок **Применять доверенную зону**, если в задаче вы хотите исключить из области проверки объекты, описанные в доверенной зоне Kaspersky Industrial CyberSecurity for Nodes 2.5.

Если вы планируете использовать создаваемую задачу в качестве задачи проверки важных областей компьютера, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**. Программа Kaspersky Security Center будет оценивать состояние безопасности компьютера (компьютеров) по результатам выполнения задач со статусом *Задача проверки важных областей*, а не только по результатам выполнения системной задачи **Проверка важных областей**. При создании локальной задачи проверки по требованию флажок недоступен.

Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый приоритет **Низкий**, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**. По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes 2.5, имеют приоритет **Средний**. Понижение приоритета процесса увеличивает время выполнения задачи, но оно также может положительно повлиять на скорость выполнения процессов других активных программ.

- Если вы создаете одну из задач обновления, установите параметры задачи в соответствии с вашими требованиями:
 - a. Выберите источник обновлений в окне **Источник обновлений**.
 - b. Нажмите на кнопку **Настройка параметров локальной сети**. Откроется окно **Настройка параметров соединения**.
 - c. На закладке **Настройка параметров соединения** выполните следующие действия:

Укажите режим FTP-сервера для соединения с защищаемым компьютером.

Если требуется, измените время ожидания при соединении с источником обновления.

Настройте параметры доступа к прокси-серверу при соединении с источником обновлений.

Укажите местоположение защищаемого компьютера (компьютеров), чтобы оптимизировать получение обновлений.
- Если вы создаете задачу **Обновление модулей программы**, в окне **Настройка параметров обновления модулей программы** настройте нужные параметры обновления программных модулей:
 - a. Выберите, копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
 - b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка компьютера. Чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически запускал перезагрузку компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**. Чтобы отменить автоматическую перезагрузку после завершения задачи, снимите флажок **Разрешать перезагрузку операционной системы**.
 - c. Если вы хотите получать информацию о выходе плановых обновлений модулей Kaspersky Industrial CyberSecurity for Nodes 2.5, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта "Лаборатории Касперского". Уведомление администратора о событии **Доступны новые плановые обновления модулей программы** можно настроить. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Если вы создаете задачу *Копирование обновлений*, в окне **Настройка параметров копирования обновлений** укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.
 - Если вы создаете задачу *Активация программы*, в окне **Параметры активации** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если хотите создать задачу для продления срока действия лицензии.
 - Если вы создаете задачу *Формирование правил контроля устройств или задачу Формирование правил контроля запуска программ*, в окне **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил:
 - a. Укажите префикс для названий правил (только для задачи формирования правил контроля запуска программ).
 - b. Настройте параметры области применения разрешающих правил (только для задачи формирования правил контроля запуска программ). Нажмите на кнопку **Далее**.
 - c. Укажите действия, которые задача будет выполнять во время формирования разрешающих правил (только для задачи формирования правил контроля запуска программ) и по завершении.
5. Настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз). В окне **Расписание** выполните следующие действия:
- a. Чтобы включить расписание, установите флажок **Запускать задачу по расписанию**.
 - b. Укажите частоту запуска задачи: выберите одно из следующих значений из списка **Частота запуска: Ежечасно, Ежесуточно, Еженедельно, При запуске программы, После обновления баз программы** (в групповых задачах Обновление баз программы, Обновление модулей программы вы также можете указать частоту запуска **После получения обновлений Сервером администрирования**): Обновление баз программы и Обновление модулей программы):
 - если вы выбрали **Ежечасно**, укажите количество часов в поле **Раз в <количество> ч** в группе параметров **Параметры запуска задачи**;
 - если вы выбрали **Ежесуточно**, укажите количество дней в поле **Раз в <количество> сут** в группе параметров **Параметры запуска задачи**;
 - если вы выбрали **Еженедельно**, укажите количество недель в поле **Раз в <количество> нед.** в группе параметров **Параметры запуска задачи**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача будет запускаться по понедельникам).
 - c. В поле **Время запуска** укажите время первого запуска задачи; в поле **Начать с** укажите дату начала действия расписания.
 - d. Если требуется, задайте остальные параметры расписания: нажмите на кнопку **Дополнительно** и в окне **Дополнительные параметры расписания** выполните следующие действия:

- Укажите максимальную продолжительность выполнения задачи: в группе **Параметры остановки задачи**, в поле **Длительность** введите количество часов и минут.
 - Укажите промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено: в группе **Параметры остановки задачи** введите начальное и конечное значение промежутка в поле **Приостановить с ... до**.
 - Укажите дату, начиная с которой расписание перестанет действовать: установите флажок **Отменить расписание с** и с помощью окна **Календарь** выберите дату, начиная с которой расписание перестанет действовать.
 - Включите запуск пропущенных задач: установите флажок **Запускать пропущенные задачи**.
 - Включите использование параметра распределения времени запуска: установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
- е. Нажмите на кнопку **ОК**.
6. Если создаваемая задача является задачей для произвольного набора компьютеров, выберите компьютеры сети (группы), на которых она будет выполняться.
 7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.
 8. В окне **Завершение создания задачи** установите флажок **Запустить задачу после завершения работы мастера**, если хотите, чтобы задача была запущена по созданию. Нажмите на кнопку **Готово**.
- Созданная задача отобразится в списке **Задачи**.

Настройка локальных задач в окне Параметры программы в Kaspersky Security Center

► Чтобы настроить локальные задачи или общие параметры программы для одного компьютера в окне **Параметры программы**, выполните следующие действия:

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 компьютера>** одним из следующих способов:
 - двойным щелчком мыши на имени защищаемого компьютера;
 - откройте контекстное меню на имени защищаемого компьютера и выберите пункт **Свойства**.
 Откроется окно **Свойства: <Имя компьютера>**.
4. Чтобы настроить параметры локальной задачи, выполните следующие действия:
 - а. Перейдите в раздел **Задачи**.
 - б. В списке задач выберите локальную задачу, параметры которой вы хотите настроить:
 - Дважды щелкните на имени задачи в списке задач.
 - Выберите имя задачи и нажмите на кнопку **Свойства**.

- Затем выберите пункт **Свойства** в контекстном меню выбранной задачи.
5. Чтобы настроить параметры программы, выполните следующие действия:
- с. Перейдите в блок **Программы**.
 - д. В списке установленных программ выберите программу, которую хотите настроить:
 - двойным щелчком мыши на названии программы в списке установленных программ;
 - выделите название программы в списке установленных программ и нажмите на кнопку **Свойства**;
 - откройте контекстное меню на названии программы в списке установленных программ и выберите пункт **Свойства**.

Если программа работает под управлением политики Kaspersky Security Center, и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

Контроль проектов ПЛК

Этот раздел содержит информацию о том, как настроить и выполнить задачи получения данных о проектах программируемых логических контроллеров и проверки целостности проектов программируемых логических контроллеров (далее также "проектов ПЛК").

В этом разделе

О проверке целостности проектов ПЛК	105
О Реестре Конфигураций ПЛК	106
Настройка реестра ПЛК.....	106
Настройка проверки целостности проекта ПЛК	108
Настройка проверки целостности проекта ПЛК	109
Включение и выключение проверки целостности ПЛК	110
Импорт и экспорт данных для задачи Получение данных о проектах ПЛК.....	111

О Проверке целостности проектов ПЛК

Функция предназначена для проверки целостности проектов ПЛК, используемых в промышленной сети.

Проект ПЛК – микропрограмма, написанная для ПЛК. Проект ПЛК хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК.

Для проверки целостности проектов ПЛК требуется доступ по сети компьютера с установленной программой Kaspersky Industrial CyberSecurity for Nodes 2.5 к ПЛК.

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

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

После запуска локальной задачи Проверка целостности проектов ПЛК программа выводит предупреждения в случае изменения проектов ПЛК в сравнении с эталонными проектами ПЛК.

По умолчанию Проверка целостности проектов ПЛК выключена.

Отчеты

Отчетность входит в число базовых функций Сервера администрирования Kaspersky Security Center. Воспользоваться этой функцией можно только через Консоль Kaspersky Security Center.

После успешного завершения задачи Проверка целостности проектов ПЛК вы можете создать и просмотреть отчет со следующей информацией:

- имя компьютера, на котором завершена задача Проверка целостности проектов ПЛК;
- ПЛК, целостность которых контролируется;
- дата последней проверки;
- результаты проверки целостности.

► *Чтобы создать отчет на Сервере администрирования Kaspersky Security Center, выполните следующие действия:*

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

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

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, содержащиеся в Реестре. При этом, конфигурации ПЛК не будут удалены из Реестра, так как внесение изменений в Реестр возможно только через параметры хранилищ Kaspersky Security Center.

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 2.5 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 Kaspersky Industrial CyberSecurity for Nodes 2.5 (список синхронизируется автоматически).
- Конфигурации ПЛК с идентификационными номерами, добавленные администратором из Реестра конфигураций ПЛК.

Если конфигурация ПЛК, добавленная в список задачи Получение данных о проектах ПЛК, удалена из Реестра, Kaspersky Industrial CyberSecurity for Nodes 2.5 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**.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

4. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и выберите **Реестр конфигураций ПЛК** из раскрывающегося списка.

Откроется окно **Управление списком конфигураций ПЛК**.

5. Чтобы добавить новую конфигурацию вручную, нажмите на кнопку **Добавить**.

Откроется окно **Параметры ПЛК (добавлен через Реестр ПЛК)**.

6. В блоке **Общие параметры**:

- a. Введите **Имя** ПЛК.
- b. Выберите **Тип ПЛК** из раскрывающегося списка.

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

- c. Введите **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. Введите значение времени в секундах для параметра **Ожидать соединение**.

7. В блоке **Параметры соединения** введите следующую информацию:

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

Флажок включает или выключает применение пароля при подключении к ПЛК.

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

Если флажок снят, программа подключается к ПЛК без использования пароля.

По умолчанию флажок снят.

Флажок не задает новый пароль для подключения к ПЛК. Установка пароля выполняется на стороне ПЛК.

- c. 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.

- d. Нажмите на кнопку **ОК**.

8. Вы также можете **Импортировать** и **Экспортировать** xml-файл с конфигурацией ПЛК, нажав на соответствующую кнопку в окне **Реестр конфигураций проектов ПЛК**.
9. Чтобы изменить параметры конфигурации ПЛК, нажмите на кнопку **Изменить**.

Изменение конфигурации ПЛК в реестре ПЛК влияет на результаты задачи Проверка целостности проектов ПЛК. Вам потребуется запустить задачу Получение данных о проектах ПЛК, чтобы получить обновленные данные, и затем снова запустить задачу Проверка целостности проектов ПЛК, чтобы получить актуальные результаты.

10. Нажмите на кнопку **Удалить**, если больше не используете конфигурацию ПЛК.

После удаления из реестра ПЛК проект ПЛК становится недоступным для получения данных и проверки целостности.

11. Используйте поле **Фильтр**, чтобы увидеть все конфигурации ПЛК с требуемыми значениями.

Вы не можете использовать фильтр по ID Реестра ПЛК.

12. 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 программ решения *Kaspersky Industrial CyberSecurity*.
13. Нажмите на кнопку **Заккрыть**.

Реестр ПЛК будет сохранен.

Настройка Проверки целостности проектов ПЛК

Перед проверкой целостности проектов ПЛК необходимо получить информацию о проектах ПЛК, которые используются в промышленной сети в настоящее время. Получение информации выполняется с помощью локальной задачи Получение данных о проектах ПЛК.

► Настройка Получения данных о проектах ПЛК

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. Откройте блок **Конфигурации ПЛК**.

В списке конфигураций ПЛК отображаются конфигурации, добавленные через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

Добавленные через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5.

5. Нажмите на кнопку **Добавить ПЛК из реестра**, чтобы добавить необходимые конфигурации проектов ПЛК из реестра ПЛК (см.раздел "Настройка реестра ПЛК" на стр. [106](#)).

Откроется окно **Реестр конфигураций ПЛК**.

6. Выберите конфигурацию ПЛК и нажмите на кнопку **Добавить в список задач**.
7. Добавьте все нужные конфигурации ПЛК и закройте окно **Реестр 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 **Подключить 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. В разделе **Задачи** выберите **Проверка целостности проектов ПЛК > Свойства**.

Откроется окно **Свойства: Проверка целостности проектов ПЛК**.

3. 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 Kaspersky Security Center Получение данных о проектах ПЛК.

4. 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. Установите значение параметра **Интервал опроса ПЛК**, чтобы указать интервал времени, через который программа запрашивает информацию о параметрах проекта 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**.
5. В графе **Тип ПЛК** окна **Данные для проверки целостности проекта ПЛК** установите флажки напротив тех типов ПЛК, целостность проектов которых вы хотите проверять.
6. В окне **Данные для проверки целостности проекта ПЛК** нажмите на кнопку **ОК**.
7. В окне **Свойства: Проверка целостности проектов ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Включение и выключение Проверки целостности проектов ПЛК

Задача Проверка целостности проектов ПЛК выполняется только после того, как Kaspersky Industrial CyberSecurity for Nodes 2.5 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. В разделе **Задачи** выберите **Проверка целостности проектов ПЛК > Свойства**.

Откроется окно **Свойства: Проверка целостности проектов ПЛК**.

3. 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.

4. В окне **Свойства: Проверка целостности проектов ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

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. В разделе **Задачи** выберите **Получение данных о проектах ПЛК > Свойства**.

Откроется окно **Свойства: Получение данных о проектах ПЛК**.

3. В разделе **Настройка** выполните одно из следующих действий:
 - Нажмите на кнопку **Импорт**, чтобы импортировать в таблицу *Получение данных о проекте ПЛК* данные о ПЛК, информацию о проекте которого 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.
4. В окне **Свойства: Получение данных о проектах ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Настройка групповых задач в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

► Чтобы настроить групповую задачу для нескольких компьютеров, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Имя задачи>** одним из следующих способов:
 - двойным щелчком мыши на имени задачи в списке созданных задач;
 - выделите имя задачи в списке созданных задач и перейдите по ссылке **Изменить параметры задачи**;
 - откройте контекстное меню на имени задачи в списке созданных задач и выберите пункт **Свойства**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке Kaspersky Security Center.

5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
 - Если вы настраиваете задачу проверки по требованию:
 - a. В разделе **Настройка** сформируйте область проверки.
 - b. В разделе **Параметры** настройте интеграцию с другими компонентами программы и уровень приоритета задачи.
 - Если вы настраиваете одну из задач обновления, установите параметры задачи в соответствии с вашими требованиями:
 - a. В разделе **Источник обновлений** настройте параметры источника обновлений и оптимизацию использования дисковой подсистемы.
 - b. По кнопке **Настройка параметров соединения** настройте общие параметры соединения и параметры соединения с источником обновлений.
 - Если вы настраиваете задачу Обновление модулей программы, в разделе **Настройка параметров обновления модулей программы** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
 - Если вы настраиваете задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.

- Если вы настраиваете задачу **Активация программы**, в блоке **Параметры активации** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного кода активации или ключа**, если хотите добавить код активации или ключ для продления срока действия лицензии.
 - Если вы настраиваете одну из задач автоматического формирования разрешающих правил контроля компьютера, в блоке **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
 7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу. Подробная информация о настройке параметров в этом разделе содержится 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 содержится в справке *Kaspersky Security Center*.
 9. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Параметры групповых задач, доступные для настройки, описаны в таблице ниже.

Таблица 22. Параметры групповых задач Kaspersky Industrial CyberSecurity for Nodes 2.5

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
Автоматическое формирование правил (задача Формирование правил контроля запуска программ и задача Формирование правил контроля устройств).	Настройка	При настройке параметров задачи Формирование правил контроля запуска программ вы можете: <ul style="list-style-type: none"> • изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами; • учитывать или не учитывать запущенные программы.
	Параметры	Вы можете указать действия при формировании разрешающих правил контроля запуска программ: <ul style="list-style-type: none"> • 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

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
		<p>рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.</p> <ul style="list-style-type: none"> • Использовать заголовок и отпечаток цифрового сертификата <p>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.</p>

		<ul style="list-style-type: none"> • Если сертификат отсутствует <p>Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ для случая, если файл, на основе которого формируется правило, не имеет цифрового сертификата.</p> • Использовать хеш SHA256 <p>Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.</p> <p>Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.</p> <p>Данный вариант выбран по умолчанию.</p>
--	--	--

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
		<ul style="list-style-type: none"> • Формировать правила для пользователя или группы пользователей Поле, в котором отображаются пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / или группой. По умолчанию выбрана группа Все. Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 создает по завершении задач.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Активация программы	Параметры активации программы	Вы можете добавить ключ для активации программы или для продления срока действия лицензии.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Копирование обновлений	Источник обновлений	<p>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.</p> <p>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.</p>
	Окно Настройка параметров соединения	В блоке Параметры соединения с источниками обновлений вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
	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 2.5 будет сохранять скопированные обновления.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Обновление баз программы	Источник обновлений	<p>В блоке 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.</p> <p>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.</p> <p>В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:</p> <ul style="list-style-type: none"> • Снизить нагрузку на дисковую систему Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти. Если флажок установлен, функция активна. По умолчанию флажок снят. • Объем оперативной памяти, используемый для оптимизации (МБ).
Объем оперативной памяти (в мегабайтах), который программа использует для размещения файлов обновлений.	Окно Настройка параметров соединения	В блоке Параметры соединения с источниками обновлений вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
По умолчанию установлен объем оперативной памяти 512 МБ.	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Обновление модулей программы	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 Настройка параметров соединения	В блоке Параметры соединения с источниками обновлений вы можете настроить параметры использования прокси-сервера 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 2.5 будет совершать при наличии критических обновлений модулей программы, при наличии информации о доступных плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Проверка по требованию	Настройка	Вы можете сформировать область проверки для задачи проверки по требованию, а также перейти к настройке уровня безопасности.
	Окно Настройка проверки по требованию	Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную.

Типы задач Kaspersky Industrial CyberSecurity for Nodes 2.5	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
	Параметры	<p>В блоке Эвристический анализатор вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка.</p> <p>В блоке Дополнительные параметры вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> • применение доверенной зоны в задаче проверки по требованию; • применение служб KSN в задаче 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 настраивать параметры запуска задачи по расписанию.
Задача Проверка целостности модулей программы	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.

Для задачи типа Откат обновления баз программы вы можете 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 содержится в справке Kaspersky Security Center.

В этом разделе

Задачи Автоматическое формирование разрешающих правил и Формирование правил контроля запуска программ.....	120
Задача Активация программы	122
Задачи обновления программы.....	123
Проверка целостности модулей программы	124

Задачи формирования правил контроля устройств и контроля запуска программ

► Чтобы настроить задачу *Формирование правил контроля устройств* или задачу *Формирование правил контроля запуска программ*, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.
5. Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.
6. В разделе **Настройка** вы можете настроить следующие параметры:
 - изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами;
 - учитывать или не учитывать запущенные программы.
7. В разделе **Параметры** вы можете 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.

- **Использовать заголовок и отпечаток цифрового сертификата**

Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. В дальнейшем программа будет разрешать запуск программ, которые запускаются с помощью файлов с указанными в правиле заголовком и отпечатком цифрового сертификата.

Использование этого флажка наиболее строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

Если флажок снят, то в качестве критерия срабатывания разрешающих правил

контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

По умолчанию флажок установлен.

- **Если сертификат отсутствует**

Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ для случая, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

- **Хеш SHA256.** В качестве критерия разрешающего правила контроля запуска программ устанавливается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
- **Путь к файлу.** В качестве критерия разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице Создавать разрешающие правила для программ из папок.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

Данный вариант выбран по умолчанию.

- **Создавать правила для пользователя или группы пользователей**

Поле, в котором отображаются пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / или группой.

По умолчанию выбрана группа **Все**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 создает по завершении задач.

8. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
9. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
10. 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 содержится в справке *Kaspersky Security Center*.

11. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Задача Активация программы

► Чтобы настроить задачу Активация программы, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.
5. Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.
6. В разделе **Параметры активации программы** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если хотите добавить ключ для продления срока действия лицензии.
7. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
8. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
9. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.

10. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Задачи обновления

Чтобы настроить задачу Копирование обновлений, Обновление баз программы или Обновление модулей программы, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

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

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке Kaspersky Security Center.

5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
 - В разделе **Источник обновлений** настройте параметры источника обновлений и оптимизацию использования дисковой подсистемы.
 - a. В блоке **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.
 - b. В блоке **Оптимизация использования дисковой подсистемы** для задачи Обновление баз программы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:
 - **Снизить нагрузку на дисковую систему**

Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

Если флажок установлен, функция активна.

По умолчанию флажок снят.
 - **Объем оперативной памяти, используемый для оптимизации (МБ).**

Объем оперативной памяти (в мегабайтах), который программа использует для размещения файлов обновлений. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.
 - c. Нажмите на кнопку **Настройка параметров соединения** и в открывшемся окне **Параметры соединения** настройте параметры использования прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского» и другими серверами.

- В разделе **Настройка параметров обновления модулей программы** для задачи Обновление модулей программы вы можете указать действия, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет совершать при наличии критических обновлений модулей программы, при наличии информации о доступных плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
 - В блоке **Настройка параметров копирования обновлений** для задачи **Копирование обновлений** укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
 7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.

Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.

8. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы вы можете настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в блоках **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.

Задача Проверка целостности модулей программы

► Чтобы настроить групповую задачу Проверка целостности модулей программы, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.

5. В разделе **Устройства**, выберите устройства для которых вы хотите настроить задачу проверки целостности модулей программы.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).

7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
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 содержится в справке *Kaspersky Security Center*.

9. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.



Создание задачи проверки по требованию

► 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 Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемый компьютер.
 - b. В панели результатов на закладке **Устройства** откройте контекстное меню на строке с информацией о защищаемом компьютере и выберите пункт **Свойства**.
 - c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
 - Для создания групповой задачи:
 - a. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, для которой вы хотите создать задачу.
 - b. В панели результатов откройте контекстное меню на закладке **Задачи** и выберите пункт **Создать > Задачу**.
 - Для создания задачи для произвольного набора компьютеров в дереве Консоли администрирования Kaspersky Security Center в узле **Выборки устройств** выберите пункт **Создать задачу**.

Откроется окно мастера создания задачи.

2. В окне **Определение названия задачи** введите имя задачи (не более 100 символов, не может содержать символы `! * < > ? \ / | : .`). Рекомендуется включить в имя задачи ее тип (например, "Проверка по требованию папок общего доступа").
3. В окне **Выбор типа задачи** под заголовком **Kaspersky Industrial CyberSecurity for Nodes 2.5** выберите задачу **Проверка по требованию** и нажмите кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки:

По умолчанию область проверки включает критические области 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 предопределенные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

- Чтобы исключить из проверки все области проверки, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
- Чтобы включить предустановленную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
 - a. Щелкните правой клавишей мыши по таблице **Область проверки** и выберите **Добавить область** или нажмите кнопку **Добавить**.
 - b. В окне **Добавление в область проверки** выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом компьютере или другом компьютере в сети и нажмите 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 параметр **Настроить**.
 - b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
 - c. На закладке **Общие** в окне параметров **Проверка по требованию** снимите флажки **Вложенные папки и файлы**.
- Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
 - a. Откройте контекстное меню на области, параметры которой вы хотите изменить, и выберите **Настроить**.
 - b. В окне **Настройка проверки по требованию** выберите один из предустановленных 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. 173).

- Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:
 - a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить исключение**.
 - b. Укажите объекты, которые вы хотите исключить: выберите предустановленную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на компьютере или другом компьютере сети.
 - c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и дополнительные параметры:

- Настройте использование эвристического анализатора (см. раздел "Использование эвристического анализатора" на стр. [168](#)).
- Установите флажок **Применять доверенную зону**, если в задаче вы хотите исключить из области проверки объекты, описанные в доверенной зоне Kaspersky Industrial CyberSecurity for Nodes 2.5.

Флажок включает или выключает применение доверенной зоны в работе задачи.

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

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

По умолчанию флажок установлен.

- Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

Флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

Если флажок снят, задача постоянной защиты файлов не использует службы KSN.

По умолчанию флажок установлен.

- Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый 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 компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes 2.5 и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки и увеличивается при уменьшении нагрузки.

Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 и другие программы. В этом случае скорость выполнения задачи увеличивается.

По умолчанию флажок снят.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes 2.5, имеют приоритет **Средний**.

- Чтобы использовать создаваемую задачу в качестве задачи проверки важных областей компьютера, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты компьютера. Kaspersky Security Center оценивает безопасность компьютера (компьютеров) по показателям производительности задачи и присваивает статус *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

Если флажок установлен, Сервер администрирования регистрирует событие *Выполнена проверка важных областей* и обновляет статус защиты компьютера по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

Если флажок снят, задача проверки выполняется с низким приоритетом.

Флажок установлен по умолчанию для задачи Проверка важных областей.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** настройте расписание задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. [133](#)).
8. Укажите учетную запись пользователя, под которой вы хотите выполнять задачу, и укажите имя задачи.
9. Нажмите на кнопку **Готово**.

Будет создана новая задача проверки по требованию для выбранного компьютера или группы компьютеров.

Настройка задач проверки по требованию

► Чтобы настроить задачу Проверка по требованию, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.
Откроется окно **Свойства: <Имя задачи>**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке Kaspersky Security Center.

5. В блоке **Параметры** вы можете выполнить следующие действия:
 - a. В блоке **Область проверки** установите флажки напротив тех, файловых ресурсов, которые вы хотите включить в область проверки.
 - b. Нажмите кнопку **Настроить** и выберите уровень безопасности.

Вы можете установить один из предустановленных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную.

- с. Чтобы настроить уровень безопасности вручную, в окне **Настройка проверки по требованию** нажмите на кнопку **Настройка**.
6. В блоке **Параметры** вы можете выполнить следующие действия:
 - а. В блоке **Эвристический анализатор** включить или выключить использование эвристического анализатора и настроить уровень анализа с помощью ползунка.
 - б. Настройте Дополнительные параметры (см. раздел "Создание задачи проверки по требованию" на стр. [125](#)).
7. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
8. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
9. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в справке *Kaspersky Security Center*.

10. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Присвоение задаче проверки по требованию статуса Задача проверки важных областей

По умолчанию Kaspersky Security Center присваивает компьютеру статус *Предупреждение*, если задача "Проверка важных областей" выполняется реже, чем указано параметром Kaspersky Industrial CyberSecurity for Nodes 2.5 **Порог формирования события "Проверка важных областей не проводилась давно"**.

- Чтобы настроить проверку всех компьютеров, входящих в одну группу администрирования, выполните следующие действия:

1. Создайте групповую задачу проверки по требованию.
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей компьютера**. Указанные вами параметры задачи – область проверки и параметры безопасности – будут едиными для всех компьютеров группы. Настройте расписание задачи.

Вы можете установить флажок **Считать выполнение задачи проверкой важных областей** как при создании задачи проверки по требованию для группы компьютеров или для набора компьютеров, так и позже, в окне **Свойства: <Имя задачи>**.

3. С помощью новой или существующей политики отключите запуск по расписанию системных задач проверки по требованию на группе компьютеров (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [96](#)).

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого компьютера и уведомлять вас о нем по результатам последнего выполнения задачи со статусом *Задача проверки важных областей*, а не по результатам выполнения системной задачи Проверка важных областей.

Вы можете присваивать статус *Задача проверки важных областей* как групповым задачам проверки по требованию, так и задачам для наборов компьютеров.

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете просмотреть, является ли задача проверки по требованию задачей проверки важных областей компьютера.

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 флажок **Считать выполнение задачи проверки важных областей** отображается в свойствах задач, но он не доступен для редактирования.

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Industrial CyberSecurity for Nodes 2.5 возникла проблема (например, Kaspersky Industrial CyberSecurity for Nodes 2.5 завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

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

Kaspersky Industrial CyberSecurity for Nodes 2.5 записывает информацию в файлы трассировки и дампа в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. [Ошибка! Закладка не определена.](#)) и разрешить доступ к журналам, файлам трассировки и дампа 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 "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).
2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:
 - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
 - В поле ниже укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файлы трассировки.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- Настройте уровень детализации отладочной информации.

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

Вы можете выбрать один из следующих уровней детализации:

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

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

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

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

- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Таблица 23. Коды подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Industrial CyberSecurity for Nodes 2.5.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.

scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

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

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

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

- Если вы хотите создавать файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
 - В поле ниже укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файл дампа.

3. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут применены на защищаемом компьютере.

Работа с расписанием задач

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

В этом разделе

Настройка параметров расписания запуска задач	133
Включение и выключение запуска по расписанию	134

Настройка параметров расписания запуска задач

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

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

1. В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:
 - Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политика > <Имя политики> > <Раздел> > Настроить > Управление задачами**.
 - Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно **Параметры задачи** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)) в Kaspersky Security Center.
Откроется окно **Параметры**.
2. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.

Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск задачи по расписанию запрещен действием политики Kaspersky Security Center.

3. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
 - с. в списке **Частота запуска** выберите одно из следующих значений:
 - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество часов, и укажите количество часов в поле **Раз в <количество> ч.**;
 - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут.**;
 - **Еженедельно**, если хотите, чтобы задача запускалась с периодичностью несколько недель, и задайте количество недель в поле **Раз в <количество> нед.** Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
 - **При запуске программы**, если хотите, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes 2.5;
 - **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.
 - а. В поле **Время запуска** укажите время первого запуска задачи.
 - б. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы откроете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики Kaspersky Security Center (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [96](#)).

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

Включение и выключение запуска по расписанию

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

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

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.
Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:
 - установите флажок **Запускать задачу по расписанию**, если хотите включить запуск задачи по расписанию;

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- снимите флажок **Запускать задачу по расписанию**, если хотите выключить запуск задачи по расписанию.

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

4. Нажмите кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center.

В этом разделе

Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center	136
О настройке общих параметров программы в Kaspersky Security Center	137
О настройке дополнительных возможностей программы	142
О настройке журналов и уведомлений	155

Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленным Kaspersky Industrial CyberSecurity for Nodes 2.5, включенными в группу администрирования, с помощью Плагина Kaspersky Industrial CyberSecurity for Nodes 2.5. Также вы можете отдельно настраивать параметры работы для каждого компьютера, входящего в группу администрирования, в Kaspersky Security Center.

Группа администрирования формируется на стороне Kaspersky Security Center вручную и включает несколько компьютеров с установленным Kaspersky Industrial CyberSecurity for Nodes 2.5, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *справке Kaspersky Security Center*.

Параметры программы для одного компьютера недоступны для настройки, если работа Kaspersky Industrial CyberSecurity for Nodes 2.5 на этом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center следующими способами:

- **Использование политик Kaspersky Security Center.** Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы компьютеров. Параметры задач, заданные в активной политике, имеют приоритет над параметрами задач, настроенными локально в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 или удаленно в окне **Свойства: <Имя компьютера>** Kaspersky Security Center.

С помощью политик вы можете настроить общие параметры работы программы, параметры задач постоянной защиты, параметры задач контроля компьютера, параметры запуска системных задач по расписанию, параметры использования профилей.

- **Использование групповых задач Kaspersky Security Center.** Групповые задачи Kaspersky Security Center позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для группы компьютеров.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления, параметры задачи автоматического формирования разрешающих правил.
- **Использование задач для набора устройств.** Задачи для набора устройств позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для компьютеров, которые не включены ни в одну из созданных групп администрирования.
- **Использование окна настройки параметров одного компьютера.** В окне **Свойства: <Имя компьютера>** вы можете удаленно настроить параметры задачи для одного компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Industrial CyberSecurity for Nodes 2.5, если выбранный 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 как для группы компьютеров, так и для одного компьютера.

О настройке общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center для группы компьютеров или для одного компьютера.

В этом разделе

Настройка масштабируемости и интерфейса в Kaspersky Security Center	137
Настройка параметров безопасности в Kaspersky Security Center	139
Настройка параметров соединения в Kaspersky Security Center	141

Настройка масштабируемости и интерфейса в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

► Чтобы настроить параметры масштабируемости и интерфейса программы, 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Параметры программы** в блоке **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
4. В окне **Масштабируемость и интерфейс** на закладке **Общие** настройте следующие параметры:
 - В блоке **Параметры масштабируемости** настройте параметры, определяющие количество используемых Kaspersky Industrial CyberSecurity for Nodes 2.5 рабочих процессов:
 - **Определять параметры масштабируемости автоматически.**
Kaspersky Industrial CyberSecurity for Nodes регулирует количество используемых процессов автоматически.
Это значение установлено по умолчанию.
 - **Указать количество рабочих процессов вручную.**
Kaspersky Industrial CyberSecurity for Nodes регулирует количество активных рабочих процессов в соответствии с указанными значениями.
 - **Максимальное количество активных процессов.**
Максимальное количество процессов, которые использует Kaspersky Industrial CyberSecurity for Nodes 2.5. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
 - **Число процессов для постоянной защиты.**
Максимальное количество процессов, которые используют компоненты задач постоянной защиты. 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**

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

процессов вручную.

В блоке **Взаимодействие с пользователем** настройте отображение **Значка области уведомлений** программы в панели задач: снимите или установите флажок **Показывать значок области уведомлений**.

5. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

► Чтобы вручную настроить параметры безопасности, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Свойства программы** в блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.
4. В окне **Параметры безопасности** настройте следующие параметры:
 - В блоке **Параметры надежности** настройте параметры восстановления задач Kaspersky Industrial CyberSecurity for Nodes 2.5 в случае возникновения 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.

- **Выполнять восстановление задач проверки по требованию не более (раз).**

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 блоке **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на компьютер, создаваемой Kaspersky Industrial CyberSecurity for Nodes 2.5 при переходе на источник бесперебойного питания:

- **Не запускать задачи проверки по расписанию.**

Флажок включает или выключает запуск задач проверки по расписанию при переходе 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 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 компьютера.

По умолчанию флажок установлен.

- **Остановить выполнение задачи проверки.**

Флажок включает или выключает остановку запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes останавливает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes продолжает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

По умолчанию флажок установлен.

Переход на источник бесперебойного питания осуществляется только при уменьшении заряда устройства ниже 90%.

- В блоке **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

5. Нажмите на кнопку **ОК**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

Настроенные параметры соединения используются для подключения Kaspersky Industrial CyberSecurity for Nodes 2.5 к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► Чтобы настроить параметры соединения, 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Свойства программы** в блоке **Прокси-сервер**: нажмите на кнопку **Настройка**.
Откроется окно **Настройка параметров соединения**.
4. В окне **Параметры соединения** настройте следующие параметры:
 - В блоке **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.
 - **Автоматически определять параметры прокси-сервера.**
Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes 2.5

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

автоматически определяет параметры подключения к службам KSN с использованием протокола Web Proxy Auto-Discovery Protocol (WPAD).

Данный вариант выбран по умолчанию.

- **Использовать параметры указанного прокси-сервера.**

Если выбран этот вариант, для соединения с KSN Kaspersky Industrial CyberSecurity for Nodes 2.5 использует параметры прокси-сервера, указанные вручную.

- IP-адрес или символьное имя прокси-сервера и номер порта.

- **Не использовать настройки прокси-сервера для локальных адресов.**

Флажок включает или выключает использование прокси-сервера при обращении к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Industrial CyberSecurity for Nodes 2.5.

Если флажок установлен, обращение к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Industrial CyberSecurity for Nodes 2.5, выполняется напрямую. Прокси-сервер не используется.

Если флажок снят, для обращения к локальным компьютерам используется прокси-сервер.

По умолчанию флажок установлен.

- В блоке **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 с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft, а также 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 блоке **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы.**

5. Нажмите на кнопку **ОК**.

Настроенные параметры соединения будут сохранены.

О настройке дополнительных возможностей программы

Вы можете настроить дополнительные возможности Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center для группы компьютеров или для одного компьютера.

В этом разделе

Настройка параметров доверенной зоны в Kaspersky Security Center	143
Проверка съёмных дисков	148
Настройка прав доступа в Kaspersky Security Center	150
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center	151
Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы	152

Настройка параметров доверенной зоны в Kaspersky Security Center

По умолчанию во вновь созданных политиках и задачах доверенная зона применяется.

► Чтобы настроить параметры доверенной зоны, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.
Откроется окно **Доверенная зона**.
4. На закладке **Исключения** укажите объекты, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке:
 - Если вы хотите добавить рекомендуемые исключения, нажмите на кнопку **Добавить рекомендуемые исключения**.

При нажатии на эту кнопку в список исключений добавляются исключения, рекомендованные корпорацией Microsoft и исключения, рекомендованные "Лабораторией Касперского".

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- Если вы хотите импортировать исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файлы, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет считать доверенными.
 - Если вы хотите вручную указать условия, при удовлетворении которым файл будет считаться доверенным, нажмите на кнопку **Добавить**. В открывшемся окне укажите следующие параметры:
 - **Проверяемый объект.**
Имя или маска имени файла, локальный или съемный диск компьютера, локальная или сетевая папка, predetermined область.
 - **Обнаруживаемые объекты.**
Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.
Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные объекты, доступные для обнаружения.
Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes обнаруживает все объекты, указанные в программе по умолчанию.
По умолчанию флажок снят.
 - **Область применения исключения.**
Название задачи Kaspersky Industrial CyberSecurity for Nodes, в которой применяется правило.
 - Если требуется, укажите дополнительную информацию, поясняющую исключение, в поле **Комментарий**.
5. В окне **Доверенная зона** на закладке **Доверенные процессы** укажите процессы, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет пропускать при проверке:
- **Не проверять файловые операции резервного копирования.**
Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются установленными на компьютере средствами резервного копирования.
Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке операции чтения файлов, выполняемые установленными на компьютере средствами резервного копирования.
Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет операции чтения файлов, выполняемые установленными на компьютере средствами резервного копирования.
По умолчанию флажок установлен.
 - **Не проверять файловую активность указанных процессов.**
Флажок включает или выключает проверку файловой активности доверенных процессов.
Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке файловые операции доверенных процессов.
Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файловые операции доверенных процессов.

По умолчанию флажок снят.

6. Если требуется, добавьте процессы, файловую активность которых вы не хотите проверять, нажав кнопку **Добавить** (см. раздел "Добавление доверенных процессов" на стр. [145](#)).
7. Нажмите на кнопку **ОК** в окне **Доверенная зона**, чтобы сохранить изменения.

Добавление доверенных процессов

► Чтобы добавить один или несколько процессов в список доверенных, 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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

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

а. Использовать полный путь для определения доверенности процесса.

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

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

По умолчанию флажок установлен.

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

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

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

По умолчанию флажок установлен.

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

d. Выберите исполняемый файл в открывшемся окне.

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

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

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

g. Нажмите на кнопку **ОК**.

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

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

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

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

b. Нажмите на кнопку **ОК**.

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

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

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

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

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

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

По умолчанию флажок установлен.

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

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

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

По умолчанию флажок установлен.

d. Нажмите на кнопку **ОК**.

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

7. В окне **Добавление доверенного процесса** 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 во время проверки легальное программное обеспечение 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 2.5 применит действия, указанные в настройках задачи для программ и ресурсов, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus:*

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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.

Откроется окно **Доверенная зона**.

4. На закладке **Исключения**, прокрутите список и выберите строку со значением **not-a-virus:***, если флажок снят.
5. Нажмите на кнопку **ОК**.

Новые настройки будут применены.

Проверка съёмных дисков

Вы можете настроить проверку съёмных дисков, подключаемых по USB к защищаемому компьютеру.

Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет проверку съёмного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу Проверка по требованию в момент подключения съёмного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется с предустановленным уровнем безопасности, указанным для проверки съёмных дисков. Вы не можете настроить параметры временной задачи Проверка по требованию.

Kaspersky Industrial CyberSecurity for Nodes запускает проверку съёмных дисков, подключаемых по USB при их регистрации в операционной системе в качестве запоминающего устройства (USB Mass Storage Device). Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к съёмному диску на время проверки.

Результаты проверки каждого съёмного диска доступны в журнале выполнения задачи Проверка по требованию, созданной при подключении этого диска.

Вы можете изменять значения параметров компонента Проверка съёмных дисков (см.таблицу ниже).

Таблица 24. Параметры проверки съёмных дисков

Параметр	Значение по умолчанию	Описание
Проверять съёмные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске.

		Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	<p>Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности:</p> <ul style="list-style-type: none"> • Максимальная защита • Рекомендуемый • Максимальное быстроедействие <p>Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют предустановленным уровням безопасности в задачах проверки по требованию.</p>

Чтобы настроить параметры проверки съёмных дисков при подключении, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 параметры** нажмите на кнопку **Настройка** в блоке **Проверка съёмных дисков**.
Откроется окно **Проверка съёмных дисков**.
4. В блоке **Параметры проверки при подключении** выполните следующие действия:
 - Установите флажок **Проверять съёмные диски при их подключении по USB**, если вы хотите, чтобы Kaspersky Industrial CyberSecurity for Nodes автоматически выполнял проверку съёмных дисков при подключении.

- Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
 - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съёмных дисков.
5. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

Настройка прав доступа в Kaspersky Security Center

Вы можете настроить права доступа к управлению программой и к управлению службой Kaspersky Security в Kaspersky Security Center для группы компьютеров и для одного компьютера.

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

► Чтобы настроить права доступа к управлению программой и службой Kaspersky Security, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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. Откройте раздел **Дополнительные возможности** и выполните следующие действия:
 - Если вы хотите настроить права доступа к управлению Kaspersky Industrial CyberSecurity for Nodes 2.5 для пользователей или группы пользователей, в блоке **Права пользователей на управление программой** нажмите кнопку **Настройка**.
 - Если вы хотите настроить права доступа к управлению службой Kaspersky Security для пользователей или группы пользователей, в блоке **Права пользователей на управление службой Kaspersky Security** нажмите кнопку **Настройка**.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

4. В открывшемся окне настройте права доступа в соответствии с вашими требованиями (см. раздел "О правах доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. [Ошибка! Закладка не определена.](#)).

Настроенные параметры будут сохранены.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

► Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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** нажмите на кнопку **Настройка** в блоке **Хранилища**.
4. В окне **Параметры хранилищ** на закладке **Резервное хранилище** 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.
 - Если вы хотите задать максимальный размер **резервного хранилища**, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- Если вы хотите задать порог свободного места в резервном хранилище, определите значение параметра **Максимальный размер резервного хранилища (МБ)**, установите флажок **Порог доступного пространства (МБ)** и укажите минимальный размер свободного места в папке резервного хранилища в мегабайтах.
 - Если вы хотите задать папку для восстановления, в группе параметров Параметры восстановления объектов выберите нужную папку на локальном диске защищаемого компьютера или в поле **Папка, в которую восстанавливаются объекты** введите имя папки и полный путь к ней.
5. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие **параметры карантина**:
- Если вы хотите изменить **папку карантина**, в поле ввода **Папка карантина** укажите полный путь к папке на локальном диске защищаемого компьютера.
 - Если вы хотите указать **максимальный размер карантина**, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.
 - Если вы хотите указать минимальный размер свободного пространства в **карантине**, установите флажок **Максимальный размер карантина (МБ)** и флажок **Порог доступного пространства (МБ)**, затем в поле ввода укажите пороговое значение параметра в мегабайтах.
 - Если вы хотите изменить папку, в которую восстанавливаются объекты из карантина, в поле ввода **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого компьютера.
6. Нажмите на кнопку **ОК**.
- Настроенные параметры карантина и резервного хранилища будут сохранены.

Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать недоверенные компьютеры и настроить параметры хранилища заблокированных компьютеров.

В этом разделе

О блокировании доступа к сетевым файловым ресурсам.....	152
Включение блокирования доступа к сетевым файловым ресурсам.....	153
Настройка параметров заблокированных компьютеров	154

О блокировании доступа к сетевым файловым ресурсам

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов, Защита от шифрования. Задачи отслеживают попытки удаленных компьютеров получить доступ к общим сетевым папкам защищаемого компьютера или сетевого хранилища в соответствии со списком недоверенных компьютеров. Информация обо всех недоверенных компьютерах со всех защищаемых компьютеров отправляется в Kaspersky Security Center. Kaspersky Industrial

CyberSecurity for Nodes 2.5 блокирует доступ к общим сетевым папкам компьютера или общим папкам сетевого хранилища для всех узлов в хранилище заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Если в ходе выполнения задачи Постоянная защита файлов со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена вредоносная активность и в параметрах задачи Постоянная защита файлов установлен флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных**.
- Если в ходе выполнения задачи Защита от шифрования со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена активность вредоносного шифрования.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает критическое событие блокировки узла. Любые попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет недоверенные компьютеры из хранилища через 30 минут после добавления. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка недоверенных. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

Обратите внимание, что в случае наложения запрета доступа к управлению хранилищами какому-либо пользователю, хранилище Заблокированных узлов останется доступным. Настройки хранилища Заблокированных узлов не могут быть изменены только если пользователь не имеет **прав на изменение** для управления Kaspersky Industrial CyberSecurity for Nodes 2.5. (см. раздел "Настройка прав доступа для Kaspersky Industrial CyberSecurity for Nodes 2.5 и службы Kaspersky Security" на стр. 81).

Включение блокирования доступа к сетевым файловым ресурсам

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище заблокированных узлов и заблокировать этим узлам доступ к сетевым файловым ресурсам, необходимо, чтобы хотя бы одна из следующих задач работала 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 блоке **Постоянная защита файлов**.

Откроется окно **Постоянная защита компьютера**.

3. В блоке **Интеграция с другими компонентами** установите флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных**, если вы хотите, чтобы

программа Kaspersky Industrial CyberSecurity for Nodes 2.5 блокировала доступ к сетевым файловым ресурсам для компьютеров, со стороны которых в ходе работы задачи Постоянная защита файлов обнаружена вредоносная активность.

4. Если задача не запустилась, откройте закладку **Управление задачами**:
 - a. Установите флажок **Запускать задачу по расписанию**.
 - b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
5. В окне **Постоянная защита компьютера** 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 блоке **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

3. Если задача не запустилась, откройте закладку **Управление задачами**:
 - a. Установите флажок **Запускать задачу по расписанию**.
 - b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
4. В окне **Защита от шифрования** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройка параметров хранилища заблокированных узлов

► Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).
2. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке **Хранилища**.

Откроется окно **Параметры хранилищ**.

Вы можете настроить параметры блокирования компьютеров для группы управляемых компьютеров через параметры политики. Чтобы настроить период блокирования узлов, откройте **<Имя политики> > Дополнительные возможности** и нажмите кнопку **Настройка**. На закладке **Заблокированные узлы** настройте параметры блокирования удаленных компьютеров. Список заблокированных компьютеров недоступен в параметрах политики.

3. Откройте закладку **Заблокированные узлы**.

4. В блоке **Действия** укажите количество суток, часов и минут, через которые, с момента блокировки, заблокированные компьютеры получают доступ к сетевым файловым ресурсам.
5. Нажмите кнопку **Список недоверенных узлов**.
6. Выполните одно из следующих действий:
 - В открывшемся окне **Список недоверенных компьютеров** выберите компьютеры, доступ которых вы хотите восстановить, и нажмите на кнопку **Удалить из списка**.
 - Нажмите на кнопку **Очистить весь список**, чтобы удалить компьютеры из списка недоверенных и восстановить доступ для всех заблокированных узлов.
7. Нажмите кнопку **ОК**.
Выбранные компьютеры будут разблокированы и удалены из списка заблокированных.
8. Нажмите на кнопку **ОК** в окне **Параметры хранилищ**.
Настроенные параметры заблокированных узлов будут сохранены.

О настройке журналов и уведомлений

В Консоли администрирования Kaspersky Security Center вы можете настроить уведомление администратора и пользователей о следующих событиях, связанных с работой Kaspersky Industrial CyberSecurity for Nodes 2.5 и состоянием антивирусной защиты защищаемого компьютера:

- администратор может получать информацию о событиях выбранных типов;
- пользователи локальной сети, которые обращаются к защищаемому компьютеру, и терминальные пользователи компьютера могут получать информацию о событиях типа *Обнаружен объект*.

Уведомления о событиях Kaspersky Industrial CyberSecurity for Nodes 2.5 можно настроить либо для отдельного компьютера в окне **Свойства: <Имя компьютера>** для выбранного компьютера, либо для группы компьютеров в окне **Свойства: <Имя политики>** для выбранной группы администрирования.

На закладке **События** или в окне **Параметры уведомлений** вы можете настраивать следующие типы уведомлений:

- На закладке **События** (стандартная закладка программы Kaspersky Security Center) вы можете настраивать уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений содержится в справке *Kaspersky Security Center*.
- В окне **Параметры уведомлений** вы можете настраивать уведомления как администратора, так и пользователей.

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

Уведомления о событиях некоторых типов вы можете настраивать только на закладке или в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите уведомления о событиях одного типа одним способом и на закладке **События**, и в окне **Параметры уведомлений**, системный администратор будет получать уведомления об этих событиях указанным способом дважды.

В этом разделе

Настройка параметров журналов.....	156
Журнал безопасности.....	157
Настройка параметров интеграции с SIEM	157
Настройка параметров уведомлений.....	161
Настройка формирования инцидентов и взаимодействия с Сервером администрирования	162

Настройка параметров журналов

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes*.

► Чтобы настроить параметры журналов Kaspersky Industrial CyberSecurity for Nodes 2.5, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.
4. В окне **Параметры журналов** настройте следующие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 согласно вашим требованиям:
 - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
 - а. В списке **Компонент** выберите функциональный компонент Kaspersky Industrial CyberSecurity for Nodes 2.5, уровень детализации событий которого вы хотите указать.
 - б. Чтобы задать уровень детализации в журналах выполнения задач и журнале системного аудита выбранного функционального компонента, выберите нужный уровень в списке **Уровень важности**.
 - Чтобы изменить местоположение журналов по умолчанию, укажите полный путь к папке или выберите папку с помощью кнопки **Обзор**.
 - Укажите, сколько дней будут храниться журналы выполнения задач.
 - Укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита**.
5. Нажмите на кнопку **ОК**.

Настроенные параметры журналов будут сохранены.

Журнал безопасности

Kaspersky Industrial CyberSecurity for Nodes 2.5 ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера и проверки по требованию, задач Мониторинг файловых операций, Контроль запуска программ).

Вы можете очистить журнал безопасности, так же, как и журнал системного аудита. При этом Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие системного аудита об очистке журнала безопасности.

Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и снизить риск деградации системы в результате увеличения объемов журналов программы, вы можете настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия в рамках управления журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: этот режим предполагает, что все события выполнения задач, публикация которых настроенная в параметрах журналов, а также все события системного аудита продолжают храниться на локальном компьютере даже после отправки в SIEM.

Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: этот режим предполагает, что все события, зарегистрированные в ходе работы программы и опубликованные в SIEM, будут удалены с локального компьютера.

Программа никогда не удаляет локальные версии журнала нарушений безопасности

Kaspersky Industrial CyberSecurity for Nodes 2.5 может конвертировать события в журналах программы в форматы, поддерживаемые syslog-компьютером, для передачи событий и их успешного распознавания на стороне SIEM. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий в SIEM, вы можете задать параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если подключение к основному syslog-серверу или его использование недоступны.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и отключать интеграцию с SIEM, а также настраивать параметры функциональности (см. таблицу ниже).

Таблица 25. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.
Протокол подключения	TCP	С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам

Параметр	Значение по умолчанию	Описание
		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.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.
Откроется окно **Параметры журналов и уведомлений**.
4. Выберите закладку **Интеграция с SIEM**.

Ошибка! Используйте закладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

5. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

Если флажок установлен, программа выполняет отправку публикуемых событий в SIEM в соответствии с настроенными параметрами интеграции с SIEM.

Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

По умолчанию флажок снят.

6. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

Флажок включает или отключает удаление локальных копий журналов по их отправке в SIEM.

Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы в SIEM. Рекомендуется использовать этот режим на маломощных компьютерах.

Если флажок снят, программа только отправляет события в SIEM. Копии журналов продолжают храниться локально.

По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

7. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события по работе программы для их отправки в SIEM.

По умолчанию программа выполняет конвертацию в формат структурированных данных.

8. В блоке **Параметры соединения**:

- Укажите протокол подключения к SIEM.
- Укажите параметры соединения с основным syslog-сервером.
Вы можете указать IP-адрес только в формате IPv4.
- Если требуется, установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер недоступна.
 - Укажите параметры подключения к зеркальному syslog-серверу. **IP-адрес** и **Порт**.

Поля **IP-адрес** и **Порт** для зеркального syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

Вы можете указать IP-адрес только в формате IPv4.

9. Нажмите на кнопку **ОК**.

Настроенные параметры интеграции с SIEM будут применены.

Настройка параметров уведомлений

► Чтобы настроить параметры уведомлений Kaspersky Industrial CyberSecurity for Nodes 2.5, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Журналы и уведомления** в блоке **Уведомления о событиях** нажмите на кнопку **Настройка**.
4. В окне **Параметры уведомлений** настройте следующие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 согласно вашим требованиям:
 - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.
 - В блоке **Уведомление пользователей** настройте способ уведомления пользователя. Если требуется, задайте текст сообщения для уведомления.
 - В блоке **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст сообщения для уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
 - В блоке **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Industrial CyberSecurity for Nodes 2.5 регистрирует события "**Базы программы устарели**", "**Базы программы сильно устарели**" и "**Проверка важных областей давно не выполнялась**":
 - **Базы программы сервустарели (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 компьютера давно не выполнялась (сут).**
Количество дней с момента последнего успешного завершения задачи Проверка

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

важных областей.

По умолчанию установлено 30 дней.

5. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

Настройка формирования инцидентов и взаимодействия с Сервером администрирования

► Чтобы выбрать типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет передавать на Сервер администрирования Kaspersky Security Center, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 Журналы и уведомления в блоке Взаимодействие с Сервером администрирования нажмите кнопку **Настройка**.

Откроется окно **Сетевые списки Сервера администрирования**.

4. В открывшемся окне выберите типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes 2.5 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.

Чтобы настроить параметры задачи Контроль Wi-Fi для группы компьютеров с помощью политики Kaspersky Security Center, обязательно включите отправку данных о доступных сетях Wi-Fi на Сервер администрирования.

5. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 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 компьютерах.

► Чтобы настроить уведомления, на основании которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет формировать инциденты в Kaspersky Security Center, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Журналы и уведомления** в блоке **Инциденты** нажмите кнопку **Настройка**.
Откроется окно **Инциденты**.
4. В окне **Инциденты** измените выборку событий, представленных в таблице ниже, на основании которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет формировать инциденты:

Таблица 26. Список событий для формирования инцидентов

Событие	Значение по умолчанию
Проект ПЛК не соответствует эталонному проекту.	Выбрано
Не удалось сравнить проект ПЛК с эталонным.	Выбрано
Не удалось получить данные о проекте ПЛК.	Выбрано
Срок действия лицензии истек.	Не выбрано
Нарушено Лицензионное соглашение	Выбрано
Не обновлено	Не выбрано

Базы программы повреждены	Не выбрано
Базы программы устарели	Не выбрано
Базы программы сильно устарели	Не выбрано
Целостность модулей программы нарушена	Выбрано
Компьютер добавлен в список недоверенных	Выбрано
Запуск программы запрещен	Не выбрано
Запуск программы не обработан	Не выбрано
Подключение устройства не обработано	Выбрано
Обнаружено и запрещено недоверенное устройство	Выбрано
Обнаружен зараженный объект или объект другого типа	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

5. Нажмите на кнопку **ОК** в окне **Параметры программы**.

Параметры формирования инцидентов будут сохранены.

Постоянная защита компьютера

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

В этом разделе

Постоянная защита файлов	165
Использование KSN	181
Защита от эксплойтов	188

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	165
Настройка задачи "Постоянная защита файлов"	166
Применение эвристического анализатора	168
Выбор режима защиты	169
Область защиты в задаче Постоянная защита файлов.....	170
Настройка параметров безопасности вручную	173

О задаче Постоянная защита файлов

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

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

При записи или считывании записанного файла любой программой на компьютере Kaspersky Industrial CyberSecurity for Nodes 2.5 перехватывает этот файл, проверяет его на наличие угроз компьютерной безопасности и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные

по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Kaspersky Industrial CyberSecurity for Nodes возвращает файл программе, если он не заражен или успешно вылечен.

Kaspersky Industrial CyberSecurity for Nodes 2.5 также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem для Linux. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих настройках.

Настройка задачи Постоянная защита файлов

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

Таблица 27. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь компьютер, исключая виртуальные диски.	Вы можете ограничить область защиты.
Уровень безопасности	Единый для всей области защиты; соответствует уровню безопасности Рекомендуемый .	Для выбранных узлов в дереве файловых ресурсов компьютера вы можете: <ul style="list-style-type: none"> • применить другой предустановленный уровень безопасности; • вручную изменить уровень безопасности; • сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Режим защиты объектов	При открытии и изменении.	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет их.
Эвристический анализатор	Применяется уровень безопасности Средний .	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Применять доверенную зону.	Применяется.	Единый список исключений, который вы можете применять в выбранных задачах.
Использование служб KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Расписание запуска задачи	При запуске программы	Вы можете настраивать параметры запуска задачи по расписанию.
Блокировать компьютеры, с которых ведется вредоносная активность	Не применяется	Вы можете включить добавление компьютеров, со стороны которых выявлена вредоносная активность, в список недоверенных узлов.

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

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Постоянная защита файлов** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.
Откроется окно **Постоянная защита файлов**.
4. Настройте следующие параметры задачи:
 - На закладке **Общие**:
 - Режим защиты (см. раздел "Выбор режима защиты" на стр. [169](#));
 - Применение эвристического анализатора (на стр. [168](#)).
 - Параметры интеграции с другими компонентами Kaspersky Industrial CyberSecurity for Nodes 2.5.
 - На закладке **Управление задачами**:
 - Запуск задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. [133](#)).
5. Выберите закладку **Область защиты** и выполните следующие действия:
 - Нажмите кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Область защиты в задаче "Постоянная защита файлов" на стр. [170](#)).
 - В открывшемся окне выберите, что вы хотите включить в область защиты задачи:
 - **Предопределенная область**
 - **Диск, папка или сетевое расположение**
 - **Файл**
 - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности" на стр. [171](#)) или настройте параметры защиты объектов вручную (см. раздел "Настройка параметров безопасности вручную" на стр. [173](#)).

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

6. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

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

Применение эвристического анализатора

Вы можете использовать эвристический анализатор и выбрать уровень анализа для задач Kaspersky Industrial CyberSecurity for Nodes 2.5.

► Чтобы настроить эвристический анализатор, выполните следующие действия:

1. Откройте параметры программы (см. раздел "О способах управления Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center" на стр. [136](#)) или настройки политики (см. раздел "Настройка политики" на стр. [90](#)), для которой вы хотите настроить использование эвристического анализатора.

2. 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.

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

Существуют следующие уровни детализации проверки:

- **Поверхностный.** Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний.** Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
Этот уровень выбран по умолчанию.
- **Глубокий.** Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества

ложных срабатываний.

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

4. Нажмите на кнопку **ОК**.

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

Выбор режима защиты объектов

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

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

► Чтобы выбрать режим защиты объектов, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. 90).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 103).

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 **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

Откроется окно **Постоянная защита файлов**.

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

- **Интеллектуальный режим**

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

- **При открытии и изменении.**

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

Данный вариант выбран по умолчанию.

- **При открытии.**

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

- **При выполнении.**

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

5. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

Область защиты в задаче Постоянная защита файлов

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

В этом разделе

Предопределенные области защиты.....	170
Выбор предустановленных уровней безопасности	171

Предопределенные области защиты

Файловые ресурсы защищаемого компьютера отображаются в параметрах задачи **Постоянная защита файлов** на закладке **Область защиты**.

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

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

- **Локальные жесткие диски.** Kaspersky Industrial CyberSecurity for Nodes 2.5 защищает файлы на жестких дисках компьютера.
- **Съемные диски.** Kaspersky Industrial CyberSecurity for Nodes 2.5 защищает файлы на внешних устройствах, например, на компакт-дисках или флеш-накопителях. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.

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

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

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

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на компьютере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Выбор предустановленных уровней безопасности

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

Максимальное быстродействие

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

Рекомендуемый

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

Максимальная защита

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

Таблица 28. Предустановленные уровни безопасности и соответствующие им

значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	По расширению	По формату	По формату
Проверка только новых и измененных файлов	Включена	Включена	Выключено
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и выполнить рекомендуемое действие.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Проверять загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	<ul style="list-style-type: none"> упакованные объекты* * Только новые и измененные 	<ul style="list-style-type: none"> SFX-архивы* упакованные объекты* Вложенные OLE- объекты* * Только новые и измененные 	<ul style="list-style-type: none"> SFX-архивы* упакованные объекты* Вложенные OLE- объекты* *Все объекты

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

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

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

Откроется окно **Постоянная защита файлов**.

4. На закладке **Область защиты**, выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

Откроется окно **Настройка параметров постоянной защиты файлов**.

5. Выберите требуемый уровень безопасности в раскрывающемся списке:

- **Максимальная защита**
- **Рекомендуемый**
- **Максимальное быстрое действие**

6. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

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

Настройка параметров безопасности вручную

По умолчанию в задаче **Постоянная защита файлов** применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют значениям предустановленного уровня безопасности **Рекомендуемый** (см. раздел "Выбор предустановленных уровней безопасности" на стр. [171](#)).

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

При работе с деревом файловых ресурсов компьютера параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► Чтобы вручную настроить параметры безопасности выбранного узла, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.
Откроется окно **Постоянная защита файлов**.
4. На закладке **Область защиты**, выберите узел, параметры безопасности которого вы хотите настроить, и нажмите кнопку **Настроить**.
Откроется окно **Настройка параметров постоянной защиты файлов**.
5. На закладке **Уровень безопасности** вы можете выбрать любой существующий уровень или нажать кнопку **Настройка**, чтобы создать пользовательскую конфигурацию.
6. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями.
 - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. [175](#))
 - Действия (см. раздел "Настройка действий" на стр. [177](#))
 - Производительность (см. раздел "Настройка производительности" на стр. [179](#))
7. Нажмите кнопку **Сохранить** в окне **Настройка области защиты**.
Новые параметры области защиты будут сохранены.

Настройка общих параметров задачи

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

1. Откройте окно **Настройка постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. [173](#)).
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 2.5 проверяет все объекты.

- **Объекты, проверяемые по формату.**

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

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes 2.5.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

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

Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes 2.5.

- **Объекты, проверяемые по указанному списку расширений.**

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

- **Проверять загрузочные секторы дисков и MBR.**

Включение защиты загрузочных секторов дисков и главных загрузочных записей.

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

По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

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

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

По умолчанию флажок установлен.

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

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

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

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

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

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

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

- **Все / Только новые архивы.**

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

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые SFX-архивы.**

Проверка самораспаковывающихся архивов.

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

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

Значение по умолчанию зависит от выбранного уровня безопасности.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

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

1. Откройте окно **Настройка постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. [173](#)).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать.**

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

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

- **Блокировать доступ.**

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

- **Выполнять дополнительное действие.**

Выберите действие из раскрывающегося списка:

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

4. Выберите действие над возможно зараженными объектами:

- **Только сообщать.**

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

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

- **Блокировать доступ.**

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

- **Выполнять дополнительное действие.**

Выберите действие из раскрывающегося списка:

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

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

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

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

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

соответственно указанным типам объектов.

По умолчанию флажок снят.

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

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

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

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

- 7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

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

1. Откройте окно **Настройка постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. [173](#)).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
 - Снимите или установите флажок **Исключать файлы**.

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

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

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

По умолчанию флажок снят.

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

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

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

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

По умолчанию флажок снят.

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

4. В блоке **Дополнительные параметры**:

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

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

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

Если флажок снят, максимальная продолжительность проверки не ограничена.

По умолчанию флажок установлен.

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

Исключение из проверки составных объектов больше указанного размера.

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

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

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

- **Использовать технологию iSwift.**

Проверка только новых или измененных с момента последней проверки объектов файловой системы 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, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

- **Использовать технологию iChecker.**

Проверка только новых или измененных с момента последней проверки файлов.

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

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы,

не учитывая дату создания и изменения.

По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Использование KSN

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

В этом разделе

О задаче Использование KSN	181
Настройка параметров задачи Использование KSN	183
Настройка обработки данных	186
Настройка передачи дополнительных данных	188

О задаче Использование KSN

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

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

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

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

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

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

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

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

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

Kaspersky Private Security Network

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

Если вы используете Локальный KSN на защищаемом компьютере, в окне **Обработка данных** (см. раздел "Настройка обработки данных" на стр. [186](#)) задачи Использование KSN вы можете прочитать Положение о KPSN и включить использование компонента, установив флажок **Я принимаю условия участия в Kaspersky Private Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KPSN (запросы безопасности, статистические данные), в службы KSN.

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

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

Отзыв согласия с Положением о KSN

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

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

Настройка параметров задачи Использование KSN

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

Таблица 29. Параметры задачи Использование KSN по умолчанию

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет выполнять над объектами, имеющими репутацию недоверенных в KSN.
Отправка данных	Контрольная сумма файла (MD5-хеш) рассчитывается для файлов, размер которых не превышает 2 МБ.	Вы можете указывать максимальный размер файлов, для которых рассчитывается контрольная сумма по алгоритму MD5 для отправки в KSN. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывает MD5-хеш для файлов любого размера.
Положение о KSN	Флажок Я принимаю условия использования Kaspersky Security Network снят.	Решите, хотите ли вы использовать KSN после установки. Вы можете изменять свое решение в любой момент.
Разрешить отправку статистики Kaspersky Security Network	Установлен (применяется, только если принято Положение о KSN)	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок.

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.
Расписание запуска задачи	Первый запуск не определен.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.
Использовать Kaspersky Security Center как прокси-сервер KSN	Выбрано	По умолчанию все данные отправляются в KSN через Kaspersky Security Center.

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

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Постоянная защита компьютера** нажмите кнопку **Настройка** в блоке **Использование KSN**.

Откроется окно **Использование KSN**.

4. На закладке **Общие** настройте следующие параметры задачи:
 - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Industrial CyberSecurity for Nodes 2.5 необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
 - **Удалить**
Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.
Этот вариант выбран по умолчанию.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

- **Фиксировать информацию в отчете**

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

- В блоке **Передача данных**, выполните следующие действия:

- Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.

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

Продолжительность расчета контрольной суммы зависит от размера файла.

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

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

По умолчанию флажок установлен.

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

- В блоке **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](#).

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

Программа будет запускать задачу Использование KSN по расписанию.

6. Настройте обработку данных (см. раздел "Настройка обработки данных" на стр. [186](#)) перед запуском задачи.

7. Нажмите на кнопку **ОК**.

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

Настройка обработки данных

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

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Постоянная защита компьютера** нажмите на кнопку **Обработка данных** в блоке **Использование KSN**.

Откроется окно **Обработка данных**.

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

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

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

По умолчанию флажок снят.

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

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

Чтобы включить службы KSN, примите Положение о KSN снова.

6. Для повышения уровня защиты следующие флажки установлены по умолчанию:

- **Разрешить отправку данных о проверяемых файлах**

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

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

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

По умолчанию флажок установлен.

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

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

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

По умолчанию флажок установлен.

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

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

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

7. Нажмите на кнопку **ОК**.

Настройка передачи дополнительных данных

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





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

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

Соответствующие флажки можно установить или снять, только если установлен флажок **Я принимаю условия участия в Kaspersky Security Network**.

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

Таблица 30. 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"
	<ul style="list-style-type: none"> • отправляются запросы репутации • действия с флажком доступны 	<ul style="list-style-type: none"> • отправляется дополнительная статистика • действия с флажком доступны
	<ul style="list-style-type: none"> • не отправляются запросы репутации • действия с флажком недоступны 	<ul style="list-style-type: none"> • не отправляется дополнительная статистика • действия с флажком недоступны
	<ul style="list-style-type: none"> • не отправляются запросы репутации • действия с флажком доступны 	<ul style="list-style-type: none"> • не отправляется дополнительная статистика • действия с флажком доступны
	<ul style="list-style-type: none"> • не отправляются запросы репутации • действия с флажком недоступны 	<ul style="list-style-type: none"> • не отправляется дополнительная статистика • действия с флажком недоступны

Защита от эксплойтов

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

В этом разделе

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

О защите от эксплойтов.....	189
Настройка параметров защиты памяти процессов	190
Добавление защищаемого процесса	192
Техники защиты от эксплойтов.....	193

О защите от эксплойтов

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

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

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Industrial CyberSecurity for Nodes 2.5, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, необходимо завершить данный процесс. Может потребоваться перезагрузка компьютера (например, если защищается системный процесс).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;
- удалить процесс из списка защищаемых и перезапустить его.

Служба Kaspersky Security Exploit Prevention

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

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

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

Режимы защиты от эксплойтов

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

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

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

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

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

Настройка параметров защиты памяти процессов

► Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Постоянная защита компьютера** нажмите кнопку **Настройка** в блоке **Защита от эксплойтов**.

Откроется окно **Защита от эксплойтов**.

4. В блоке **Защита памяти процессов** настройте следующие параметры:

- **Защищать процессы от эксплуатации уязвимостей в режиме.**

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

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

По умолчанию флажок снят.

- **Завершать скомпрометированные процессы**

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

- **Только сообщать о компрометации процесса**

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

Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать о компрометации процесса**.

5. В блоке **Профилактические действия** настройте следующие параметры:

- **Сообщать о скомпрометированных процессах посредством службы терминалов.**

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

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

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

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

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

По умолчанию флажок установлен.

6. Нажмите на кнопку **ОК**.

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

Добавление защищаемого процесса

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

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

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. 90).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 103).

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 **Постоянная защита компьютера** нажмите кнопку **Настройка** в блоке **Защита от эксплойтов**.
Откроется окно **Защита от эксплойтов**.
4. На закладке **Защищаемые процессы**, нажмите на кнопку **Обзор**.
Откроется стандартное окно Microsoft Windows **Открыть**.
5. Выберите процесс, который вы хотите добавить в список.
6. Нажмите на кнопку **Открыть**.
7. Нажмите на кнопку **Добавить**.
Указанный процесс добавится в список защищаемых процессов.
8. Выберите добавленный процесс и нажмите на кнопку **Указать техники снижения рисков**.
Откроется окно **Техники защиты от эксплойтов**.
9. Выберите один из вариантов применения техник снижения рисков:

- **Применять все доступные техники защиты от эксплойта**

Если выбран этот вариант, редактирование списка недоступно, все техники применяются по умолчанию.

- **Применять указанные техники защиты от эксплойта**

Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска:

- Установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
- Установите или снимите флажок **Применять технику Attack Surface Reduction**.

10. Настройте параметры работы для техники защиты Attack Surface Reduction:

- Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать загрузку модулей**.
- В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, запуск модулей в которых вы хотите разрешить:
 - Интернет
 - Интранет
 - Доверенные сайты
 - Сайты с ограниченным доступом
 - Компьютер

Данные параметры применимы только для Internet Explorer®.

11. Нажмите на кнопку **ОК**.

Процесс будет добавлен в область защиты задачи.

Техники защиты от эксплойтов

Таблица 31. 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 Exeption Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.

Техника защиты от эксплойтов	Описание
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll
Heap Spray Allocation (Heapspray)	Защита от выделения памяти под исполнение вредоносного кода.
Execution Flow Simulation (Anti Return Oriented Programming)	Обнаружение подозрительных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile).
Attack Surface Reduction (ASR)	Блокирование запуска уязвимых модулей через защищаемый процесс.
Anti Process Hollowing (Hollowing)	Защита от создания и запуска вредоносных копий доверенных процессов.
Anti AtomBombing (APC)	Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC).
Anti CreateRemoteThread (RThreadRemote)	Сторонний процесс создал поток в защищаемом процессе.
Anti CreateRemoteThread (RThreadRemote)	Защита внедрения потока защищаемого процесса в другой процесс.

Контроль активности на компьютерах

Этот раздел содержит информацию о функциональности Kaspersky Industrial CyberSecurity for Nodes 2.5, которая позволяет контролировать запуски программ, а также подключения защищаемого компьютера к сетям Wi-Fi.

В этом разделе

Управление запуском программ из Kaspersky Security Center	195
Контроль Wi-Fi.....	214

Управление запуском программ из Kaspersky Security Center

Вы можете запрещать или разрешать запуск программ на всех компьютерах в сети организации, формируя единые списки правил контроля запуска программ на стороне Kaspersky Security Center для групп компьютеров.

В этом разделе

Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center	195
Настройка параметров задачи Контроль запуска программ	196
О Контроле пакетов установки	201
Настройка контроля пакетов установки.....	203
Включение режима Разрешение по умолчанию	206
О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center	207

Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center

Правила контроля запуска программ, настроенные в политике, применяются ко всем компьютерам группы администрирования. Если в одну группу администрирования добавлены компьютеры разных типов, для контроля запуска программ на каждом из них могут потребоваться индивидуальные списки правил. Для того, чтобы разграничить применение политики к компьютерам внутри одной группы администрирования, вы можете использовать *профили политики*.

Рекомендуется применять профили политики для настройки правил контроля запуска программ на компьютерах разных типов внутри одной группы администрирования, управляемой единой политикой. Это

позволяет оптимизировать защиту компьютера, так как заданные правила контролируют запуски только тех программ, которые характерны для данного типа компьютера.

Профили политики применяются к компьютерам группы администрирования в соответствии с назначенными для них *тегами*. Вы можете настроить профиль политики для всех компьютеров группы, имеющих общий тег.

Подробная информация о тегах и профилях политики, а также инструкции по работе с ними содержатся в справке *Kaspersky Security Center*.

► Чтобы применить профиль политики в задаче *Контроль запуска программ*, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для которой хотите настроить применение профилей политики.
2. Назначьте теги для каждого компьютера, входящего в группу администрирования, в соответствии с типом компьютера. Для этого выполните следующие действия:
 - В панели результатов выбранной группы администрирования откройте закладку **Устройства** и выберите компьютер, для которого хотите назначить теги. В окне **Свойства: <Имя компьютера>** выбранного компьютера откройте блок **Теги** и сформируйте список тегов. Нажмите на кнопку **ОК**.
3. Создайте профиль политики и настройте его применение для защиты компьютеров внутри группы администрирования. Для этого выполните следующие действия:
 - В панели результатов выбранной группы администрирования откройте закладку **Политики** и выберите политику, для которой хотите настроить применение профилей. В окне **Свойства: <Имя политики>** выбранной политики откройте раздел **Профили политики** и нажмите на кнопку **Добавить**, чтобы создать новый профиль. Откроется окно **Свойства: <Имя политики>**. Выполните следующие действия:
 - a. В разделе **Правила активации** настройте область применения профиля и укажите условия, при которых профиль будет активирован.
 - b. В разделе **Контроль запуска программ** настройте списки правил контроля запуска программ для редактируемого профиля.
 - c. Нажмите на кнопку **ОК**.
4. В окне **Свойства: <Имя политики>** нажмите на кнопку **ОК**.

Настроенный профиль будет применен в политике для задачи *Контроль запуска программ*.

Настройка параметров задачи *Контроль запуска программ*

Вы можете изменять значения параметров задачи *Контроль запуска программ*, заданных по умолчанию (см. таблицу ниже).

Таблица 32. Параметры задачи Контроль запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	Только статистика. Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим Активный для защиты компьютера после того, как будет сформирован окончательный список правил.
Управление правилами	Заменить правилами политики локальные правила.	Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на локальном компьютере.
Область применения правил	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.
Использование KSN	Данные о репутации программ в KSN не используются.	Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.
Автоматически разрешать распространение для программ и пакетов из списка	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию разрешено только распространение программ с помощью службы Windows Installer.
Разрешение распространения программ через Windows Installer	Применяется.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются через Windows Installer.
Запретить запуск командных интерпретаторов без команд к исполнению	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.
Запуск задачи	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически при старте Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

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

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.

Откроется окно **Контроль запуска программ**.

4. На закладке **Общие** в блоке **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 2.5 контролирует запуск программ с помощью заданных правил.
- **Только статистика.** Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует запуск программ с помощью заданных правил, а только фиксирует в журнале выполнения задач информацию о запусках программ. Запуск всех программ разрешен. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации, зафиксированной в журнале выполнения задач.

По умолчанию задача **Контроль запуска программ** запускается в режиме **Только статистика**.

- Снимите или установите флажок **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

Флажок включает или выключает контроль повторного запуска программ на основе записей кеша о прецедентах.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает или разрешает выполнение повторно запущенной программы на основе решения, которое было принято при первом запуске программы задачей контроля запуска программ. Например, если первый запуск программы был разрешен правилами

контроля запуска программ, запись об этом событии сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки на наличие разрешающих правил.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет программу при каждом ее последующем запуске заново.

По умолчанию флажок установлен.

- Снимите или установите флажок **Запретить запуск интерпретаторов команд при отсутствии команд**.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает запуск интерпретатора командной строки, даже если запуск интерпретатора разрешен. Запуск командной строки без команд разрешается только при выполнении обоих условий:

- Запуск интерпретатора командной строки разрешен.
- Выполняемая команда разрешена.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает только разрешающие правила для запуска командной строки. Запуск блокируется, если не применено разрешающее правило, или выполняемый процесс не имеет статуса доверенного в KSN. Если разрешающее правило применено, или у процесса есть статус доверенного в KSN, запуск командной строки разрешается как с командой, так и без нее.

Kaspersky Industrial CyberSecurity for Nodes 2.5 работает со следующими интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

5. В блоке **Правила** настройте параметры применения правил:

- а. Нажмите кнопку **Список правил**, чтобы добавить разрешающие правила контроля запуска задач.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не распознает путь, включающий наклонную черту "/". Используйте обратную наклонную черту "\", чтобы правильно ввести путь.

- б. Выберите режим применения правил:

- **Заменить правилами политики локальные правила.**

Программа применяет список правил, заданных в политике, для централизованного контроля запусков программ на группе компьютеров. 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.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет два предопределенных правила, которые разрешают запуск скриптов, пакетов MSI и файлов запуска по сертификату.

6. В блоке **Область применения правил** задайте следующие параметры:

- **Использовать правила для исполняемых файлов.**

Флажок включает / выключает контроль запуска исполняемых файлов программ.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов программ с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов программ с помощью заданных правил. Запуск исполняемых файлов программ разрешен.

По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей.**

Флажок включает/выключает контроль загрузки DLL-модулей.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает или запрещает загрузку DLL-модулей с помощью заданных правил, в параметрах которых указана область применения "Исполняемые файлы".

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI.**

Флажок включает или выключает контроль запуска скриптов и пакетов MSI.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

По умолчанию флажок установлен.

7. В блоке **Использование KSN** настройте следующие параметры запуска программ:

- **Не разрешать запуск программ, недоверенных в KSN.**

Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые попадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые попадают программы.

По умолчанию флажок снят.

- **Разрешать запуск программ, доверенных в KSN.**

Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает запуск программ, имеющих статус доверенных в KSN. При этом запрещающие правила контроля запуска программ, под которые попадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые попадают программы.

По умолчанию флажок снят.

- Пользователи и/или группы пользователей, которым разрешен запуск доверенных в KSN программ.

8. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка контроля пакетов установки" на стр. [203](#)).

9. На закладке **Управление задачами** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. [133](#)).

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

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

О Контроле пакетов установки

Формирование правил контроля запуска программ может значительно усложняться, если вам требуется учитывать распространение программного обеспечения на защищаемом компьютере: например, для компьютеров, на которых выполняется периодическое автоматическое обновление установленных программ. В этом случае требуется обновлять списки разрешающих правил при каждом обновлении программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались запуски новых файлов, созданных в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения вы можете использовать соответствующую подсистему задачи Контроль запуска программ.

Подсистема Контроль пакетов установки реализована в виде дополнительного списка исключений. Вы можете добавлять в этот список *пакеты установки* (далее "доверенные пакеты") – программа будет

разрешать распаковку доверенных пакетов и автоматический запуск программного обеспечения, установленного и измененного доверенным пакетом.

Учитывайте, что Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует только полный цикл распространения программного обеспечения. Программа не сможет корректно обработать запуски файлов, измененных доверенным дистрибутивом, если при первом запуске такого пакета установки контроль распространения программного обеспечения отключен, или не установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в настройках задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш контроля пакетов установки

Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет связь между файлами, созданными при распространении программного обеспечения, и доверенными пакетами с помощью динамического формирования *кеша контроля пакетов установки* (далее – "кеш распространения"). При первом запуске доверенного пакета, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает все файлы, созданные при распространении программного обеспечения с помощью данного пакета, и сохраняет их контрольные суммы и полные пути в кеше распространения. В дальнейшем запуски всех файлов, сохраненных в кеше распространения, разрешаются автоматически.

Вы не можете просматривать, очищать, а также вручную изменять кеш распространения через пользовательский интерфейс. Kaspersky Industrial CyberSecurity for Nodes 2.5 самостоятельно наполняет его, а также контролирует его актуальность.

Вы можете экспортировать кеш распространения в конфигурационный файл (в формате XML), а также полностью очищать кеш распространения с помощью команд командной строки.

Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

Чтобы полностью очистить кеш распространения, выполните команду:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Industrial CyberSecurity for Nodes 2.5 обновляет кеш распространения раз в сутки. Если значение полного пути или контрольной суммы ранее разрешенного файла изменены, программа удаляет запись о таком файле из кеша распространения. При активном режиме работы задачи Контроль запуска программ, дальнейшие запуски такого файла будут заблокированы.

Взаимодействие с основным списком правил контроля запуска программ

Список доверенных пакетов подсистемы Контроль 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 попадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если для таких пакетов и файлов отсутствуют правила в основном списке правил контроля запуска программ.

Использование KSN-заключений

Недоверенные KSN-заключения имеют больший приоритет, чем исключение Контроля пакетов установки: распаковка доверенного пакета установки или запуск созданных и измененных им файлов будут заблокированы, если для таких файлов получено недоверенное заключение от KSN.

Настройка контроля пакетов установки

► Чтобы добавить доверенный пакет установки, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.

Откроется окно **Контроль запуска программ**.

4. На выбранной закладке установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

Если флажок установлен, программа автоматически разрешает запуск файлов, запущенных с помощью доверенных пакетов установки. Список программ и пакетов для установки, разрешенных к запуску, доступен для редактирования.

Если флажок снят, программа не применяет указанные в списке исключения.

По умолчанию флажок снят.

Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если установлен флажок **Использовать правила для исполняемых файлов** в параметрах задачи **Контроль запуска программ**.

5. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью Windows Installer**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью подсистемы Windows Installer.

Если флажок установлен, программа всегда разрешает запуск файлов, установленных с помощью Windows Installer.

Если флажок снят, использование Windows Installer для запуска программы не является критерием для разрешения такой программы.

По умолчанию флажок установлен.

Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью Windows Installer** рекомендуется снимать только в случае крайней необходимости. Снятие флажка может привести к проблемам при обновлении файлов операционной системы, а также блокированию запуска файлов, дочерних по отношению к доверенным пакетам установки.

6. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

Система контролирует запуск объектов со следующими расширениями:

- .exe
- .msi

По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения от доставки пакета на компьютер до факта установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки системы на компьютере.

7. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в раскрывшемся меню выберите один из доступных способов:

- **Добавить один вручную.**

а. Нажмите на кнопку **Обзор** и выберите файл запуска программы или пакет установки.

Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

б. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

- **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

Данный вариант выбран по умолчанию.

- **Добавить несколько по хешу**

Вы можете выбрать неограниченное число файлов запуска и пакетов установки и добавить их в список одновременно. Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

Используйте этот вариант, чтобы выбрать другой файл запуска или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла.**

Вы можете импортировать список доверенных пакетов установки из сохраненного конфигурационного файла. Для распознавания в Kaspersky Industrial CyberSecurity for Nodes 2.5 файл должен удовлетворять следующим параметрам:

- иметь текстовое расширение;
- содержать информацию в виде списка строк, каждая из которых – данные

для одного доверенного файла;

- содержать список, соответствующий одному из двух форматов:
 - <имя файла>:<хеш SHA256>;
 - <хеш SHA256>*<имя файла>.

В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

8. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск вложенных файлов будет разрешен.

Чтобы запретить запуск вложенных файлов, полностью удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

9. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Переход в режим разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и имеют доверенный статус в KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить режим только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.
4. На закладке **Общие** нажмите на кнопку **Список правил**.
Откроется окно **Правила контроля запуска программ**.

5. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите **Добавить одно правило**.
Откроется окно **Параметры правила**.
6. В поле **Название** введите название правила.
7. В раскрывающемся списке **Тип** выберите вариант **Разрешающее**.
8. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
 - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
 - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
9. В блоке **Критерий срабатывания правила** выберите **Путь к файлу**.
10. Введите следующую маску: `?:\`
11. В окне **Параметры правила** нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет режим разрешения по умолчанию.

О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center

Вы можете создавать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center сразу для всех компьютеров и групп компьютеров в сети организации. Этот вариант рекомендуется, если в сети организации нет эталонной машины, и вы не можете сформировать общий список правил с помощью задачи автоматического формирования разрешающих правил по программам, установленным на такой эталонной машине.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающие правила для скриптов и MSI, имеющих доверенный сертификат в операционной системе.
- Разрешающие правила исполняемых файлов, имеющих доверенный сертификат в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи автоматического формирования правил контроля запуска программ.

При использовании этого сценария групповая задача формирует для каждого компьютера в сети свой список правил контроля запуска программ и сохраняет эти списки в XML-файл в указанной общей папке сети. Далее вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ в политике Kaspersky Security Center. Вы также можете настроить автоматическое добавление созданных правил в список правил контроля запуска программ по завершении групповой задачи формирования правил контроля запуска программ.

Рекомендуется использовать этот сценарий, если необходимо сформировать списки правил контроля запуска программ в короткие сроки. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать только в том случае, если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

При применении политики контроля запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае, если применение общей сетевой папки в работе компьютеров сети не предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

- На основе отчета о событиях задачи, сформированного в Kaspersky Security Center по работе задачи Контроль запуска программ в режиме **Только статистика**.

При использовании этого сценария Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует запуски программ, но фиксирует в разделе **События** Kaspersky Security Center все запуски и блокировки запусков программ на всех компьютерах сети за период работы задачи контроля запуска программ в режиме **Только статистика**. Затем Kaspersky Security Center создает на основе журнала выполнения задачи единый список событий блокирования программ.

Вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнялись все возможные сценарии работы защищаемых компьютеров и групп компьютеров и хотя бы одна их перезагрузка. Далее при добавлении правил в задачу контроля запуска программ вы можете импортировать данные о запусках программ из сохраненного файла отчета о событиях Kaspersky Security Center (в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

Рекомендуется использовать этот сценарий, если сеть организации включает большое количество компьютеров разных типов (с различным набором установленных программ (см. раздел "Использование профиля при настройке задачи "Контроль запуска программ" в политике Kaspersky Security Center" на стр. [195](#)).

- На основе событий о блокировании программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на локальном компьютере должна находиться под управлением активной политики Kaspersky Security Center. Все события на локальном компьютере при этом передаются на Сервер администрирования.

Рекомендуется выполнять обновление списка правил при изменении состава программ, установленных на компьютерах сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется формировать обновленный список правил с помощью групповой задачи Формирование правил контроля запуска программ или с помощью политики Контроль запуска программ в режиме **Только статистика**, выполняемых на компьютерах тестовой группы администрирования. Тестовая группа администрирования включает компьютеры, необходимые для проверочного запуска новых программ перед их установкой на компьютеры сети.

Перед тем как добавить разрешающие правила, выберите один из доступных режимов применения правил (см. раздел "Настройка параметров задачи "Контроль запуска программ"" на стр. [196](#)). В списке правил политики Kaspersky Security Center отображаются только те правила, которые заданы в этой политике, вне зависимости от режима применения правил. В списке правил локального компьютера отображаются все применяющиеся правила - и локальные, и добавленные через политику.

В этом разделе

Создание разрешающих правил из событий Kaspersky Security Center [209](#)

Импорт правил контроля запуска программ из файла формата XML	210
Импорт правил из файла отчета Kaspersky Security Center о заблокированных запусках программ.....	212

Создание разрешающих правил из событий Kaspersky Security Center

► Чтобы сформировать разрешающие правила для программ с помощью опции *Создать разрешающие правила программ из событий Kaspersky Security Center в параметрах политики Контроль запуска программ*, 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. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
Откроется окно **Свойства: <Имя политики>**.
4. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.
5. На закладке **Общие** нажмите на кнопку **Список правил**.
Откроется окно **Правила контроля запуска программ**.
6. Нажмите кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
7. Выберите принцип добавления правил к списку уже заданных правил контроля запуска программ:
 - **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 окно **Формирование правил контроля запуска программ**.
8. Настройте следующие параметры запроса:
 - **адрес сервера администрирования**;
 - **порт**;
 - **пользователь**;
 - **пароль**.
9. Выберите типы событий, которые должны стать основой для задачи формирования:
 - **Режим Только статистика: запуск программы запрещен**.
 - **Запуск программы запрещен**.

10. Выберите период из раскрывающегося списка **Запрашивать события, созданные в течение периода**.
11. Нажмите на кнопку **Создать правила**.
12. Нажмите кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Список правил в политике Контроль запуска программ будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Если список правил контроля запуска программ уже задан в политике, Kaspersky Industrial CyberSecurity for Nodes 2.5 добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с повторяющимся хешем не добавляются, так как все правила в списке должны быть уникальными.

Импорт правил контроля запуска программ из файла формата XML

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 автоматического формирования разрешающих правил программа экспортирует созданные разрешающие правила в файлы формата XML в указанную общую сетевую папку. Каждый файл со списком правил создается на основе анализа запуска файлов и программ на каждом отдельном компьютере сети организации. Списки содержат разрешающие правила для запуска файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче автоматического формирования правил.

Процедура настройки параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 в Kaspersky Security Center не отличается от локальной настройки параметров этих компонентов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Industrial CyberSecurity for Nodes содержатся в соответствующих разделах *Руководства пользователя Kaspersky Industrial CyberSecurity for Nodes*.

► Чтобы задать разрешающие правила запуска программ для группы компьютеров на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:

1. На закладке **Задачи** в панели управления настраиваемой группы компьютеров создайте групповую задачу Формирование правил контроля запуска программ или выберите уже созданную задачу.
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 содержится в справке *Kaspersky Security Center*.

- В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Также вы можете изменять состав папок, запуск программ из которых будет разрешен: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
- В блоке **Параметры** укажите действия задачи во время ее выполнения и по ее завершении. Укажите критерий, на основе которого будут сформированы правила, и имя файла, в который будут экспортированы эти правила.
- В блоке **Расписание** настройте параметры запуска задачи по расписанию.
- В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
- В блоке **Исключения из области действия задачи** задайте группы компьютеров, которые требуется исключить из области действия задачи.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет создавать разрешающие правила по программам, запускаемым на исключенных компьютерах.

3. На закладке **Задачи** в панели управления настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу автоматического формирования разрешающих правил и нажмите кнопку **Запустить** для запуска задачи.

По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в указанной общей сетевой папке в файлах формата XML.

При применении политики контроля запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае если применение общей сетевой папки в работе компьютеров сети не предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

4. Добавьте сформированные списки разрешающих правил в задачу Контроль запуска программ. Для этого в свойствах настраиваемой 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 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:
 - **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.
 - d. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля запуска программ.
 - e. Нажмите на кнопку **ОК** в окне **Правила контроля запуска программ** и в окне **Параметры задачи**.
5. Если вы хотите применять созданные правила для контроля запуска программ, в свойствах политики Контроль запуска программ выберите режим выполнения задачи **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном компьютере, будут применены для всех компьютеров в сети, для которых применяется настраиваемая политика. Для этих компьютеров программа будет разрешать запуски только тех программ, для которых созданы разрешающие правила.

Импорт правил из файла отчета Kaspersky Security Center о заблокированных запусках программ

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 контроля запуска программ, вы можете отследить, запуск каких программ будет блокироваться.

При импорте из отчета данных о заблокированных программах в настройки политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

► Чтобы задать разрешающие правила запуска программ для группы компьютеров на основе отчета из Kaspersky Security Center о заблокированных программах, выполните следующие действия:

1. В свойствах политики в параметрах задачи Контроль запуска программ установите режим работы **Только статистика**.

2. В свойствах политики в разделе **Настройка событий** убедитесь, что:

- На закладке **Критические события** для события **Запуск программы** запрещен установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).
- На закладке **Предупреждение** для события *Только статистика: запуск программы запрещен* установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).

По завершении периода, указанного в графе **Время хранения**, информация о регистрируемых 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 установленное время хранения указанных событий.

3. По завершении задачи экспортируйте зафиксированные события в файл формата TXT.

- Для этого в свойствах задачи **Контроль запуска программ** разверните узел **Журналы и уведомления**.
- Во вложенном узле **События** создайте выборку событий по характеристике *Запрещен*, чтобы просмотреть, запуск каких программ будет блокироваться задачей контроля запуска программ.
- В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных устройствах в файл формата TXT.

Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых вы хотите разрешить.

4. 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:

- На закладке **Общие** нажмите на кнопку **Список правил**.
Откроется окно **Правила контроля запуска программ**.
- Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.
- Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля запуска программ:
 - **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.
- В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

е. Нажмите на кнопку **ОК** в окне Правила контроля запуска программ и в окне **Параметры задачи**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

Контроль Wi-Fi

Этот раздел содержит описание задачи "Контроль Wi-Fi" и инструкции по ее настройке.

В этом разделе

О задаче Контроль Wi-Fi	214
Настройка параметров задачи Контроль Wi-Fi	215
О списке доверенных сетей Wi-Fi	217

О задаче Контроль Wi-Fi

В ходе выполнения задачи Контроль Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 2.5 отслеживает попытки подключения защищаемого компьютера к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям Wi-Fi. Задача Контроль Wi-Fi работает на основе принципа блокировки по умолчанию (Default Deny), который означает автоматическое блокирование подключений к любым сетям Wi-Fi, если такие сети не разрешены в параметрах задачи.

Задача Контроль Wi-Fi может выполняться в одном из двух режимов:

- **Активный.** Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключения к сетям Wi-Fi в соответствии с настроенными параметрами задачи. Если в задаче применяется список доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi, кроме указанных в списке. Если в задаче не применяется список доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi.

При запуске задачи в режиме Активный Kaspersky Industrial CyberSecurity for Nodes 2.5 заблокирует все текущие подключения к сетям Wi-Fi, если используемые сети Wi-Fi не добавлены в список доверенных.

- **Только сообщать.** Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет блокировать подключения к сетям Wi-Fi. Вместо этого он только фиксирует в журнале выполнения задачи информацию о подключениях к доступным сетям Wi-Fi и возможный ответ программы на попытки подключения. Подключение ко всем сетям Wi-Fi разрешено.

Этот режим установлен по умолчанию.

Вы можете использовать этот режим для последующего формирования списка доверенных сетей Wi-Fi на основе информации, зафиксированной в журнале выполнения задачи.

Задача Контроль Wi-Fi доступна для запуска на серверах под управлением операционных систем, в которых установлен и запущен сервис wlsnsv. Задача Контроль Wi-Fi недоступна без донастройки параметров в операционных системах, не поддерживающих сервис wlsnsv в качестве предустановленного:

- Microsoft Windows Server 2003 R2 – сервис wlsnsv отсутствует и не может быть установлен.

- Microsoft Windows Server 2008 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.
- Microsoft Windows Server 2008 R2 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.
- Microsoft Windows Server 2012 R2 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.

Для установки сервиса wlansvc на компьютере под управлением Microsoft Windows Server 2012 R2 требуется перезагрузка защищаемого компьютера.

- Microsoft Windows Server 2016 – сервис wlansvc отсутствует и должен быть установлен до запуска задачи Контроль Wi-Fi.

Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически проверяет наличие сервиса wlansvc в операционной системе при установке и исключает компонент Контроль Wi-Fi из списка рекомендуемой установки, если не обнаруживает сервис wlansvc. В этом случае вы все равно можете выбрать Компонент Wi-Fi в списке выборочной установки: задача Контроль Wi-Fi будет недоступна для запуска до установки и запуска сервиса wlansvc.

Настройка параметров задачи Контроль Wi-Fi

Задача Контроль Wi-Fi имеет ряд параметров, настроенных по умолчанию, которые вы можете изменять в соответствии с требованиями безопасности (см. таблицу ниже).

Таблица 33. Параметры задачи Контроль Wi-Fi по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	Только сообщать	По умолчанию задача только уведомляет пользователя о блокировке и разрешении подключений к сетям Wi-Fi с помощью записей в журнале выполнения задачи. Фактическая блокировка подключений не выполняется. Вы можете выбрать режим Активный для защиты компьютера после того, как будет сформирован список доверенных сетей Wi-Fi.
Применение списка доверенных сетей 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.

► Чтобы настроить параметры задачи Контроль Wi-Fi, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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**.

Откроется окно **Свойства: Контроль Wi-Fi**.

3. На закладке **Общие**:

- В блоке **Режим работы** укажите режим работы задачи Контроль Wi-Fi:
 - **Активный.**

Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключения к сетям Wi-Fi в соответствии с настроенными параметрами задачи. Если в задаче применяется список исключений для доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi, кроме указанных в списке. Если в задаче не применяется список исключений, программа блокирует подключения к любым сетям Wi-Fi.

- **Только сообщать.**

Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует подключение к таким сетям Wi-Fi. Вместо этого он только фиксирует в журнале выполнения задачи информацию о подключениях к доступным сетям Wi-Fi и возможный ответ программы на попытки подключения. Подключение ко всем сетям Wi-Fi разрешено.

Этот режим установлен по умолчанию.

- Снимите или установите флажок **Разрешать подключение к указанным сетям Wi-Fi**.

Флажок включает или выключает применение списка исключений для доверенных сетей Wi-Fi.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает сети Wi-Fi, добавленные в список, в качестве исключений из блокирования. В случае, если вы задавали список исключений ранее и устанавливаете флажок повторно, программа автоматически применяет последнюю версию списка.

Если флажок снят, программа блокирует подключения к любым сетям Wi-Fi. Редактирование списка исключений недоступно. Заданный список исключений не учитывается, но сохраняется в параметрах задачи.

По умолчанию флажок установлен.

- Если требуется, отредактируйте список доверенных сетей Wi-Fi (см. раздел "О списке доверенных сетей Wi-Fi" на стр. [217](#)).

4. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.

5. Нажмите на кнопку **ОК**.

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

О списке доверенных сетей Wi-Fi

Вы можете задавать список доверенных сетей Wi-Fi, чтобы не учитывать такие сети при блокировании подключений. Для создания исключения для доверенной сети Wi-Fi вы можете:

- добавить доверенную сеть Wi-Fi вручную;
- выбрать доверенные сети Wi-Fi из списка доступных для подключения сетей Wi-Fi;
- использовать режим **Только сообщать** в задаче Контроль Wi-Fi.

Вы можете добавлять и удалять заданные исключения. Вы не можете редактировать заданные исключения.

Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает подключение к доверенным сетям Wi-Fi на основе следующих критериев:

- **Идентификатор беспроводной сети SSID** (далее "SSID"). SSID (Service Set Identifier) – это имя сети Wi-Fi, которое вы можете найти в списке операционной системы, содержащем данные о доступных для подключения сетях Wi-Fi. Значение SSID не является уникальным признаком сети Wi-Fi.
- **Наличие шифрования сети Wi-Fi**. Вы можете узнать, защищено ли подключение к сети Wi-Fi паролем, в списке операционной системы, содержащем данные о доступных для подключения сетях Wi-Fi.

Значения этих критериев отображаются в соответствующих графах списка доверенных сетей Wi-Fi в параметрах задачи Контроль Wi-Fi.

В ходе выполнения задачи Контроль Wi-Fi программа также блокирует подключение к сетям Wi-Fi со скрытым SSID, если сети Wi-Fi с таким SSID не добавлены в список доверенных. Вы можете добавить исключение для доверенной сети Wi-Fi со скрытым SSID только вручную.

Добавление доверенной сети Wi-Fi вручную

При добавлении доверенной сети Wi-Fi вручную вам нужно самостоятельно задать критерии, на основе которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к доверенной сети Wi-Fi.

► Чтобы добавить сети Wi-Fi в список доверенных вручную, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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**.

Откроется окно **Свойства: Контроль Wi-Fi** на закладке **Общие**.

3. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.

Флажок включает или выключает применение списка исключений для доверенных сетей Wi-Fi.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает сети Wi-Fi, добавленные в список, в качестве исключений из блокирования. 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.

4. Нажмите на кнопку **Добавить доверенную сеть Wi-Fi**.
5. В контекстном меню кнопки выберите вариант **Добавить вручную**.
Откроется окно **Добавление доверенной сети Wi-Fi**.
6. Укажите параметры сети Wi-Fi, на основе которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к доверенной сети Wi-Fi:
 - В поле **Идентификатор сети Wi-Fi (SSID)** укажите имя сети Wi-Fi.
Вы не можете задать пустое значение SSID.
 - Снимите или установите флажок **Разрешать только безопасные сети Wi-Fi**.

Флажок включает или выключает учет наличия шифрования при исключении сети Wi-Fi с заданным SSID.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает подключение к сетям Wi-Fi с заданным SSID, только если такое подключение

зашифровано и защищено паролем.

Если флажок снят, программа разрешает подключение к любым сетям Wi-Fi с заданным SSID.

По умолчанию флажок установлен.

7. В окне **Добавление доверенной сети Wi-Fi** нажмите кнопку **ОК**.

Указанная сеть Wi-Fi будет добавлена в список доверенных сетей Wi-Fi в параметрах задачи Контроль Wi-Fi. При выполнении задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к сетям Wi-Fi, которые подпадают под действие заданного исключения.

Добавление доверенной сети Wi-Fi с помощью списка доступных сетей Wi-Fi

При добавлении исключения для доверенной сети Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 2.5 получает данные обо всех доступных сетях Wi-Fi от операционной системы.

Вы не можете добавить сеть Wi-Fi в список доверенных с помощью списка доступных сетей Wi-Fi: если SSID сети Wi-Fi скрыт, она не будет отображаться в списке доступных сетей Wi-Fi.

► Если вы хотите настроить параметры задачи Контроль Wi-Fi на группе серверов с помощью политики Kaspersky Security Center, убедитесь, что в политике Kaspersky Industrial CyberSecurity for Nodes 2.5 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 открывшемся окне **Информировать Сервер администрирования** установите флажок **Данные о доступных сетях Wi-Fi**.

Kaspersky Industrial CyberSecurity for Nodes 2.5, 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. 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>** (см. раздел "Настройка политики" на стр. [90](#)).
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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**.

Откроется окно **Свойства: Контроль Wi-Fi** на закладке **Общие**.

3. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.
4. Нажмите кнопку **Добавить сеть Wi-Fi**.
5. В контекстном меню кнопки выберите пункт **Импортировать из списка Сервера администрирования**.

Откроется окно **Доступные сети Wi-Fi**.

6. Если требуется, нажмите кнопку **Обновить список**, чтобы получить актуальный список доступных сетей Wi-Fi.
7. В списке доступных сетей Wi-Fi выберите одну или несколько сетей Wi-Fi для добавления в список доверенных.
8. Нажмите на кнопку **ОК**.

Указанные сети Wi-Fi будут добавлены в список доверенных сетей Wi-Fi в параметрах задачи **Контроль Wi-Fi**. При выполнении задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к указанным сетям Wi-Fi.

Удаление исключения для сети Wi-Fi

► Чтобы удалить сеть Wi-Fi из списка доверенных, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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**.

Откроется окно **Свойства: Контроль Wi-Fi** на закладке **Общие**.

3. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.
4. В списке доверенных сетей Wi-Fi выделите сети Wi-Fi, которые вы хотите удалить.
5. Нажмите кнопку **Удалить из списка сетей Wi-Fi**.
6. Нажмите кнопку **ОК**.

Выбранные сети Wi-Fi будут удалены из списка доверенных сетей Wi-Fi. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет блокировать подключение к таким сетям Wi-Fi.

Контроль активности в сети

Этот раздел содержит информацию о задаче Защита от шифрования.

Защита от шифрования

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

В этом разделе

О задаче Защита от шифрования	222
Настройка параметров задачи Защита от шифрования	223

О задаче Защита от шифрования

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

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

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

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

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

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

Настройка параметров задачи Защита от шифрования

Задача Защита от шифрования имеет следующие параметры по умолчанию:

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

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

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.
Откроется окно **Защита от шифрования**.
4. В открывшемся окне настройте следующие параметры:
 - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. [224](#)) на закладке **Общие**.
 - Область защиты (см. раздел "Формирование области защиты" на стр. [225](#)) на закладке **Область защиты**.

- Исключения (см. раздел "Добавление исключений" на стр. [227](#)) на закладке **Исключения**.
- Запуск задачи по расписанию (см. раздел "Настройка запуска задачи по расписанию" на стр. [132](#)) на закладке **Управление задачами**.

5. Нажмите на кнопку **ОК**.

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

Общие параметры задачи

► Чтобы настроить общие параметры задачи, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

4. В блоке **Режим работы** укажите режим работы задачи:

- **Только статистика.**

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

- **Активный.**

Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует доступ к папкам общего доступа для скомпрометированных компьютеров при обнаружении попытки вредоносного шифрования.

5. Снимите или установите флажок **Использовать эвристический анализатор**.

Флажок включает или выключает использование эвристического анализатора

при проверке объектов.

Если флажок установлен, эвристический анализатор включен.

Если флажок снят, эвристический анализатор выключен.

По умолчанию флажок установлен.

6. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

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

Существуют следующие уровни детализации проверки:

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

Этот уровень выбран по умолчанию.

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

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

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

Формирование области защиты

В задаче Защита от шифрования применяются следующие типы области защиты:

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

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

► Чтобы настроить область защиты для задачи **Защита от шифрования**, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.
Откроется окно **Защита от шифрования**.
4. В блоке **Область защиты** выберите папки, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет проверять в ходе выполнения задачи **Защита от шифрования**:

- **Проверять папки общего доступа на компьютере.**

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

Этот вариант выбран по умолчанию.

- **Только указанные папки общего доступа.**

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

5. Чтобы указать общую папку компьютера, которую вы хотите включить в область защиты, используйте один из следующих способов:
 - a. Нажмите кнопку **Добавить**.
Откроется окно **Выберите папку для добавления**.
 - b. Нажмите на кнопку **Обзор**, чтобы выбрать папку, или введите путь вручную.
 - c. Нажмите на кнопку **ОК**.
6. 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. 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>** (см. раздел "Настройка политики" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [103](#)).

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 **Контроль активности в сети**, нажмите кнопку **Настройка** в блоке **Защита от шифрования**.

Откроется окно **Защита от шифрования**.

4. На закладке **Исключения**, установите флажок **Учитывать исключенные области защиты**.

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

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

По умолчанию флажок снят, список исключений пуст.

5. Нажмите кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.

6. Введите имя папки или нажмите кнопку **Обзор**, чтобы выбрать необходимую папку.

7. Нажмите на кнопку **ОК**.

Исключенные области добавлены в список.

Диагностика системы

Этот раздел содержит информацию о задаче контроля файловых операций и возможностях анализа системного журнала операционной системы.

В этом разделе

Мониторинг файловых операций	228
Анализ журналов	236

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Монитор целостности файлов.

В этом разделе

О задаче Мониторинг файловых операций.....	228
О правилах мониторинга файловых операций	229
Настройка параметров задачи Мониторинг файловых операций.....	231
Настройка правил мониторинга.....	233

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

Обрыв мониторинга — это период, когда область мониторинга временно выпадает из поля действия задачи, например, из-за приостановки выполнения задачи или физического отсутствия запоминающего устройства на защищаемом компьютере. Kaspersky Industrial CyberSecurity for Nodes 2.5 сообщит об обнаружении файловых операций в области мониторинга, как только запоминающее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

Требования к среде

Для запуска задачи Мониторинг файловых операций должны быть соблюдены следующие условия:

- На защищаемом компьютере установлено запоминающее устройство, поддерживающее файловые системы ReFS и NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN журнала компонент получает данные о файловых операциях.

Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинга файловых операций, требуется перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга (см. раздел "Настройка правил мониторинга" на стр. [233](#)). 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 нижеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания задачи и регулировать уровень важности событий для обнаруженных файловых операций, фиксируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- Доверенные пользователи
- Маркеры файловых операций

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Информационное событие в журнале выполнения задачи.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Неизвестный пользователь – данный статус присваивается пользователю в случае, когда Kaspersky Industrial CyberSecurity for Nodes 2.5 не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную неизвестным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Предупреждение в журнале выполнения задачи.

Маркеры файловых операций

В ходе выполнения задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа зафиксирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 34. 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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS
INTEGRITY_CHANGE	изменен атрибут целостности для именованного файлового потока	только ReFS
NAMED_DATA_EXTEND	размер именованного файлового потока увеличен	NTFS, ReFS
NAMED_DATA_OVERWRITE	именованный файловый поток перезаписан	NTFS, ReFS
NAMED_DATA_TRUNCATION	именованный файловый поток усечен	NTFS, ReFS
OBJECT_ID_CHANGE	изменен идентификатор файла или папки	NTFS, ReFS
RENAME_NEW_NAME	присвоено новое имя для файла или папки	NTFS, ReFS
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTIONED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

Таблица 35. Параметры задачи Мониторинга файловых операций по умолчанию

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.

Параметр	Значение по умолчанию	Описание
Список доверенных пользователей	Не задано	Вы можете задать пользователей и/или группы пользователей, действия которых в указанных каталогах будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 будет пропускать области мониторинга, заданные в качестве исключений.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров для характеристики файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Industrial CyberSecurity for Nodes 2.5 формирует событие аудита.
Расписание запуска задачи	Первый запуск не определен	Вы можете настроить параметры запуска задачи по расписанию.

Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

Откроется окно **Мониторинг файловых операций**.

4. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте параметры области мониторинга:

- 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 2.5 будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

По умолчанию флажок установлен.

- b. Добавьте области мониторинга (см. раздел "Настройка правил мониторинга" на стр. [233](#)), которые будет контролировать задача.

5. На закладке **Управление задачами** запустите задачу на базе расписания (см. раздел "Работа с расписанием задач" на стр. [132](#)).

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

По умолчанию область мониторинга не задана; задача не контролирует выполнение файловых операций ни в одной директории.

► Чтобы добавить область мониторинга, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. 90).
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 103).

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 **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

Откроется окно **Свойства**: Откроется окно **Мониторинг файловых операций**.

4. В блоке **Область мониторинга** нажмите на кнопку **Добавить**.

Откроется окно **Область мониторинга**.

5. Добавьте область мониторинга одним из следующих способов:

- Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
 - a. Нажмите на кнопку **Выбрать**.
Откроется стандартное окно Microsoft Windows Обзор папок.
 - b. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите кнопку **ОК**.
- Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
 - `<*.ext>` - все файлы с расширением `<ext>` вне зависимости от их расположения;
 - `<*\name.ext>` - все файлы с именем `name` и расширением `<ext>` вне зависимости от их расположения;
 - `<\dir*>` - все файлы в директории `<\dir>`;
 - `<\dir*\name.ext>` - все файлы с именем `name` и расширением `<ext>` в директории `<\dir>` и всех ее поддиректориях.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: `<буква тома>:\<маска>`. Если том не указан, Kaspersky Industrial CyberSecurity for Nodes 2.5 не добавит указанную область мониторинга.

6. На закладке **Доверенные пользователи**, нажмите на кнопку **Добавить**.

Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.

7. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга, и нажмите кнопку **ОК**.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 229), и формирует для них события с уровнем важности Критическое событие.

8. Выберите закладку **Маркеры файловых операций**.
9. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
 - a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
 - b. В открывшемся списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 229) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывала контрольную сумму файлов после изменений, выполните следующие действия:
 - a. В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаруживается сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех последовательных изменений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не рассчитывает контрольную сумму измененных файлов.

Программа не выполняет расчет контрольной суммы в следующих случаях:

- если в результате файловой операции файл стал недоступен (например, изменены права доступа к файлу);
- если файловая операция фиксируется для файла, который впоследствии был удален.

По умолчанию флажок снят.

- b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из вариантов:
 - **Хеш MD5**
 - **Хеш SHA256**
11. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 229) установите флажки напротив тех операций, которые вы хотите контролировать.
12. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

a. Выберите закладку **Исключения**.

b. Установите флажок **Учитывать исключенные области мониторинга**.

Флажок включает или выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 будет пропускать области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет фиксировать события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

c. Нажмите на кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите на кнопку **ОК**.

Указанная папка добавится в список исключенных областей.

13. В окне **Область мониторинга** нажмите на кнопку **ОК**.

Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

В этом разделе

О задаче Анализ журналов	236
Настройка параметров предзаданных правил задачи	238
Настройка правил анализа журналов	240

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Industrial CyberSecurity for Nodes 2.5 считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами, заданными пользователем или параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Предзаданные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью предзаданных правил, осуществляющими анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом компьютере, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь предзаданных правил. Вы можете включать и выключать применение любого правила. Вы не можете удалять существующие или создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для данных операций:

- Обработка подбора пароля
- Обработка сетевого входа

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил задачи вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил задачи Анализ журналов содержит четыре правила. Вы можете включать и выключать применение данных правил, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

Правило срабатывает при появлении новой записи в журнале событий Windows, если в параметрах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

Для каждого правила вы можете задать поджурнал журнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал, указав его имя в поле выбора источника.

Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие с уровнем важности *Критическое* событие в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает пользовательские правила.

Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробную информацию о настройке вы можете найти в [данной статье](#).

Настройка параметров предзаданных правил задачи

► Чтобы настроить параметры предзаданных правил для задачи Анализ журналов, 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>** (см. раздел "**Настройка политики**" на стр. [90](#)).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [103](#)).

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 **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

Откроется окно **Параметры анализа журналов**.

4. Перейдите на закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

Если этот флажок не установлен, то эвристический анализатор выключен, Kaspersky Industrial CyberSecurity for Nodes 2.5 использует предустановленные или пользовательские правила для обнаружения аномальной активности.

По умолчанию флажок установлен.

Для работы задачи должно быть выбрано хотя бы одно правило анализа журналов.

6. Из списка предзаданных правил, выберите правила, которые вы хотите применять для анализа журналов:

- Обнаружена возможная попытка взлома пароля с помощью подбора.
 - Обнаружены признаки компрометации журналов Windows.
 - Обнаружена подозрительная активность со стороны новой установленной службы.
 - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
 - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
 - Обнаружены подозрительные изменения привилегированной группы Администраторы.
 - Обнаружена подозрительная активность во время сетевого сеанса входа.
7. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.
Откроется окно **Анализ журналов**.
8. В блоке **Обработка перебора пароля** укажите количество попыток и промежутков времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Industrial CyberSecurity for Nodes 2.5 расценивает данное действие как аномальную активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
- a. Нажмите на кнопку **Выбрать**.
 - b. Выберите пользователя.
 - c. Нажмите на кнопку **ОК**.
- Указанный пользователь добавится в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
- a. Введите IP-адрес.
 - b. Нажмите на кнопку **Добавить**.
13. Указанный IP-адрес добавится в список доверенных.
14. На закладке **Управление задачами** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. [133](#)).
15. Нажмите на кнопку **ОК**.
- Параметры задачи Анализ журналов будут сохранены.

Настройка правил анализа журналов

► Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли 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>** (см. раздел "Настройка политики" на стр. 90).
 - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 103).

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 **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

Откроется окно **Анализ журналов**.

4. На закладке **Правила анализа журналов** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять, удалять или изменять правила анализа журналов.

Если флажок снят, вы не можете добавлять или изменять пользовательские правила. Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет параметры правил по умолчанию.

По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

Вы можете контролировать применение предустановленных правил в списке правил. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

Откроется окно **Правило анализатора журналов**.

6. В блоке **Общие** введите следующие данные нового правила:

- **Название**
- **Источник**

Выберите журнал, события которого будут использоваться для анализа. Для выбора доступны следующие виды журналов событий Windows:

- Программа
- Безопасность
- Система

Вы можете добавить новый пользовательский журнал, указав имя журнала в поле **Источник**.

7. В блоке **Параметры срабатывания** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

- Введите числовое значение идентификатора.
- Нажмите на кнопку **Добавить**.

Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

- Нажмите на кнопку **ОК**.

Правило анализа журналов добавится в общий список правил.

Контроль производительности. Счетчики Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о счетчиках ловушках SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5: счетчиках производительности системного монитора, счетчиках и ловушках SNMP.

В этом разделе

Счетчики производительности для программы Системный монитор.....	242
Счетчики и ловушки SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5	249

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 2.5 во время установки.

В этом разделе

О счетчиках производительности Kaspersky Industrial CyberSecurity for Nodes 2.5	242
Общее количество отвергнутых запросов	243
Общее количество пропущенных запросов	244
Количество запросов, не обработанных из-за нехватки системных ресурсов	245
Количество запросов, отданных на обработку	245
Среднее количество потоков диспетчера файловых перехватов.....	246
Максимальное количество потоков диспетчера файловых перехватов	246
Количество элементов в очереди зараженных объектов	247
Количество объектов, обрабатываемых за секунду.....	248

О счетчиках производительности Kaspersky Industrial CyberSecurity for Nodes 2.5

В состав устанавливаемых компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 по умолчанию включен компонент **Счетчики производительности**. Во время установки Kaspersky Industrial CyberSecurity for Nodes 2.5 регистрирует свои счетчики производительности для программы "Системный монитор" Microsoft Windows.

С помощью счетчиков Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете контролировать производительность программы во время выполнения задач постоянной защиты. Вы можете обнаруживать узкие места при его совместной работе с другими программами и недостаточность ресурсов. Вы можете диагностировать неоптимальную настройку Kaspersky Industrial CyberSecurity for Nodes 2.5 и сбой в его работе.

Вы можете просматривать счетчики производительности Kaspersky Industrial CyberSecurity for Nodes 2.5, открыв консоль **Производительность** в элементе **Администрирование** Панели управления Windows.

В следующих разделах приводятся определения счетчиков, рекомендуемые интервалы считывания показаний, пороговые значения и рекомендации по настройке Kaspersky Industrial CyberSecurity for Nodes 2.5 в случае, если значения счетчиков их превышают.

Общее количество отвергнутых запросов

Таблица 36. Общее количество отвергнутых запросов

Название	Общее количество отвергнутых запросов (Total number of requests denied)
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5; рассчитывается с момента последнего запуска Kaspersky Industrial CyberSecurity for Nodes 2.5. Программа пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: <ul style="list-style-type: none"> снижение качества постоянной защиты из-за полной загрузки рабочих процессов Kaspersky Industrial CyberSecurity for Nodes 2.5; прерывание постоянной защиты из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: <ul style="list-style-type: none"> счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Kaspersky Industrial CyberSecurity for Nodes 2.5 были полностью загружены, поэтому Kaspersky Industrial CyberSecurity for Nodes 2.5 не удалось проверить объекты. <p>Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты. Вы можете использовать параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 Максимальное количество активных процессов и Число процессов для постоянной защиты.</p>

	<ul style="list-style-type: none"> количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Industrial CyberSecurity for Nodes 2.5 не проверяет объекты при доступе. Перезапустите Kaspersky Industrial CyberSecurity for Nodes 2.5.
--	--

Общее количество пропущенных запросов

Таблица 37. Общее количество пропущенных запросов

Название	Общее количество пропущенных запросов (Total number of requests skipped).
Определение	<p>Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Industrial CyberSecurity for Nodes 2.5, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы.</p> <p>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 2.5 пропускает такой объект и на 1 увеличивается значение счетчика Общее количество отвергнутых запросов.</p>
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за простоя потоков диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1.
Рекомендуемый интервал считывания показаний	1 ч.
Рекомендации по настройке, если значение превышает пороговое	<p>Если значение счетчика отличается от нулевого, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент.</p> <p>Если скорость проверки не удовлетворительна, перезапустите Kaspersky Industrial CyberSecurity for Nodes 2.5, чтобы восстановить простаивающие потоки.</p>

Количество запросов, не обработанных из-за нехватки системных ресурсов

Таблица 38. 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 2.5. Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает объекты, запросы на проверку которых не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, рабочие процессы Kaspersky Industrial CyberSecurity for Nodes 2.5 нуждаются в увеличении объема оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

Количество запросов, отданных на обработку

Таблица 39. Количество запросов, отданных на обработку

Название	Количество запросов, отданных на обработку (Number of requests sent to be processed).
Определение	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 и общий уровень файловой активности на компьютере.
Нормальное / пороговое значение	Значение счетчика может колебаться в зависимости от уровня файловой активности на компьютере.
Рекомендуемый интервал считывания показаний	1 мин.

Рекомендации по настройке, если значение превышает пороговое	Нет
--	-----

Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).

Таблица 40. Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).

Название	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, среднее по всем процессам, занятым в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты из-за полной загрузки процессов Kaspersky Industrial CyberSecurity for Nodes 2.5.
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 2.5 пропустит объект. Увеличьте количество процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 для задач постоянной защиты. Вы можете использовать параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 Максимальное количество активных процессов Количество процессов для постоянной защиты .

Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).

Таблица 41. Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, наибольшее из всех процессов, занятых в задачах постоянной защиты в текущий момент.

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 2.5 неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Kaspersky Industrial CyberSecurity for Nodes 2.5.

Количество элементов в очереди зараженных объектов

Таблица 42. Количество элементов в очереди зараженных объектов

Название	Количество элементов в очереди зараженных объектов (Number of items in the infected object queue).
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: <ul style="list-style-type: none"> • прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими программами и Kaspersky Industrial CyberSecurity for Nodes 2.5; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Industrial CyberSecurity for Nodes 2.5 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	<p>Если значение счетчика остается ненулевым длительное время:</p> <ul style="list-style-type: none"> • Kaspersky Industrial CyberSecurity for Nodes 2.5 не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов); Перезапустите Kaspersky Industrial CyberSecurity for Nodes 2.5. • Недостаточно процессорного времени для обработки объектов; Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes 2.5 дополнительного процессорного времени, например, снизив нагрузку на компьютер другими программами. • Возникла вирусная эпидемия. <p>О возникновении вирусной эпидемии говорит 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.</p>
---	---

Количество объектов, обрабатываемых за секунду

Таблица 43. 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 компьютера, возникшее из-за недостаточности выделяемого рабочим процессам Kaspersky Industrial CyberSecurity for Nodes 2.5 процессорного времени или сбоя в работе Kaspersky Industrial CyberSecurity for Nodes 2.5.
Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	<p>Значения счетчика зависят от установленных значений параметров Kaspersky Industrial CyberSecurity for Nodes 2.5 и загрузки компьютера процессами других программ.</p> <p>Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился, то могла произойти одна из следующих ситуаций:</p> <ul style="list-style-type: none"> • Рабочим процессам Kaspersky Industrial CyberSecurity for Nodes 2.5 не хватает процессорного времени для обработки объектов.

	<p>Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes 2.5 дополнительного процессорного времени, например, снизив нагрузку на компьютер другими программами.</p> <ul style="list-style-type: none"> • Возник сбой в работе Kaspersky Industrial CyberSecurity for Nodes 2.5 (простаивает несколько потоков). <p>Перезапустите Kaspersky Industrial CyberSecurity for Nodes 2.5.</p>
--	---

Счетчики и ловушки SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о счетчиках и ловушках SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

О счетчиках и ловушках SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.....	249
Счетчики SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.....	249
Ловушки SNMP	252

О счетчиках и ловушках SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5

Если вы включили в состав устанавливаемых компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 компонент **Счетчики и ловушки SNMP**, вы можете просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes 2.5 по протоколам Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes 2.5 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).

Счетчики SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит таблицы с описанием параметров счетчиков SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Счетчики производительности	250
Счетчики карантина	250

Счетчики резервного хранилища	250
Общие счетчики	251
Счетчик обновления	251
Счетчики постоянной защиты	251

Счетчики производительности

Таблица 44. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отданных на обработку (см. стр. 245).
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов (см. раздел "Количество элементов в очереди зараженных объектов" на стр. 247).
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (см. стр. 248).
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 в текущий момент

Счетчики карантина

Таблица 45. 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	Объем данных в папке карантина (МБ)

Счетчики резервного хранилища

Таблица 46. Счетчики резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Объем данных в папке резервного хранилища (МБ)

Общие счетчики

Таблица 47. Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней проверки важных областей компьютера (промежуток времени в секундах между датой завершения задачи, имеющей статус <i>Задача проверки важных областей</i> , и текущим моментом).
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлены активный и дополнительный ключи или коды активации, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом или кодом активации.
currentApplicationUptime	Время работы Kaspersky Industrial CyberSecurity for Nodes 2.5 с момента его последнего запуска, в сотых долях секунды
currentFileMonitorTaskStatus	Статус задачи Постоянная защита файлов: On – работает; Off – остановлена или приостановлена.

Счетчик обновления

Таблица 48. Счетчик обновлений

Счетчик	Определение
avBasesAge	"Возраст" баз (промежуток времени в сотых долях секунды между датой создания последних установленных обновлений баз и текущим моментом).

Счетчики постоянной защиты

Таблица 49. Счетчики постоянной защиты

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 других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 поместил на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

Счетчик	Определение
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 пытался поместить на карантин, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDisinfected	Общее количество зараженных объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 вылечил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 пытался вылечить, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 удалил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 должен был удалить, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsBackedUp	Общее количество зараженных и других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 поместил в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotBackedUp	Общее количество зараженных и других объектов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

Ловушки SNMP

Параметры ловушек SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5 описаны в таблице ниже.

Таблица 50. Ловушки SNMP Kaspersky Industrial CyberSecurity for Nodes 2.5

Ловушка	Описание	Параметры
eventThreatDetected	Обнаружен объект.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType

Ловушка	Описание	Параметры
		detectCertainty
eventBackupStorageSizeExceeds	Превышен максимальный размер резервного хранилища. Общий объем данных в папке резервного хранилища превысил значение, указанное параметром Максимальный размер резервного хранилища (МБ) . Kaspersky Industrial CyberSecurity for Nodes 2.5 продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Достигнут порог свободного места в резервном хранилище. Размер свободного пространства в папке резервного хранилища, заданный параметром Порог доступного пространства (МБ) , уменьшился до указанного значения. Kaspersky Industrial CyberSecurity for Nodes 2.5 продолжает резервировать зараженные объекты.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром Максимальный размер карантина (МБ) . Kaspersky Industrial CyberSecurity for Nodes 2.5 продолжает помещать возможно зараженные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Достигнут порог свободного места в карантине. Размер свободного пространства в папке карантина, заданный параметром Порог доступного пространства в карантине (МБ) , уменьшился до указанного значения. Kaspersky Industrial CyberSecurity for Nodes 2.5 продолжает помещать возможно зараженные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Ошибка карантина.	eventSeverity eventDateAndTime eventSource userName computerName objectName

Ловушка	Описание	Параметры
		storageObjectNotAddedEvent Reason
eventObjectNotBackuped	Ошибка сохранения копии объекта в резервном хранилище.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEvent Reason
eventQuarantineInternalError	Ошибка карантина.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Ошибка резервного хранилища.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Базы программы устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Базы программы сильно устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Industrial CyberSecurity for Nodes 2.5 запущен.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Industrial CyberSecurity for Nodes 2.5 остановлен.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Проверка важных областей не проводилась давно. Рассчитывается количество дней с момента последнего завершения задачи, имеющей статус <i>Задача проверки важных областей</i> .	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Срок действия лицензии истек.	eventSeverity

Ловушка	Описание	Параметры
		eventDateAndTime eventSource
eventLicenseExpiresSoon	Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Ошибка выполнения задачи.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Ошибка выполнения задачи обновления.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

В таблице ниже описаны параметры ловушек и возможные значения параметров.

Таблица 51. Значения параметров ловушек SNMP

Параметр	Описание и возможные значения
eventDateAndTime	Время возникновения события.
eventSeverity	Уровень важности события. Параметр принимает следующие значения: <ul style="list-style-type: none"> critical (1) – критический, warning (2) – предупреждение, info (3) – информационный.
username	Имя пользователя (например, пользователя, который пытался получить доступ к зараженному файлу).
computerName	Имя компьютера (например, компьютера, с которого пользователь пытался получить доступ к зараженному файлу).
eventSource	Источник события: функциональный компонент, в работе которого возникло событие. Параметр принимает следующие значения: <ul style="list-style-type: none"> 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;

Параметр	Описание и возможные значения
	<ul style="list-style-type: none"> onDemandScanning (6) – Проверка по требованию; product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Industrial CyberSecurity for Nodes 2.5 в целом; systemAudit (8) – Журнал системного аудита.
eventReason	<p>Причина возникновения события. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> 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 для доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
objectName	Имя объекта (например, имя файла, в котором обнаружена угроза).
threatName	Имя обнаруженного объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes 2.5 возвращает при обнаружении объекта. Полное имя обнаруженного объекта можно просмотреть в журнале выполнения задач (см. раздел "Настройка параметров журналов" на стр. 156).
detectType	<p>Тип обнаруженного объекта.</p> <p>Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> 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 компьютеру или данным.
detectCertainty	<p>Степень уверенности обнаружения угрозы. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> Suspicion (возможно зараженный) – Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаружил частичное совпадение участка кода объекта с известным вредоносным кодом;

Параметр	Описание и возможные значения
	<ul style="list-style-type: none"> • Sure (зараженный) – Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаружил полное совпадение участка кода объекта с известным вредоносным кодом.
Days	Количество дней (например, количество дней до окончания срока действия лицензии).
errorCode	Код ошибки.
knowledgeBaseld	Адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
taskName	Имя задачи.
updaterErrorEventReason	<p>Причина, по которой обновление не было применено. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> • 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 – компьютер не найден; • reasonServerBusy – сервер недоступен; • reasonConnectionError – ошибка соединения; • reasonModuleNotFound – объект не найден; • reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.
storageObjectNotAddedEventReason	<p>Причина непомещения объекта в резервное хранилище или на карантин. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> • reasonUnknown (0) – причина не определена; • reasonStorageInternalError – ошибка базы данных; восстановите Kaspersky Industrial CyberSecurity for Nodes 2.5. • reasonStorageReadOnly – база данных доступна только для чтения; восстановите Kaspersky Industrial CyberSecurity for Nodes 2.5.

Параметр	Описание и возможные значения
	<ul style="list-style-type: none"> • reasonStorageIOError – ошибка ввода-вывода: а) Kaspersky Industrial CyberSecurity for Nodes 2.5 поврежден, восстановите Kaspersky Industrial CyberSecurity for Nodes 2.5; б) диск, на котором хранятся файлы Kaspersky Industrial CyberSecurity for Nodes 2.5, поврежден. • reasonStorageCorrupted – хранилище повреждено; восстановите Kaspersky Industrial CyberSecurity for Nodes 2.5. • reasonStorageFull – база данных полна; освободите место на диске. • reasonStorageOpenError – не удалось открыть файл базы данных; восстановите Kaspersky Industrial CyberSecurity for Nodes 2.5. • reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Industrial CyberSecurity for Nodes 2.5. • reasonObjectNotFound – помещаемый в хранилище 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.

Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки

Этот раздел содержит описание работы с Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки.

В этом разделе

Команды командной строки	260
Коды возврата командной строки.....	286

Команды командной строки

Вы можете выполнять основные команды управления Kaspersky Industrial CyberSecurity for Nodes 2.5 из командной строки защищаемого компьютера, если при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 вы включили компонент Утилита командной строки в список устанавливаемых.

С помощью команд командной строки вы можете управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Industrial CyberSecurity for Nodes 2.5.

Некоторые из команд Kaspersky Industrial CyberSecurity for Nodes 2.5 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 на комбинацию клавиш **CTRL+C**.

При вводе команд Kaspersky Industrial CyberSecurity for Nodes 2.5 применяйте следующие правила:

- вводите ключи и команды символами верхнего или нижнего регистра;
- разделяйте ключи символом пробела;
- если имя файла, которое вы указываете в качестве значения ключа, содержит символ пробела, заключите это имя файла (и путь к нему) в кавычки, например: "C:\TEST\test cpp.exe"
- если требуется, в масках имен файлов или путей используйте заместительные символы, например: "C:\Temp\Temp*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc"

При помощи командной строки вы можете выполнить полный спектр операций по управлению и администрированию Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. таблицу ниже).

Таблица 52. Документация Kaspersky Industrial CyberSecurity for Nodes 2.5

Команда	Описание
KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ из файла KAVSHELL APPCONTROL" на стр. 273).	Дополняет список сформированных правил контроля запуска программ в соответствии с выбранным принципом добавления.
KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачами Контроль запуска программ KAVSHELL APPCONTROL /CONFIG" на стр. 270).	Управляет режимами работы задачи Контроль запуска программ.
KAVSHELL APPCONTROL /GENERATE (см. раздел "Автоматическое формирование разрешающих правил KAVSHELL APPCONTROL /GENERATE" на стр. 271).	Запускает задачу автоматического формирования разрешающих правил контроля запуска программ.
KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала Kaspersky Industrial CyberSecurity for Nodes 2.5.KAVSHELL VACUUM" на стр. 281).	Дефрагментирует файлы журнала выполнения Kaspersky Industrial CyberSecurity for Nodes 2.5.
KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Industrial CyberSecurity for Nodes 2.5.KAVSHELL HELP" на стр. 262).	Вызывает справку о командах Kaspersky Industrial CyberSecurity for Nodes 2.5.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" на стр. 263).	Запускает службу Kaspersky Industrial CyberSecurity for Nodes 2.5.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" на стр. 263).	Останавливает службу Kaspersky Industrial CyberSecurity for Nodes 2.5.
KAVSHELL SCAN (см. раздел "Проверка выбранной области.KAVSHELL SCAN" на стр. 263).	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды.
KAVSHELL SCANCritical (см. раздел "Запуск задачи Проверка важных областей.KAVSHELL SCANCritical" на стр. 267).	Запускает системную задачу Проверка важных областей.
KAVSHELL TASK (см. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK" на стр. 268).	Запускает / приостанавливает / возобновляет / останавливает указанную задачу в асинхронном режиме / возвращает текущее состояние задачи / статистику задачи.

Команда	Описание
KAVSHELL RTP (см. раздел "Запуск и остановка задачи Постоянная защита.KAVSHELL RTP" на стр. 269).	Запускает или останавливает все задачи постоянной защиты.
KAVSHELL VACUUM (см. раздел "Запуск задачи Обновление баз Kaspersky Industrial CyberSecurity for Nodes 2.5.KAVSHELL UPDATE" на стр. 274).	Запускает задачу обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 с параметрами, указанными с помощью ключей команды.
KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5.KAVSHELL ROLLBACK" на стр. 277).	Откатывает базы до предыдущей версии.
KAVSHELL LICENSE (см. раздел "Активация программы KAVSHELL LICENSE" на стр. 278).	Управляет ключами.
KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журнала трассировки.KAVSHELL TRACE" на стр. 280).	Включает или выключает запись журнала трассировки, управляет параметрами журнала трассировки.
KAVSHELL DUMP (см. раздел "Включение и выключение файла дампа.KAVSHELL DUMP" на стр. 283).	Включает или выключает создание файлов дампов памяти процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 при аварийном завершении процессов.
KAVSHELL IMPORT (см. раздел "Импорт параметров.KAVSHELL IMPORT" на стр. 284).	Импортирует общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры его функций и задач из предварительно созданного конфигурационного файла.
KAVSHELL EXPORT (см. раздел "Экспорт параметров.KAVSHELL EXPORT" на стр. 285).	Экспортирует все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 и существующих задач в конфигурационный файл.
KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств.KAVSHELL DEVCONTROL" на стр. 274).	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

Отображение справки о командах Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните одну из следующих команд:

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

Чтобы получить описание и синтаксис команды, 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 команду

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускаются задачи Постоянная защита файлов и Проверка при старте системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните команду

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

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 Запустить помощью команды KAVSHELL SCAN, является временной. Она отображается в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 только во время ее выполнения (в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы не можете просматривать параметры задачи). В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

Указывая пути в задаче проверки отдельных областей, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте 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 указанной задачей в асинхронном режиме.KAVSHELL TASK на стр. [268](#)).

Синтаксис команды KAVSHELL SCAN

```
KAVSHELL          SCAN          <области          проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]  [/L:<имя файла
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] [/W:<имя файла журнала выполнения
задачи>] [/ANSI] [/ALIAS:<альтернативное имя задачи>]
```

В состав команды KAVSHELL SCAN входят как обязательные, так и дополнительные ключи, использование которых не является обязательным (см. таблицу ниже).

Примеры 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 53. Ключи команды KAVSHELL SCAN

Ключ	Описание
Область проверки. Обязательный ключ.	
<файлы>	Область проверки – список файлов, папок, сетевых путей и предопределенных областей. Указывайте сетевые пути в формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL: KAVSHELL SCAN Folder4 Если имя объекта, который вы хотите проверить, содержит пробелы, требуется заключить его в кавычки. Если вы выбрали папку, то Kaspersky Industrial CyberSecurity for Nodes 2.5 проверит также все вложенные подпапки для данной папки. Для проверки группы файлов вы можете использовать символы * или ?.
<папки>	
<сетевой путь>	
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на компьютере.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.
/MYCOMP	Проверять все области защищаемого компьютера.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Ключ	Описание
/L: <имя файла со списком областей проверки>	Имя файла со списком областей проверки, включая полный путь к файлу. Разделяйте области проверки в файле символом перевода строки. Вы можете указывать predetermined области проверки, как показано в следующем в примере файла со списком областей проверки: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Проверяемые объекты (File types). Если вы не укажете никаких значений этого ключа, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 будет проверять все объекты.
/AI: Действия над зараженными и другими обнаруженными объектами. Если вы не зададите никаких значений этого ключа, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет выполнять действие Пропускать .	
DISINFECT	Лечить, если невозможно, пропускать.
DISINFDEL	Лечить, если невозможно, удалять.
DELETE	Удалять Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Industrial CyberSecurity for Nodes 2.5 для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI и /AS. В этом случае Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
/AS: Действия над возможно зараженными объектами. Если вы не зададите никаких значений этого ключа, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет выполнять действие Пропускать .	
QUARANTINE	Карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие

Ключ	Описание
Исключения	
/E:ABMSPO	Ключ исключает составные объекты следующих типов: А – SFX-архивы; В – почтовые базы; М – файлы почтовых форматов; S – архивы (включая SFX-архивы); Р – упакованные объекты; О – 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 в продолжительности проверки нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанный значением <размер>. По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты любого размера.
/TZOFF	Отменить исключения доверенной зоны.
Дополнительные параметры (Options)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ANALYZERLEVEL:<уровень анализа>	Включить использование эвристического анализатора, настроить уровень анализа. Сюда входят следующие уровни эвристического анализа: 1 – поверхностный; 2 – средний; 3 – глубокий. Если вы опустите этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет использовать эвристический анализатор.
/ALIAS:<альтернативное имя задачи>	Ключ позволяет присвоить задаче проверки по требованию временное имя, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5. Если этот ключ не задан, задаче присваивается альтернативное имя scan_<kavshell_pid>, например, scan_1234. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 задаче присваивается имя Scan objects (<дата и время>), например: Scan objects 8/16/2007 5:13:14 PM.
Параметры журналов выполнения задач (Report settings)	

Ключ	Описание
/W:<имя файла журнала выполнения задачи>	<p>Если вы укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.</p> <p>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.</p> <p>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Industrial CyberSecurity for Nodes 2.5 в консоли "Просмотр событий".</p> <p>Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.</p> <p>Если Kaspersky Industrial CyberSecurity for Nodes 2.5 не удастся создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.</p>
/ANSI	<p>Ключ позволяет записывать события в журнал выполнения задач в кодировке ANSI.</p> <p>Ключ ANSI не будет применяться, если не задан ключ W.</p> <p>Если ключ ANSI не указан, то журнал выполнения задач ведется в кодировке UNICODE.</p>

Запуск задачи Проверка важных областей. KAVSHELL SCANCritical

Используйте команду `KAVSHELL SCANCritical`, чтобы запустить системную задачу проверки по требованию Проверка важных областей с параметрами, заданными в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

Синтаксис команды KAVSHELL SCANCritical

`KAVSHELL SCANCritical [/W:<имя файла журнала выполнения задачи>]`

Примеры команды KAVSHELL SCANCritical

Чтобы выполнить задачу проверки по требованию Проверка важных областей; сохранить журнал выполнения задачи в файле `scancritical.log` в текущей папке, выполните следующую команду:

`KAVSHELL SCANCritical /W:scancritical.log`

В зависимости от синтаксиса ключа /W вы можете настраивать местоположение файла журнала выполнения задачи (см. таблицу ниже).

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Таблица 54. Синтаксис ключа /W команды KAVSHELL SCANCritical

Ключ	Описание
/W:<имя файла журнала выполнения задачи>	<p>Если вы укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.</p> <p>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.</p> <p>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий программы в консоли "Просмотр событий".</p> <p>Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.</p> <p>Если Kaspersky Industrial CyberSecurity for Nodes 2.5 не удастся создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.</p>

Управление указанной задачей в асинхронном режиме. KAVSHELL TASK

С помощью команды KAVSHELL TASK вы можете 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:<password>].

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное имя задачи> </START | /STOP | /PAUSE | /RESUME  
| /STATE | /STATISTICS >]
```

Примеры команды KAVSHELL TASK

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

KAVSHELL TASK scan-computer /STATE

Команда KAVSHELL TASK может быть выполнена как без ключей, так и с использованием одного либо нескольких ключей (см. таблицу ниже).

Таблица 55. Ключи команды KAVSHELL TASK

Ключ	Описание
Без ключей	Команда возвращает список всех существующих задач Kaspersky Industrial CyberSecurity for Nodes 2.5. Список содержит поля: альтернативное имя задачи, категория задачи (системная или пользовательская) и текущий статус задачи.
<альтернативное имя задачи>	Вместо имени задачи в команде SCAN TASK используйте ее альтернативное имя (Task alias) – дополнительное, краткое имя, которое Kaspersky Industrial CyberSecurity for Nodes 2.5 присваивает задачам. Чтобы просмотреть альтернативные имена задач Kaspersky Industrial CyberSecurity for Nodes 2.5, введите команду KAVSHELL TASK без ключей.
/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, Восстанавливается)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

Коды возврата команды KAVSHELL TASK (см. раздел "Коды возврата команды KAVSHELL TASK" на стр. [288](#)).

Запуск и остановка задач постоянной защиты. KAVSHELL RTP

С помощью команды KAVSHELL RTP вы можете запустить или остановить все задачи постоянной защиты.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

Синтаксис команды KAVSHELL RTP

KAVSHELL RTP </START | /STOP>

Примеры команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты, выполните следующую команду:

KAVSHELL RTP /START

Команда KAVSHELL RTP может включать любой из двух обязательных ключей (см. таблицу ниже).

Таблица 56. Ключи команды KAVSHELL RTP

Ключ	Описание
/START	Остановить все задачи постоянной защиты. Постоянная защита файлов и Использование KSN.
/STOP	Остановить все задачи постоянной защиты.

Управление задачами Контроль запуска программ KAVSHELL APPCONTROL /CONFIG

С помощью команды KAVSHELL APPCONTROL /CONFIG вы можете 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 выполнять задачу Контроль запуска программ в режиме **Активный** без загрузки DLL-модуля и сохранить параметры задачи по завершении, выполните 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 57. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
/mode:<applyrules statistics>	Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: <ul style="list-style-type: none"> • active - Активный; • statistics - Только статистика.
/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.

Автоматическое формирование разрешающих правил KAVSHELL APPCONTROL /GENERATE

С помощью команды KAVSHELL APPCONTROL /GENERATE вы можете формировать списки правил контроля запуска программ.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

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 всех доступных расширений в указанной папке и по завершении задачи сохранить сформированные правила в указанный файл формата XML, выполните команду:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c:\rules\appctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете настраивать параметры автоматического формирования правил контроля запуска программ (см. таблицу ниже).

Таблица 58. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
Область применения разрешающих правил	

Ключ	Описание
<путь к папке>	Путь к папке, содержащей исполняемые файлы, для которых требуется автоматически создать разрешающие правила.
/source: <путь к файлу со списком папок>	Путь к файлу в формате TXT, содержащий список папок с исполняемыми файлами, для которых требуется автоматически создать разрешающие правила.
/masks: <edms>	<p>Расширения исполняемых файлов, для которых требуется создать разрешающие правила контроля запуска программ.</p> <p>Вы можете включить в область срабатывания создаваемых правил файлы следующих расширений:</p> <ul style="list-style-type: none"> • 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 момент выполнения задачи.
Действия при автоматическом формировании правил	
/rules: <ch cp h>	<p>Указать действия, которые задача совершает во время формирования разрешающих правил контроля запуска программ:</p> <ul style="list-style-type: none"> • ch - использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256. • cp - использовать цифровой сертификат. Если сертификат отсутствует, использовать значение пути к исполняемому файлу. • h - использовать хеш SHA256.
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании правил контроля 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.
Действия по завершении автоматического формирования правил	
/export: <полный путь к XML файлу>	Сохранять сформированные правила в файл формата XML.
/unique	Добавлять информацию о компьютере, по программам которого формируются разрешающие правила контроля запуска программ.
/prefix: <префикс для названий правил>	Префикс для названий создаваемых правил контроля запуска программ.

Ключ	Описание
/import: <a r m>	<p>Импортировать сформированные правила в список заданных правил контроля запуска программ в соответствии с указанным принципом добавления новых правил:</p> <ul style="list-style-type: none"> • а - Добавлять к существующим правилам (одинаковые правила дублируются); • г - Заменять существующие правила (новые правила добавляются вместо заданных правил); • т - Объединять с существующими правилами (добавляются новые правила, параметры которых не совпадают с параметрами уже заданных правил).

Заполнение списка правил задачи Контроль запуска программ KAVSHELL APPCONTROL

С помощью команды `KAVSHELL APPCONTROL` вы можете добавлять правила в список правил задачи Контроль запуска программ из файла формата XML в соответствии с выбранным принципом, а также удалять все заданные правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

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 заданным правилам контроля запуска программ правила из файла формата XML по принципу **Добавить к существующим правилам**, выполните команду:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете выбирать принцип добавления новых правил из указанного файла формата XML в список заданных правил задачи Контроль запуска программ (см. таблицу ниже).

Таблица 59. Ключи команды KAVSHELL APPCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	<p>Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - Добавить к существующим правилам (одинаковые правила дублируются).</p>

/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - Заменить существующие правила (новые правила добавляются вместо заданных правил).
/merge <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления – Объединить правила с существующими (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля запуска программ.

Запуск задачи обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL UPDATE

С помощью команды `KAVSHELL UPDATE` вы можете запускать задачу обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 в синхронном режиме.

Задача обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5, запущенная с помощью команды `KAVSHELL UPDATE`, является временной. Она отображается в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 только во время ее выполнения. В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. К задачам обновления, созданным и запущенным с помощью команды `KAVSHELL UPDATE`, как и к задачам обновления, созданным в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, могут применяться политики программы Kaspersky Security Center. Об управлении Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах с помощью программы Kaspersky Security Center читайте в разделе "Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 из Kaspersky Security Center".

Указывая путь к источнику обновлений в этой задаче, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду `KAVSHELL UPDATE` с правами этого пользователя.

Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE < Источник обновления | /AK | /KL> [/NOUSEKL]
[/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>]
[/PROXYPWD:<пароль>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<количество секунд>] [/REG:<код iso3166>] [/W:<имя
файла журнала выполнения задачи>] [/ALIAS:<альтернативное имя задачи>]
```

В состав команды `KAVSHELL UPDATE` входят как обязательные, так и дополнительные ключи, использование которых не является обязательным (см. таблицу ниже).

Примеры команды KAVSHELL UPDATE

► Чтобы запустить пользовательскую задачу обновления баз, выполните следующую команду:

```
KAVSHELL UPDATE
```


- Чтобы запустить задачу обновления баз, файлы обновлений для которой хранятся в сетевой папке `\\server\databases`, выполните следующую команду:

```
KAVSHELL UPDATE \\server\bases
```

- Чтобы запустить задачу обновления с FTP-сервера <ftp://dnl-ru1.kaspersky-labs.com/>, записать все события задачи в файл журнала `c:\update_report.log`, выполните команду:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- Чтобы получить обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 с сервера обновлений "Лаборатории Касперского", соединиться с источником обновлений через прокси-сервер (адрес прокси-сервера: `proxy.company.com`, порт: 8080) для доступа к компьютеру использовать встроенную проверку подлинности Microsoft Windows (NTLM-authentication) под учетной записью: имя пользователя, пароль: 123456, выполните следующую команду:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1  
/PROXYUSER:inetuser /PROXYPWD:123456
```

При использовании данного способа обновлений программа выходит из сертифицированного состояния.

Таблица 60. Ключи команды KAVSHELL UPDATE

Ключ	Описание
Источники обновления (обязательный ключ). Укажите один или несколько источников. Kaspersky Industrial CyberSecurity for Nodes 2.5 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. Пользовательский источник обновлений – адрес HTTP- или FTP-сервера, на котором помещается папка с обновлениями.
<Локальная папка>	Пользовательские источники обновления. Папка на защищаемом компьютере.
/AK	Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
/KL	Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений
/NOUSEKL	Не использовать серверы обновлений "Лаборатории Касперского", если другие указанные источники обновлений недоступны (по умолчанию используются).
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет автоматически

Ключ	Описание
	распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	<p>Этот ключ задает метод проверки подлинности для доступа к прокси-серверу. Он может принимать следующие значения:</p> <p>0 – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Industrial CyberSecurity for Nodes 2.5 будет обращаться к прокси-серверу под учетной записью Локальная система (SYSTEM);</p> <p>1 – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Industrial CyberSecurity for Nodes 2.5 будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD;</p> <p>2 – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication).</p> <p>Если для доступа к прокси-серверу не требуется проверка подлинности, указывать этот ключ нет необходимости.</p>
/PROXYUSER:<имя пользователя>	Имя пользователя, которое будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.
/PROXYPWD:<пароль>	Пароль пользователя, который будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если вы укажете ключ /PROXYUSER, а ключ /PROXYPWD опустите, считается что пароль пустой.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию используются)
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используются)
/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 вы укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать пассивный режим FTP-сервера, если возможно.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать значение по умолчанию: 10 сек. В качестве значения ключа вы можете вводить только целые числа.
/REG:<код iso3166>	Региональные параметры. Ключ "Региональные" используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Industrial CyberSecurity for Nodes 2.5 оптимизирует загрузку обновлений на защищаемый компьютер, выбирая ближайший к нему сервер обновлений.

Ключ	Описание
	В качестве значения ключа укажите буквенный код страны местоположения защищаемого компьютера в соответствии со стандартом ISO 3166-1, например, /REG:gr или /REG:RU. Если вы опустите этот ключ или укажете несуществующий код страны, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет распознавать местоположение защищаемого компьютера в соответствии с региональными настройками компьютера, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
/ALIAS:<альтернативное имя задачи>	Этот ключ 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 имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5. Если этот ключ не задан, задаче присваивается альтернативное имя update_<kavshell_pid>, например, update_1234. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 задаче присваивается имя Update-bases <дата и время>, например: Update-bases 8/16/2007 5:41:02 PM.
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Industrial CyberSecurity for Nodes 2.5 в консоли "Просмотр событий". Вы можете указать как абсолютный, так и 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 Kaspersky Industrial CyberSecurity for Nodes 2.5. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 не удастся создать файл журнала, он не прерывает выполнение команды и не отображает сообщение об ошибке.

Коды возврата команды KAVSHELL UPDATE (на стр. [289](#)).

Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL ROLLBACK

С помощью команды `KAVSHELL ROLLBACK` вы можете выполнить системную задачу Откат обновления баз – откатить базы Kaspersky Industrial CyberSecurity for Nodes 2.5 до предыдущих установленных обновлений. Команда выполняется синхронно.

Синтаксис команды

KAVSHELL ROLLBACK

Коды возврата команды KAVSHELL ROLLBACK (на стр. [289](#)).

Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR

Команда KAVSHELL TASK LOG-INSPECTOR позволяет настроить контроль целостности среды компьютера, основываясь на анализе журнала событий Windows.

Синтаксис команды

KAVSHELL TASK LOG-INSPECTOR

Пример команды

KAVSHELL TASK LOG-INSPECTOR /stop

Таблица 61. Ключи команды KAVSHELL TASK LOG-INSPECTOR

Ключ	Описание
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/STATE	Получить текущее состояние задачи (например, <i>Выполняется, Завершена, Приостановлена, Остановлена, Завершена с ошибкой, Запускается, Восстанавливается</i>)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

Команда "Коды возврата команды KAVSHELL TASK LOG-INSPECTOR" (см. раздел "Коды возврата команды KAVSHELL TASK LOG-INSPECTOR" на стр. [287](#)).

Активация программы KAVSHELL LICENSE

Управлять ключами DE-Cleaner powered by Kaspersky можно с помощью команды KAVSHELL LICENSE.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

Синтаксис команды KAVSHELL LICENSE

KAVSHELL LICENSE [/ADD:<файл ключа> [/R] | /DEL:<номер ключа>]

Примеры команды KAVSHELL LICENSE

► Чтобы активировать программу, выполните команду:

KAVSHELL.EXE LICENSE / ADD: Номер 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 62. Ключи команды KAVSHELL LICENSE

Ключ	Описание
Без ключей	Команда возвращает следующую информацию о добавленных ключах: <ul style="list-style-type: none"> • Номер ключа. • Тип лицензии (коммерческая или пробная). • Срок действия связанной с ключом лицензии. • Статус ключа (активный или дополнительный). Если указано значение *, ключ добавлен в качестве дополнительного.
/ADD:<имя файла ключа>	Добавляет ключ с помощью указанного файла. Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/R	Ключ /R является дополнительным к ключу /ADD и указывает на то, что ключ добавляется в качестве дополнительного.
/DEL:<номер ключа>	Удаляет ключ с указанным номером.

Коды возврата команды KAVSHELL LICENSE (см. раздел "Коды возврата команды KAVSHELL LICENSE" на стр. [290](#)).

Включение, настройка и выключение создания журнала трассировки. KAVSHELL TRACE

С помощью команды `KAVSHELL TRACE` вы можете включать или выключать ведение журнала трассировки всех подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5, а также устанавливать уровень детализации информации в журнале.

Kaspersky Industrial CyberSecurity for Nodes записывает информацию в файлы трассировки и файл дампа в незашифрованном виде.

Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<папка с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Если журнал трассировки ведется и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом `/ON` и задайте параметры журнала значениями ключей `/S` и `/LVL` (см. таблицу ниже).

Таблица 63. Ключи команды KAVSHELL TRACE

Ключ	Описание
<code>/ON</code>	Включить ведение журнала трассировки.
<code>/F:<папка с файлами журнала трассировки></code>	<p>Этот ключ указывает полный путь к папке, в которой будут сохранены файлы журнала трассировки (обязательный ключ).</p> <p>Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Вы можете указывать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого компьютера.</p> <p>Если имя папки, путь к которой вы указываете в качестве значения ключа, содержит символ пробела, заключите этот путь в кавычки, например: <code>/F:"C:\Trace Folder"</code>. <code>/F:"C:\Trace Folder"</code>.</p> <p>Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p>
<code>/S: /S: <максимальный размер файла журнала в мегабайтах></code>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Industrial CyberSecurity for Nodes 2.5 начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.

Ключ	Описание
	Если вы не укажете этот ключ, максимальный размер одного файла журнала составит 50 МБ.
/LVL:debug info warning error critical	Этот ключ 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 вы не укажете этот ключ, в журнал трассировки будут записываться события с уровнем детализации Вся отладочная информация .
/OFF	Этот ключ выключает ведение журнала трассировки.

Примеры 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 папке C:\Trace Folder, выполните команду:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

- Чтобы выключить ведение журнала трассировки, выполните команду:

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE (см. раздел "Коды возврата команды KAVSHELL TRACE" на стр. [290](#)).

Дефрагментация файлов журнала Kaspersky Industrial CyberSecurity for Nodes 2.5. KAVSHELL VACUUM

С помощью команды KAVSHELL VACUUM вы можете провести дефрагментацию файлов журнала событий программы. Это позволяет избежать ошибок в работе системы или Kaspersky Industrial CyberSecurity for Nodes 2.5, связанных с хранением большого количества файлов отчетов, сформированных по событиям работы программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

Рекомендуется применять команду KAVSHELL VACUUM для оптимизации хранения файлов отчетов при частых запусках задач проверки по требованию или задач обновления. При выполнении команды Kaspersky Industrial CyberSecurity for Nodes 2.5 обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом компьютере по указанному пути.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

По умолчанию файлы журнала событий работы программы сохраняются по пути C:\ProgramData\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes 2.5\2.5\Reports. Если вы вручную указали другой путь для хранения файлов журналов, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журналов Kaspersky Industrial CyberSecurity for Nodes 2.5.

Большой размер дефрагментируемых файлов журнала событий увеличивает время выполнения команды `KAVSHELL VACUUM`.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля компьютера. Процедура дефрагментации блокирует доступ к журналам Kaspersky Industrial CyberSecurity for Nodes 2.5 и запрещает запись событий в журнал. Во избежание снижения уровня защиты компьютера рекомендуется заранее планировать выполнение команды `KAVSHELL VACUUM` в нерабочее время.

- Чтобы выполнить дефрагментацию файлов журналов, созданных по событиям работы Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните команду:

```
KAVSHELL VACUUM
```

Выполнение команды доступно при запуске с правами учетной записи локального администратора.

Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Industrial CyberSecurity for Nodes 2.5 использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

В системном каталоге %SYSTEMDRIVE%\System Volume Information Kaspersky Industrial CyberSecurity for Nodes 2.5 создает файлы fidbox.dat и fidbox2.dat, которые содержат информацию об уже проверенных незараженных объектах. Чем больше различных файлов проверил Kaspersky Industrial CyberSecurity for Nodes 2.5, тем больше размер файла fidbox.dat (fidbox2.dat). В данном файле хранится только актуальная информация о реально существующих в системе файлах: если какой-либо файл в системе удаляется, то Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет информацию о нем из файла fidbox.dat.

Для очищения данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла fidbox.dat с помощью команды `KAVSHELL FBRESET` Kaspersky Industrial CyberSecurity for Nodes 2.5 не приостанавливает защиту (в отличие от удаления файла fidbox.dat вручную).
- После очистки файла fidbox.dat Kaspersky Industrial CyberSecurity for Nodes 2.5 может увеличить нагрузку на компьютер. При этом антивирусная программа проверяет все файлы, к которым обращается впервые после очистки файла fidbox.dat. После проверки Kaspersky Industrial CyberSecurity for Nodes 2.5 вновь заносит в файл fidbox.dat информацию о проверенном объекте. При повторном обращении к этому же объекту технология iSwift позволит не сканировать файл повторно, если он не был изменён.

Для выполнения команды `KAVSHELL FBRESET` необходимо запускать командную строку под учетной записью `SYSTEM`.

Включение и выключение создания файла дампа. KAVSHELL DUMP

С помощью команды `KAVSHELL DUMP` вы можете включать или выключать создание образов памяти (файла дампа) процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 при их аварийном завершении (см. таблицу ниже). Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Kaspersky Industrial CyberSecurity for Nodes 2.5.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена под учетной записью локальной системы (`SYSTEM`).

Синтаксис команды KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом дампа> / P:<pid> | /OFF>
```

Примеры команды KAVSHELL DUMP

- Чтобы включить создание файла дампа; сохранять 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 файла дампа, выполните команду:

```
KAVSHELL DUMP /OFF
```

Таблица 64. Ключи команды KAVSHELL DUMP

Ключ	Описание
/ON	Включает создание файла дампа процесса при его аварийном завершении.
/F:<папка с файлами дампов>	Это обязательный ключ. Обязательный ключ; указывает путь к папке, в которой будет сохранен файл дампа. Если вы укажете путь к несуществующей папке, файл дампа не будет создан. Вы можете использовать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого компьютера.

Ключ	Описание
	Указывая путь к папке с файлом дампа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/SNAPSHOT	Снимает образ памяти указанного выполняющегося процесса Kaspersky Industrial CyberSecurity for Nodes 2.5 и сохраняет файл дампа в папке, путь к которой указан ключом /F.
/P	Идентификатор PID процесса; отображается в Диспетчере задач Microsoft Windows.
/OFF	Выключает создание файла дампа при аварийном завершении.

Коды возврата команды KAVSHELL DUMP (см. раздел "Коды возврата команды KAVSHELL DUMP" на стр. [291](#)).

Импорт параметров. KAVSHELL IMPORT

С помощью команды KAVSHELL IMPORT вы можете импортировать параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, его функций и задач из конфигурационного файла в Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере. Вы можете создать конфигурационный файл с помощью команды KAVSHELL EXPORT.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<password>].

Синтаксис команды KAVSHELL IMPORT

KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>

Примеры команды KAVSHELL IMPORT

KAVSHELL IMPORT Host1.xml

Таблица 65. Ключи команды KAVSHELL IMPORT

Ключ	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 (см. раздел "Коды возврата команды KAVSHELL IMPORT" на стр. [291](#)).

Экспорт параметров. KAVSHELL EXPORT

С помощью команды `KAVSHELL EXPORT` вы можете экспортировать все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Industrial CyberSecurity for Nodes 2.5 на других компьютерах.

Синтаксис команды KAVSHELL EXPORT

`KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>`

Примеры команды KAVSHELL EXPORT

`KAVSHELL EXPORT Host1.xml`

Таблица 66. Ключи команды KAVSHELL EXPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Вы можете присвоить конфигурационному файлу любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды `KAVSHELL EXPORT` (см. раздел "Коды возврата команды KAVSHELL EXPORT" на стр. [292](#)).

Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

С помощью команды `KAVSHELL OMSINFO` можно просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами и службой KSN. Данные об угрозах поступают из доступных журналов событий.

Синтаксис команды KAVSHELL OMSINFO

`KAVSHELL OMSINFO <полный путь к сгенерированному файлу с именем файла>`

Примеры команды KAVSHELL OMSINFO

`KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json`

Таблица 67. Ключи команды KAVSHELL OMSINFO

Ключ	Описание
<путь к сгенерированному файлу с именем файла>	Имя сгенерированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах.

Ошибка! Используйте вкладку "Главная" для применения Heading 1 к тексту, который должен здесь отображаться.

Коды возврата командной строки

В этом разделе

Коды возврата команд KAVSHELL START и KAVSHELL STOP	286
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical.....	287
Коды возврата команды KAVSHELL TASK LOG-INSPECTOR.....	287
Коды возврата команды KAVSHELL TASK.....	288
Коды возврата команды KAVSHELL RTP	288
Коды возврата команды KAVSHELL UPDATE.....	289
Коды возврата команды KAVSHELL ROLLBACK.....	289
Коды возврата команды KAVSHELL LICENSE	290
Коды возврата команды KAVSHELL TRACE	290
Коды возврата команды KAVSHELL FBRESET.....	291
Коды возврата команды KAVSHELL DUMP.....	291
Коды возврата команды KAVSHELL IMPORT	291
Коды возврата команды KAVSHELL EXPORT	292

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Таблица 68. 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 Industrial CyberSecurity for Nodes 2.5 уже запущена или уже остановлена)
-7	Служба не зарегистрирована
-8	Автоматический запуск службы отключен
-9	Попытка запустить службу под другой учетной записью не была успешной (по умолчанию служба Kaspersky Industrial CyberSecurity for Nodes 2.5 работает под учетной записью Локальная система).
-99	Неизвестная ошибка

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical

Таблица 69. 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 обнаруженных объектов
-81	Возможно зараженных объектов
-82	Обнаружены ошибки обработки
-83	Обнаружены непроверенные объекты
-84	Обнаружены поврежденные объекты
-85	Не удалось создать файл журнала выполнения задачи
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Таблица 70. Код возврата команды KAVSHELL TASK LOG-INSPECTOR

Код возврата	Описание
0	Операция выполнена успешно
-6	Неверная операция (например, служба Kaspersky Industrial CyberSecurity for Nodes 2.5 уже запущена или уже остановлена)
402	Задача уже запущена (для ключа /STATE)

Коды возврата команды KAVSHELL TASK

Таблица 71. 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 ключа /STATE)
402	Задача уже запущена (для ключа /STATE)
403	Задача уже приостановлена (для ключа /STATE)
-404	Ошибка выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL RTP

Таблица 72. 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 какая-либо из задач постоянной защиты или все задачи постоянной защиты)
-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 73. 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 2.5 не прошел проверку подлинности при соединении с источником обновлений
-236	Базы программы повреждены
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Таблица 74. 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 75. 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 76. 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, указанный в качестве пути к папке с файлами журнала трассировки)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL FBRESET

Таблица 77. Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL DUMP

Таблица 78. 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, указанный в качестве пути к папке с файлом дампа; не найден процесс с указанным PID)
-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 79. 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 найден импортируемый конфигурационный файл)
-5	Неверный синтаксис
-99	Неизвестная ошибка

Код возврата	Описание
501	Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Kaspersky Industrial CyberSecurity for Nodes 2.5 не импортировал параметры какого-либо из функциональных компонентов
-502	Импортируемый файл отсутствует или имеет неизвестный формат
-503	Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Industrial CyberSecurity for Nodes 2.5 более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Таблица 80. 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 команды возникла ошибка / замечание, например, Kaspersky Industrial CyberSecurity for Nodes 2.5 не экспортировал параметры какого-либо из функциональных компонентов

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, программы еще раз проведут контроль целостности загружаемых обновлений.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений программы на дисках.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (<https://support.kaspersky.ru/general/certificates>) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (<https://forum.kaspersky.com>).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. [296](#)).

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2c>) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2c>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;

- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Microsoft, Active Directory, Excel, Outlook, Internet Explorer, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Schneider Electric – товарный знак компании Schneider Electric.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 81. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
операционная система, промышленная инфраструктура, промышленная сеть	среда функционирования
защищаемый компьютер	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь
уведомления пользователей и администратора	сигналы тревоги

Глоссарий

К

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, интернет-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

О

OLE-объект

Объект, прикрепленный к другому файлу или вложенный в другой файл путем использования технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel®, встроенная в документ Microsoft Office Word.

S

SIEM

Технология, которая обеспечивает анализ событий безопасности, исходящих от различных сетевых устройств и приложений.

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

3

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера и Обновление баз программы.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует обрабатывать такие объекты.

К

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

М

Маска файла

Представление имени файла с помощью специальных символов. Стандартными специальными символами, используемыми в масках файлов, являются * и ?, где * представляет любое количество символов, а ? представляет любой отдельный символ.

О

Обновление

Процедура замены/добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор программ, необходимых для запуска и правильной работы операционной системы и установленного на компьютере программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

П

Параметры задачи

Параметры программы, специфические для каждого типа задач.

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный "Лаборатории Касперского". Подозрительные объекты обнаруживаются с помощью эвристического анализатора.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться одновременно к каждой программе.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект (на чтение, запись и исполнение) и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы, или возможно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются или помещаются на карантин).

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe и dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Р

Резервное хранилище:

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой дезинфекции или удаления.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

У

Уровень безопасности

Уровень безопасности представляет собой предварительно заданный набор параметров компонентов программы.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Ошибка.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу

ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

Приложение. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированной конфигурации на другие значения, выводит программу из безопасного состояния.

Таблица 82. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметры установки		
Компонент Управление сетевым экраном	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (по умолчанию)
Компонент Контроль устройств	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (флажок снят)
Компонент Постоянная защита	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Контроль запуска программ	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Настройки прав доступа и функциональных компонентов		
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5. <ul style="list-style-type: none"> Запущена Остановлена 	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5: <ul style="list-style-type: none"> Разрешить Запретить 	Учетные записи пользователей-администраторов безопасности должны быть добавлены в группу KICS Administrators. Для всех пользователей и групп, кроме KICS Administrators и SYSTEM, установлены флажки Запретить .

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5. <ul style="list-style-type: none"> Запущена Остановлена 	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Выполняется Остановлена 	Выполняется
Лицензирование	Активация программы с помощью ключа.	Добавлен файл ключа. По окончании срока действия ключа программа выходит из сертифицированного состояния.
Использовать Локальный KSN	Взаимодействие с Глобальным или Локальным KSN, настраиваемое в Kaspersky Security Center.	Запускать задачу Использование KSN следует только при использовании Локального KSN (флажок Настроить Локальный KSN установлен), в том числе при отсутствии управления программой через Kaspersky Security Center.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметры задач Постоянная защита / проверка по требованию		
Архивы	<p>Проверка архивов в указанной области защиты в параметрах задачи Постоянной защиты файлов.</p> <ul style="list-style-type: none"> • Применяется (флажок установлен). • Не применяется (флажок снят). 	Применяется (флажок установлен).
Загрузочные секторы дисков и MBR	<p>Проверять загрузочные секторы и загрузочные надписи на жестких и съемных дисках сервера.</p> <ul style="list-style-type: none"> • Применяется (флажок установлен). • Не применяется (флажок снят). 	Применяется (флажок установлен).
Область защиты	<p>Папки и файлы находящиеся под защитой задач Постоянная защита и Проверка по требованию.</p> <ul style="list-style-type: none"> • Любые локальные и сетевые папки. 	<p>По умолчанию.</p> <p>Исключение папок из области защиты, установленной по умолчанию, ведет к выходу из сертифицируемого состояния.</p>
Пропускать для любого типа объектов	<p>Действия при обнаружении объектов:</p> <ul style="list-style-type: none"> • Лечить • Удалять • Помещать на карантин • Пропускать 	<p>Не выбрано.</p> <p>При выборе действия Пропускать для любого типа объектов, программа выходит из сертифицированного состояния.</p>
Объекты, проверяемые по указанному списку расширений	<p>На закладке Общие, выберите объекты, которые необходимо защищать:</p> <ul style="list-style-type: none"> • Все объекты • Объекты, проверяемые по формату • Объекты, проверяемые по списку расширений, указанному в антивирусных базах • Объекты, проверяемые по указанному списку расширений 	<p>Флажок снят.</p> <p>Наполнение списка расширений объектов вручную ведет к выходу программы из сертифицированного состояния.</p>

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Исключать файлы	Исключение файлов из проверки по имени файла или маске имени файла: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Применяется (флажок установлен). Не применяется (флажок снят). 	Не применяется (Флажок снят).
Использовать эвристический анализатор	Применение эвристического анализатора: <ul style="list-style-type: none"> Применяется (флажок установлен). Не применяется (флажок снят). 	Применяется (флажок установлен). Снятие флажка ведет к выходу программы из сертифицированного состояния.
Параметры задач обновления		
Серверы обновлений «Лаборатории Касперского» на компьютере-ретрансляторе (Задача Копирование обновлений)	Источник обновлений баз программы: <ul style="list-style-type: none"> Сервер администрирования Kaspersky Security Center. Серверы обновлений «Лаборатории Касперского». Другие HTTP-, FTP-серверы или сетевые ресурсы. 	На компьютере-ретрансляторе выбран вариант Серверы обновлений «Лаборатории Касперского» . Для работы программы в сертифицированной конфигурации, задачи обновления должны осуществляться через один из защищаемых компьютеров сети.
Копировать обновления программы (Задача Копирование обновлений)	Укажите условия копирования обновлений программы: <ul style="list-style-type: none"> Копировать обновления программы. Копировать критические обновления модулей программы. Копировать обновления баз программы и критические обновления модулей программы. 	Выбран вариант Копировать обновления программы . Kaspersky Industrial CyberSecurity for Nodes 2.5 загружает только обновления баз Kaspersky Security.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Другие HTTP-, FTP-серверы или сетевые ресурсы на серверах-ресиверах.	<p>Источник обновлений баз программы:</p> <ul style="list-style-type: none"> Сервер администрирования Kaspersky Security Center Серверы обновлений «Лаборатории Касперского» Другие HTTP-, FTP-серверы или сетевые ресурсы 	<p>На серверах-ресиверах выбран вариант Другие HTTP-, FTP-серверы или сетевые ресурсы.</p> <p>В качестве источника должна быть указана сетевая папка, настроенная в качестве папки локального источника обновлений в задаче Копирование обновлений на компьютер-ретрансляторе.</p>
Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны на серверах-ресиверах. (Задача Обновление баз программы)	<p>При выборе источника обновления Другие HTTP-, FTP-серверы или сетевые ресурсы, активируется функция использования серверов обновлений «Лаборатории Касперского».</p> <ul style="list-style-type: none"> Применяется (флажок установлен). Не применяется (флажок снят). 	<p>Не применяется (флажок снят).</p> <p>Обновление через сервера обновлений «Лаборатории Касперского» запрещено.</p>
Частота запуска задачи Обновление баз программы	<p>Промежуток времени, через которое задача осуществляет проверку наличия обновлений:</p> <ul style="list-style-type: none"> Ежечасно Ежесуточно Еженедельно При запуске программы После получения обновлений Сервером администрирования 	<p>Ежечасно (по умолчанию).</p> <p>Снижение частоты запусков задачи, установленного по умолчанию ведет к выходу программы из сертифицированного состояния.</p>

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройка параметров аудита		
События для компонентов постоянной защиты, проверки по требованию, KSN, лицензирования и обновлений баз программы.	Регистрация событий в параметрах журналов. <ul style="list-style-type: none"> • Все события • Набор событий по умолчанию 	Для компонентов Постоянная защита, Проверка по требованию, Использование KSN, Лицензирование и задачи Обновление баз программы установлены оповещения о событиях по умолчанию.
Удалять события в журналах выполнения задач старше, чем (сут.)	Очистка журнала выполнения задач через заданный прометужок времени.	30 сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Удалять события в журнале системного аудита старше, чем (сут.)	Очистка журнала системного аудита через заданный прометужок времени.	60 сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Пороги формирования событий	Промежуток времени, через который возникают события: <ul style="list-style-type: none"> • Базы программы устарели. • Базы программы сильно устарели. • Проверка важных областей компьютера давно не выполнялась. 	По умолчанию выставлены следующие значения: 7 (сут) 14 (сут) 30 (сут) Уменьшение порога формирования событий ведет к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройка сигналов тревоги		
Путем запуска исполняемого файла	<p>Способы уведомления администраторов:</p> <ul style="list-style-type: none"> • Средствами службы сообщений; • Путем запуска исполняемого файла; • По электронной почте. 	<p>Флажок Путем запуска исполняемого файла установлен для событий:</p> <ul style="list-style-type: none"> • Обнаружен объект • Объект не вылечен • Объект не удален • Запуск программы запрещен • Запуск программы запрещен по прецеденту • Объект не помещен на карантин • Объект не помещен в резервное хранилище
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.