kaspersky

# Kaspersky Embedded Systems Security для Windows

Руководство по эксплуатации

Версия программы: 3.3.0.87

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: 26.10.2023

© 2023 АО "Лаборатория Касперского"

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

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

kaspersky

# Содержание


О Kaspersky Embedded Systems Security для Windows ..... 20
Что нового ..... 22
Источники информации о Kaspersky Embedded Systems Security для Windows ..... 23
Источники для самостоятельного поиска информации ..... 23
Обсуждение программ "Лаборатории Касперского" на форуме ..... 24
Kaspersky Embedded Systems Security для Windows ..... 25
Комплект поставки ..... 25
Программные и аппаратные требования ..... 28
Функциональные требования и ограничения ..... 33
Установка и удаление ..... 33
Мониторинг файловых операций ..... 34
Управление сетевым экраном ..... 35
Прочие ограничения ..... 35
Установка и удаление программы ..... 37
Об обновлении Kaspersky Embedded Systems Security для Windows ..... 37
Миграция значений параметров обновляемой версии программы ..... 38
Об обновлении средств администрирования Kaspersky Embedded Systems Security для Windows ..... 40
Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows ..... 41
Программные компоненты Kaspersky Embedded Systems Security для Windows ..... 42
Программный компонент "Средства администрирования" ..... 45
Изменения в системе после установки Kaspersky Embedded Systems Security для Windows ..... 45
Процессы Kaspersky Embedded Systems Security для Windows ..... 48
Параметры установки и удаления и ключи командной строки для службы установщика Windows ..... 49
Журналы установки и удаления Kaspersky Embedded Systems Security для Windows ..... 53
Планирование установки ..... 54
Выбор средств администрирования ..... 54
Выбор способа установки ..... 56
Установка и удаление программы с помощью мастера ..... 57
Установка с помощью мастера установки ..... 57
Установка Kaspersky Embedded Systems Security для Windows ..... 58
Установка Консоли Kaspersky Embedded Systems Security для Windows ..... 60
Дополнительная настройка после установки Консоли программы на другое устройство ..... 62
Действия после установки Kaspersky Embedded Systems Security для Windows ..... 65
Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security для Windows ..... 68
Удаление с помощью мастера установки ..... 70
Удаление Kaspersky Embedded Systems Security для Windows ..... 70

Удаление Консоли Kaspersky Embedded Systems Security для Windows ..... 71
Установка и удаление программы из командной строки ..... 72
Об установке и удалении Kaspersky Embedded Systems Security для Windows из командной строки ..... 72
Примеры команд установки Kaspersky Embedded Systems Security для Windows ..... 73
Действия после установки Kaspersky Embedded Systems Security для Windows ..... 75
Добавление и удаление компонентов. Примеры команд ..... 76
Удаление Kaspersky Embedded Systems Security для Windows. Примеры команд ..... 77
Коды возврата ..... 78
Установка и удаление программы с помощью Kaspersky Security Center ..... 79
Общие сведения об установке через Kaspersky Security Center ..... 79
Права для установки или удаления Kaspersky Embedded Systems Security для Windows ..... 80
Установка Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center ..... 80
Действия после установки Kaspersky Embedded Systems Security для Windows ..... 82
Установка Консоли программы через Kaspersky Security Center ..... 83
Удаление Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center ..... 84
Установка и удаление программы через групповые политики Active Directory ..... 84
Установка Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory ..... 85
Действия после установки Kaspersky Embedded Systems Security для Windows ..... 86
Удаление Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory ..... 86
Проверка функций Kaspersky Embedded Systems Security для Windows. Использование тестового вируса EICAR ..... 87
О тестовом вирусе EICAR ..... 87
Проверка функций постоянной защиты файлов и проверки по требованию ..... 88
Интерфейс программы ..... 91
Лицензирование программы ..... 92
О Лицензионном соглашении ..... 92
О лицензии ..... 93
О Лицензионном сертификате ..... 94
О ключе ..... 94
О файле ключа ..... 95
О коде активации ..... 95
О предоставлении данных ..... 95
Активация программы с помощью файла ключа ..... 101
Активация программы с помощью кода активации ..... 102
Просмотр информации о действующей лицензии ..... 103
Функциональные ограничения после окончания срока действия лицензии ..... 106
Продление срока действия лицензии ..... 106
Удаление ключа ..... 107

Работа с Плагином управления ..... 108
Управление Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center ..... 108
Управление параметрами программы ..... 109
Навигация ..... 109
Переход к общим параметрам из политики ..... 110
Переход к общим параметрам из окна свойств программы ..... 110
Настройка общих параметров программы в Kaspersky Security Center ..... 111
Настройка параметров масштабируемости, интерфейса и проверки в Kaspersky Security Center ..... 111
Настройка параметров безопасности в Kaspersky Security Center ..... 113
Настройка параметров соединения в Kaspersky Security Center ..... 115
Настройка запуска по расписанию локальных системных задач ..... 116
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center ..... 118
Создание и настройка политик ..... 119
Создание политики ..... 120
Разделы параметров политики Kaspersky Embedded Systems Security для Windows ..... 122
Настройка политики ..... 127
Создание и настройка задач в Kaspersky Security Center ..... 128
О создании задач в Kaspersky Security Center ..... 128
Создание задачи в Kaspersky Security Center ..... 129
Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера ..... 131
Настройка групповых задач в Kaspersky Security Center ..... 132
Задача Активация программы ..... 139
Задачи обновления ..... 140
Проверка целостности программы ..... 142
Настройка параметров диагностики сбоев в Kaspersky Security Center ..... 143
Работа с расписанием задач ..... 145
Настройка расписания задач ..... 145
Включение и выключение запуска задач по расписанию ..... 147
Отчеты в Kaspersky Security Center ..... 148
Работа с Консолью Kaspersky Embedded Systems Security для Windows ..... 151
О Консоли Kaspersky Embedded Systems Security для Windows ..... 151
Интерфейс Консоли Kaspersky Embedded Systems Security для Windows ..... 152
Окно консоли Kaspersky Embedded Systems Security для Windows ..... 152
Значок области уведомлений в панели задач ..... 156
Управление Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на другом устройстве ..... 157
Настройка общих параметров программы в Консоли программы ..... 157
Управление задачами Kaspersky Embedded Systems Security для Windows ..... 163
Категории задач Kaspersky Embedded Systems Security для Windows ..... 163

Запуск, приостановка, возобновление, остановка задач вручную ..... 164
Работа с расписанием задач ..... 165
Настройка параметров расписания задач ..... 165
Включение и выключение запуска задач по расписанию ..... 166
Использование учетных записей для запуска задач ..... 167
Об использовании учетных записей для запуска задач ..... 167
Указание учетной записи для запуска задачи ..... 168
Импорт и экспорт параметров ..... 168
Об импорте и экспорте параметров ..... 169
Экспорт параметров ..... 170
Импорт параметров ..... 171
Использование шаблонов параметров безопасности ..... 172
О шаблонах параметров безопасности ..... 172
Создание шаблона параметров безопасности ..... 172
Просмотр параметров безопасности в шаблоне ..... 173
Применение шаблона параметров безопасности ..... 173
Удаление шаблона параметров безопасности ..... 174
Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security для Windows ..... 176
Работа с Веб-плагином из Веб-консоли и Облачной консоли ..... 182
Управление Kaspersky Embedded Systems Security для Windows из Веб-консоли и Облачной консоли ..... 182
Ограничения Веб-плагина ..... 183
Управление параметрами программы ..... 184
Настройка общих параметров программы с помощью Веб-плагина ..... 184
Настройка параметров масштабируемости, интерфейса и проверки с помощью Веб-плагина ..... 184
Настройка параметров безопасности с помощью Веб-плагина ..... 187
Настройка параметров соединения с помощью Веб-плагина ..... 188
Настройка запуска по расписанию локальных системных задач ..... 190
Настройка параметров карантина и резервного хранилища с помощью Веб-плагина ..... 191
Создание и настройка политик ..... 192
Создание политики ..... 193
Разделы параметров политики Kaspersky Embedded Systems Security для Windows ..... 194
Создание и настройка задач в Kaspersky Security Center ..... 199
О создании задач с помощью Веб-плагина ..... 199
Создание задачи с помощью Веб-плагина ..... 200
Настройка групповых задач с помощью Веб-плагина ..... 201
Настройка задачи Активация программы с помощью Веб-плагина ..... 202
Настройка задач обновления с помощью Веб-плагина ..... 203
Настройка параметров диагностики сбоев с помощью Веб-плагина ..... 204
Работа с расписанием задач ..... 206

Настройка расписания задач ..... 206
Включение и выключение запуска задач по расписанию ..... 207
Отчеты в Kaspersky Security Center ..... 208
Диагностическое окно ..... 211
О диагностическом окне ..... 211
Просмотр состояния Kaspersky Embedded Systems Security для Windows с помощью диагностического окна ..... 212
Просмотр статистики событий безопасности ..... 213
Просмотр текущей активности программы ..... 214
Настройка записи файлов дампов и файлов трассировки ..... 215
Обновление баз и модулей Kaspersky Embedded Systems Security для Windows ..... 216
О задачах обновления ..... 216
Об обновлении модулей программы ..... 217
Об обновлении баз программы ..... 218
Схемы обновления баз и модулей антивирусных программ в организации ..... 219
Настройка задач обновления ..... 223
Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security для Windows ..... 223
Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы ..... 226
Настройка параметров задачи Копирование обновлений ..... 227
Настройка параметров задачи Обновление модулей программы ..... 228
Откат обновления баз Kaspersky Embedded Systems Security для Windows ..... 229
Откат обновления программных модулей ..... 230
Статистика задач обновления ..... 230
Изолирование и резервное копирование объектов ..... 232
Изолирование возможно зараженных объектов. Карантин ..... 232
Об изолировании возможно зараженных объектов ..... 232
Просмотр объектов на карантине ..... 233
Сортировка объектов на карантине ..... 233
Фильтрация объектов на карантине ..... 234
Проверка объектов на карантине ..... 235
Восстановление содержимого карантина ..... 236
Помещение объектов на карантин ..... 238
Удаление объектов с карантина ..... 239
Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" ..... 239
Настройка параметров карантина ..... 241
Статистика карантина ..... 242
Резервное копирование объектов. Резервное хранилище ..... 243
О резервном копировании объектов перед лечением или удалением ..... 243
Просмотр объектов в резервном хранилище ..... 244
Сортировка файлов в резервном хранилище ..... 244

Фильтрация файлов в резервном хранилище ....244
Восстановление файлов из резервного хранилища ....245
Удаление файлов из резервного хранилища ....247
Настройка параметров резервного хранилища ....248
Статистика резервного хранилища ....249
Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы ....250
Список заблокированных сетевых сеансов ....250
Управление списком заблокированных сетевых сеансов с помощью Плагина управления ....251
Включение блокировки недоверенных узлов ....251
Настройка параметров списка заблокированных сетевых сеансов ....252
Управление списком заблокированных сетевых сеансов с помощью Консоли программы ....253
Включение блокировки недоверенных узлов ....253
Настройка параметров списка заблокированных сетевых сеансов ....254
Управление списком заблокированных сетевых сеансов с помощью Веб-плагина ....255
Включение блокировки сетевых сеансов ....255
Настройка параметров списка заблокированных сетевых сеансов ....256
Запись событий. Журналы Kaspersky Embedded Systems Security для Windows ....257
Способы записи событий Kaspersky Embedded Systems Security для Windows ....257
Журнал системного аудита ....258
Сортировка событий в журнале системного аудита ....259
Фильтрация событий в журнале системного аудита ....259
Удаление событий из журнала системного аудита ....260
Журналы выполнения задач ....260
О журналах выполнения задач ....261
Просмотр списка событий в журналах выполнения задач ....261
Сортировка журналов выполнения задач ....261
Фильтрация журналов выполнения задач ....262
Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач ....263
Экспорт информации из журнала выполнения задачи ....264
Удаление журналов выполнения задач ....264
Журнал безопасности ....265
Просмотр журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий" ....265
Настройка параметров журнала с помощью Консоли программы ....266
Об интеграции с SIEM ....269
Настройка параметров интеграции с SIEM ....270
Настройка параметров журналов и уведомлений с помощью Плагина управления ....272
Настройка параметров журналов задач ....273
Журнал безопасности ....274
Настройка параметров интеграции с SIEM ....274

Настройка параметров уведомлений ....278
Настройка обмена информацией с Сервером администрирования ....279
Настройка уведомлений ....280
Способы уведомления администратора и пользователей ....280
Настройка уведомлений администратора и пользователей ....281
Запуск и остановка Kaspersky Embedded Systems Security для Windows ....284
Запуск Плагина управления Kaspersky Embedded Systems Security для Windows ....284
Запуск Консоли Kaspersky Embedded Systems Security для Windows из меню Пуск ....284
Запуск и остановка службы Kaspersky Security ....285
Запуск компонентов Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы ....286
О работе Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы ....286
Запуск Kaspersky Embedded Systems Security для Windows в безопасном режиме ....287
Механизмы самозащиты Kaspersky Embedded Systems Security для Windows ....289
О механизмах самозащиты Kaspersky Embedded Systems Security для Windows ....289
Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security для Windows ....289
Защита от изменений ключей реестра Kaspersky Embedded Systems Security для Windows ....290
Регистрация службы Kaspersky Security как защищенной службы ....291
Управление правами доступа к функциям Kaspersky Embedded Systems Security для Windows ....291
О правах на управление Kaspersky Embedded Systems Security для Windows ....292
О правах на управление регистрируемыми службами ....294
О правах доступа к службе Kaspersky Security Management ....295
О правах на управление службой Kaspersky Security ....295
Управление правами доступа с помощью Плагина управления ....297
Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security ....297
Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ....300
Управление правами доступа с помощью Консоли программы ....302
Настройка прав доступа на управление Kaspersky Embedded Systems Security для Windows и службой Kaspersky Security ....302
Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ....304
Управление правами доступа с помощью Веб-плагина ....306
Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security ....306
Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ....307
Постоянная защита файлов ....309
О задаче Постоянная защита файлов ....309
Об области защиты и параметрах безопасности задачи ....310

О виртуальной области защиты ....311
Стандартные области защиты ....311
Стандартные уровни безопасности ....312
Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов ....315
Параметры задачи Постоянная защита файлов по умолчанию ....317
Управление задачей Постоянная защита файлов с помощью Плагина управления ....319
Навигация ....319
Переход к параметрам политики для задачи Постоянная защита файлов ....319
Переход к параметрам задачи Постоянная защита файлов ....320
Настройка задачи Постоянная защита файлов ....320
Выбор режима защиты ....321
Настройка эвристического анализатора и интеграции с другими компонентами программы ....322
Настройка расписания задач ....324
Создание и настройка области защиты задачи ....326
Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ....327
Настройка параметров безопасности вручную ....327
Настройка общих параметров задачи ....328
Настройка действий ....331
Настройка производительности ....333
Управление задачей Постоянная защита файлов с помощью Консоли программы ....335
Навигация ....336
Переход к параметрам задачи Постоянная защита файлов ....336
Переход к параметрам области действия задачи Постоянная защита файлов ....336
Настройка задачи Постоянная защита файлов ....336
Выбор режима защиты объектов ....337
Настройка эвристического анализатора и интеграции с другими компонентами программы ....338
Настройка параметров расписания задач ....340
Формирование области защиты ....342
Настройка отображения сетевых файловых ресурсов ....342
Формирование области защиты ....342
Включение сетевых объектов в область защиты ....344
Формирование виртуальной области защиты ....345
Настройка параметров безопасности вручную ....346
Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ....347
Настройка общих параметров задачи ....347
Настройка действий ....350
Настройка производительности ....353
Статистика задачи Постоянная защита файлов ....354
Управление задачей Постоянная защита файлов с помощью Веб-плагина ....356
Настройка задачи Постоянная защита файлов ....356

Настройка области защиты для задачи ..... 360
Использование KSN ..... 367
О задаче Использование KSN ..... 367
Параметры по умолчанию для задачи Использование KSN ..... 369
Управление использованием KSN с помощью Плагина управления ..... 370
Настройка задачи Использование KSN с помощью Плагина управления ..... 370
Настройка обработки данных с помощью Плагина управления ..... 372
Управление использованием KSN с помощью Консоли программы ..... 373
Настройка задачи Использование KSN с помощью Консоли программы ..... 374
Настройка обработки данных с помощью Консоли программы ..... 375
Управление использованием KSN с помощью Веб-плагина ..... 376
Настройка передачи дополнительных данных ..... 379
Статистика задачи Использование KSN ..... 380
Защита от сетевых угроз ..... 382
О задаче Защита от сетевых угроз ..... 382
Параметры по умолчанию для задачи Защита от сетевых угроз ..... 383
Настройка задачи Защита от сетевых угроз с помощью Консоли программы ..... 383
Общие параметры задачи ..... 383
Добавление исключений ..... 384
Настройка задачи Защита от сетевых угроз с помощью Плагина управления ..... 384
Общие параметры задачи ..... 385
Добавление исключений ..... 385
Настройка задачи Защита от сетевых угроз с помощью Веб-плагина ..... 386
Общие параметры задачи ..... 386
Добавление исключений ..... 387
Контроль запуска программ ..... 388
О задаче Контроль запуска программ ..... 388
О правилах контроля запуска программ ..... 390
О Контроле пакетов установки ..... 392
Об использовании KSN в задаче Контроль запуска программ ..... 394
О формировании правил контроля запуска программ ..... 395
Параметры по умолчанию для задачи Контроль запуска программ ..... 397
Управление контролем запуска программ с помощью Плагина управления ..... 401
Навигация ..... 401
Переход к параметрам политики для задачи Контроль запуска программ ..... 401
Переход к списку правил контроля запуска программ ..... 402
Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам ..... 402
Настройка параметров задачи Контроль запуска программ ..... 403
Настройка Контроля пакетов установки ..... 406

Настройка задачи Формирование правил контроля запуска программ ....409
Настройка правил контроля запуска программ в Kaspersky Security Center ....411
Добавление правила контроля запуска программ ....412
Включение режима разрешения по умолчанию ....415
Формирование разрешающих правил контроля запуска программ на основе событий Kaspersky Security Center ....416
Импорт правил из отчета Kaspersky Security Center о заблокированных программах ....417
Импорт правил контроля запуска программ из XML-файла ....418
Проверка запуска программ ....420
Создание задачи Формирование правил контроля запуска программ ....421
Ограничение области действия задачи ....422
Действия при автоматическом формировании правил ....423
Действия по завершении автоматического формирования правил ....424
Управление контролем запуска программ с помощью Консоли программы ....425
Навигация ....426
Переход к параметрам задачи Контроль запуска программ ....426
Переход к окну с правилами контроля запуска программ ....426
Переход к параметрам задачи Формирование правил контроля запуска программ ....426
Настройка параметров задачи Контроль запуска программ ....427
Выбор режима работы задачи Контроль запуска программ ....428
Настройка области действия задачи Контроль запуска программ ....429
Настройка использования KSN ....430
Контроль пакетов установки ....432
Настройка правил контроля запуска программ ....434
Добавление правила контроля запуска программ ....435
Включение режима разрешения по умолчанию ....438
Формирование разрешающих правил по событиям задачи Контроль запуска программ ....439
Экспорт правил контроля запуска программ ....439
Импорт правил контроля запуска программ из XML-файла ....440
Удаление правил контроля запуска программ ....440
Настройка задачи Формирование правил контроля запуска программ ....441
Ограничение области действия задачи ....442
Действия при автоматическом формировании правил ....442
Действия по завершении автоматического формирования правил ....445
Управление контролем запуска программ с помощью Веб-плагина ....446
Контроль устройств ....451
О задаче Контроль устройств ....451
О правилах контроля устройств ....453
О формировании правил контроля устройств ....455
О задаче Формирование правил контроля устройств ....457

Параметры по умолчанию для задачи Контроль устройств ....457
Управление контролем устройств с помощью Плагина управления ....458
Навигация ....459
Переход к параметрам политики для задачи Контроль устройств ....459
Переход к списку правил контроля устройств ....459
Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам ....460
Настройка задачи Контроль устройств ....461
Настройка задачи Формирование правил контроля устройств ....462
Настройка правил контроля устройств в Kaspersky Security Center ....463
Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center ....463
Формирование правил для подключенных устройств ....464
Формирование правил на основе реестра Kaspersky Security Center ....464
Просмотр свойств правил Контроля устройств ....464
Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах ....466
Создание правил с помощью задачи Формирование правил контроля устройств ....468
Добавление сформированных правил в список правил контроля устройств ....470
Управление Контролем устройств с помощью Консоли программы ....471
Навигация ....471
Переход к параметрам задачи Контроль устройств ....471
Переход к окну с правилами контроля устройств ....472
Переход к параметрам задачи Формирование правил контроля устройств ....472
Настройка параметров задачи Контроль устройств ....472
Настройка правил контроля устройств ....474
Импорт правил контроля устройств из файла формата XML ....474
Формирование списка правил по событиям задачи Контроль устройств ....475
Добавление разрешающего правила для одного или нескольких внешних устройств ....475
Удаление правил контроля устройств ....476
Экспорт правил контроля устройств ....476
Активация и выключение правила контроля устройств ....477
Расширение области применения правил контроля устройств ....477
Настройка задачи Формирование правил контроля устройств ....478
Управление Контролем устройств с помощью Веб-плагина Консоли программы ....480
Управление сетевым экраном ....482
О задаче Управление сетевым экраном ....482
О правилах сетевого экрана ....484
Параметры по умолчанию для задачи Управление сетевым экраном ....485
Настройка задачи Управление сетевым экраном с помощью Плагина управления ....486
Настройка общих параметров задачи Управление сетевым экраном ....486
Создание и настройка правил сетевого экрана ....489

Включение и выключение правил сетевого экрана ....491
Удаление правил сетевого экрана ....492
Настройка задачи Управление сетевым экраном с помощью Консоли программы ....493
Настройка общих параметров задачи Управление сетевым экраном ....493
Создание и настройка правил сетевого экрана ....496
Включение и выключение правил сетевого экрана ....497
Удаление правил сетевого экрана ....498
Настройка задачи Управление сетевым экраном с помощью Веб-плагина ....499
Настройка общих параметров задачи Управление сетевым экраном ....499
Создание и настройка правил сетевого экрана ....502
Включение и выключение правил сетевого экрана ....503
Удаление правил сетевого экрана ....503
Мониторинг файловых операций ....505
О задаче Мониторинг файловых операций ....505
О правилах мониторинга файловых операций ....506
Параметры по умолчанию для задачи Мониторинг файловых операций ....509
Управление мониторингом файловых операций с помощью Плагина управления ....510
Настройка парметров задачи Мониторинг файловых операций ....510
Создание и настройка правила мониторинга файловых операций ....512
Экспорт и импорт правил мониторинга файловых операций ....515
Управление мониторингом файловых операций с помощью Консоли программы ....516
Настройка параметров задачи Мониторинг файловых операций ....516
Создание и настройка правила мониторинга файловых операций ....517
Экспорт и импорт правил мониторинга файловых операций ....519
Управление мониторингом файловых операций с помощью Веб-плагина ....520
Настройка параметров задачи Мониторинг файловых операций ....520
Создание и настройка правила мониторинга файловых операций ....521
Экспорт и импорт правил мониторинга файловых операций ....524
AMSI-защита ....525
О задаче AMSI-защита ....525
Параметры задачи AMSI-защита, установленные по умолчанию ....526
Настройка параметров задачи AMSI-защита с помощью Плагина управления ....526
Настройка параметров задачи AMSI-защита с помощью Консоли программы ....527
Настройка параметров задачи AMSI-защита с помощью Веб-плагина ....529
Статистика задачи AMSI-защита ....530
Мониторинг доступа к реестру ....531
О задаче Мониторинг доступа к реестру ....531
О правилах мониторинга доступа к реестру ....531
Параметры по умолчанию для задачи Мониторинг доступа к реестру ....534
Управление мониторингом доступа к реестру с помощью Плагина управления ....535

Настройка параметров задачи Мониторинг доступа к реестру ....535
Создание и настройка правила мониторинга доступа к реестру ....536
Экспорт и импорт правил мониторинга доступа к реестру ....537
Управление мониторингом доступа к реестру с помощью Консоли программы ....538
Настройка общих параметров задачи Мониторинг доступа к реестру ....538
Создание и настройка правила мониторинга доступа к реестру ....539
Экспорт и импорт правил мониторинга доступа к реестру ....540
Управление мониторингом доступа к реестру с помощью Веб-плагина ....541
Настройка параметров задачи Мониторинг доступа к реестру ....541
Создание и настройка правила мониторинга доступа к реестру ....542
Экспорт и импорт правил мониторинга доступа к реестру ....543
Анализ журналов ....544
О задаче Анализ журналов ....544
Параметры по умолчанию для задачи Анализ журналов ....546
Управление правилами анализа журналов с помощью Плагина управления ....547
Управление стандартными правилами задачи с помощью Плагина управления ....547
Добавление правил анализа журналов с помощью Плагина управления ....549
Управление правилами анализа журналов с помощью Консоли программы ....550
Управление стандартными правилами задачи с помощью Консоли программы ....550
Добавление правил анализа журналов с помощью Консоли программы ....552
Управление правилами анализа журналов с помощью Веб-плагина ....553
Проверка по требованию ....555
О задачах проверки по требованию ....555
Об области проверки и параметрах безопасности задачи ....556
Стандартные области проверки ....558
Проверка файлов в интернет-хранилище ....559
Стандартные уровни безопасности ....561
Проверка съемных дисков ....563
О задаче Мониторинг целостности файлов на основе эталона ....564
Включение запуска задачи проверки по требованию из контекстного меню ....566
Заданные по умолчанию параметры задач проверки по требованию ....567
Управление задачами проверки по требованию с помощью Плагина управления ....570
Навигация ....570
Переход к мастеру создания задачи проверки по требованию ....570
Переход к свойствам задачи проверки по требованию ....571
Создание задачи проверки по требованию ....572
Присвоение задаче проверки по требованию статуса Проверка важных областей ....575
Выполнение задач проверки по требованию в фоновом режиме ....576
Регистрация выполнения задачи Проверка важных областей ....576
Настройка области проверки для задачи ....577

Выбор стандартных уровней безопасности в задачах проверки по требованию ....578
Настройка параметров безопасности вручную ....579
Настройка общих параметров задачи ....580
Настройка действий ....583
Настройка производительности ....585
Настройка проверки съемных дисков ....586
Настройка задачи Мониторинг целостности файлов на основе эталона ....587
Управление задачами проверки по требованию с помощью Консоли программы ....588
Навигация ....589
Переход к параметрам задачи проверки по требованию ....589
Переход к параметрам области действия задачи проверки по требованию ....589
Создание и настройка задачи проверки по требованию ....589
Область проверки в задачах проверки по требованию ....592
Настройка отображения сетевых файловых ресурсов ....592
Формирование области проверки ....592
Включение в область проверки сетевых объектов ....594
Создание виртуальной области проверки ....595
Настройка параметров безопасности ....596
Выбор стандартных уровней безопасности в задачах проверки по требованию ....597
Настройка общих параметров задачи ....598
Настройка действий ....600
Настройка производительности ....602
Настройка иерархического хранилища ....604
Проверка съемных дисков ....605
Статистика задач проверки по требованию ....605
Создание и настройка задачи Мониторинг целостности файлов на основе эталона ....607
Управление задачами проверки по требованию с помощью Веб-плагина ....608
Переход к мастеру создания задачи проверки по требованию ....608
Переход к свойствам задачи проверки по требованию ....610
Настройка области проверки для задачи ....610
Настройка параметров задачи ....616
Доверенная зона ....619
О доверенной зоне ....619
Управление доверенной зоной с помощью Плагина управления ....620
Навигация ....620
Переход к параметрам политики для доверенной зоны ....621
Переход к окну параметров доверенной зоны ....621
Настройка параметров доверенной зоны с помощью Плагина управления ....622
Добавление исключений ....622
Добавление доверенных процессов с помощью Плагина управления ....624

Использование маски not-a-virus ..... 627
Управление доверенной зоной с помощью Консоли программы ..... 627
Использование доверенной зоны для задач в Консоли программы ..... 627
Настройка параметров доверенной зоны в Консоли программы ..... 628
Добавление исключений в доверенную зону ..... 629
Добавление доверенных процессов с помощью Консоли программы ..... 631
Использование маски not-a-virus ..... 634
Управление доверенной зоной с помощью Веб-плагина ..... 635
Защита от эксплойтов ..... 636
О защите от эксплойтов ..... 636
Управление защитой от эксплойтов с помощью Плагина управления ..... 638
Навигация ..... 638
Переход к параметрам политики для защиты от эксплойтов ..... 638
Переход к окну параметров защиты от эксплойтов ..... 639
Настройка защиты памяти процессов ..... 639
Добавление процесса в область защиты ..... 641
Управление защитой от эксплойтов с помощью Консоли программы ..... 642
Навигация ..... 642
Переход к основным параметрам защиты от эксплойтов ..... 642
Переход к параметрам защиты процессов при защите от эксплойтов ..... 643
Настройка защиты памяти процессов ..... 643
Добавление процесса в область защиты ..... 644
Управление защитой от эксплойтов с помощью Веб-плагина ..... 646
Настройка защиты памяти процессов ..... 646
Добавление процесса в область защиты ..... 647
Техники защиты от эксплойтов ..... 648
Интеграция со сторонними системами ..... 650
Счетчики производительности для программы Системный монитор ..... 650
О счетчиках производительности Kaspersky Embedded Systems Security для Windows ..... 651
Общее количество отвергнутых запросов ..... 651
Общее количество пропущенных запросов ..... 652
Количество запросов, не обработанных из-за нехватки системных ресурсов ..... 653
Количество запросов, отправленных на обработку ..... 654
Среднее количество потоков диспетчера файловых перехватов ..... 654
Максимальное количество потоков диспетчера файловых перехватов ..... 655
Количество элементов в очереди зараженных объектов ..... 656
Количество объектов, обрабатываемых за секунду ..... 657
SNMP-счетчики и ловушки в Kaspersky Embedded Systems Security для Windows ..... 658
О SNMP-счетчиках и ловушках Kaspersky Embedded Systems Security для Windows ..... 658
SNMP-счетчики Kaspersky Embedded Systems Security для Windows ..... 658

Счетчики производительности ....659
Счетчики карантина ....659
Счетчик резервного хранилища ....659
Общие счетчики ....660
Счетчик обновлений ....660
Счетчики постоянной защиты файлов ....660
SNMP-ловушки Kaspersky Embedded Systems Security для Windows и их параметры ....662
Описания и возможные значения параметров SNMP-ловушек Kaspersky Embedded Systems Security для Windows ....666
Интеграция с WMI ....668
Работа с Kaspersky Embedded Systems Security для Windows из командной строки ....672
Команды ....672
Вызов справки о командах Kaspersky Embedded Systems Security для Windows. KAVSHELL HELP ....675
Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP ....675
Проверка указанной области: KAVSHELL SCAN ....676
Запуск задачи Проверка важных областей: KAVSHELL SCANCRITICAL ....680
Управление задачей в асинхронном режиме: KAVSHELL TASK ....681
Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG ....683
Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP ....683
Управление задачей Контроль запуска программ: KAVSHELL APPCONTROL /CONFIG ....684
Формирование правил контроля запуска программ: KAVSHELL APPCONTROL /GENERATE ....685
Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL ....687
Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL ....688
Запуск задачи Обновление баз программы: KAVSHELL UPDATE ....689
Откат обновления баз Kaspersky Embedded Systems Security для Windows: KAVSHELL ROLLBACK ....692
Управление анализом журналов: KAVSHELL TASK LOG-INSPECTOR ....693
Активация программы. KAVSHELL LICENSE ....693
Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE ....694
Дефрагментация файлов журнала Kaspersky Embedded Systems Security для Windows. KAVSHELL VACUUM ....697
Очищение базы iSwift. KAVSHELL FBRESET ....698
Включение и выключение создания файла дампа. KAVSHELL DUMP ....698
Импорт параметров. KAVSHELL IMPORT ....699
Экспорт параметров. KAVSHELL EXPORT ....700
Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO ....701
Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE ....701
Коды возврата команд ....704
Коды возврата команд KAVSHELL START и KAVSHELL STOP ....704
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL ....705

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR ..... 705
Коды возврата команды KAVSHELL TASK ..... 706
Коды возврата команды KAVSHELL RTP ..... 706
Коды возврата команды KAVSHELL UPDATE ..... 707
Коды возврата команды KAVSHELL ROLLBACK ..... 707
Коды возврата команды KAVSHELL LICENSE ..... 708
Коды возврата команды KAVSHELL TRACE ..... 708
Коды возврата команды KAVSHELL FBRESET ..... 709
Коды возврата команды KAVSHELL DUMP ..... 709
Коды возврата команды KAVSHELL IMPORT ..... 709
Коды возврата команды KAVSHELL EXPORT ..... 710
Коды возврата команды KAVSHELL FIM /BASELINE ..... 710
Обращение в Службу технической поддержки ..... 712
Способы получения технической поддержки ..... 712
Техническая поддержка через Kaspersky CompanyAccount ..... 712
Использование файла трассировки и скрипта AVZ ..... 713
Глоссарий ..... 714
Информация о стороннем коде ..... 718
Уведомления о товарных знаках ..... 719

# О Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows защищает компьютеры и другие встроенные системы под управлением операционной системы Microsoft® Windows® (защищаемые устройства) от вирусов и прочих угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security для Windows являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Kaspersky Embedded Systems Security для Windows можно установить на различные встроенные системы под управлением Windows, включая устройства следующих типов:

- Банкоматы.
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security для Windows следующими способами:

- С помощью Консоли программы, установленной на одном защищаемом устройстве с Kaspersky Embedded Systems Security для Windows или на другом устройстве.
- С помощью команд командной строки.
- С помощью Консоли администрирования Kaspersky Security Center.

Вы можете использовать программу Kaspersky Security Center для централизованного управления защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security для Windows.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security для Windows для программы Системный монитор, а также счетчики и ловушки SNMP.

### Компоненты и функции Kaspersky Embedded Systems Security для Windows

В состав программы входят следующие компоненты:

- **Постоянная защита файлов**. Kaspersky Embedded Systems Security для Windows проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security для Windows проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - Основные загрузочные записи и загрузочные секторы локальных жестких и съемных дисков.
- **Проверка по требованию**. Kaspersky Embedded Systems Security для Windows однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память и объекты автозапуска на защищаемом устройстве.
- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ на защищаемом устройстве.
- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование внешних устройств с целью защиты устройства от угроз компьютерной безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешними устройствами других типов.

- **Управление сетевым экраном**. Этот компонент обеспечивает возможность управления брандмауэром Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует возможность настройки параметров сетевого экрана извне.
- **Мониторинг файловых операций**. Kaspersky Embedded Systems Security для Windows обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения указывают на нарушение безопасности на защищаемом устройстве.
- **Анализ журналов**. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

В программе реализованы следующие функции:

- **Обновление баз программы** и **Обновление модулей программы**. Kaspersky Embedded Systems Security для Windows загружает обновления баз и модулей программы с FTP- или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.
- **Карантин** Kaspersky Embedded Systems Security для Windows перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.
- **Резервное хранилище**. Kaspersky Embedded Systems Security для Windows сохраняет зашифрованные копии объектов со статусом *Зараженный* в папке *Резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.
- **Уведомления администратора и пользователей**. Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому устройству, о событиях, связанных с работой Kaspersky Embedded Systems Security для Windows и состоянии антивирусной защиты устройства.
- **Импорт и экспорт параметров**. Вы можете экспортировать параметры Kaspersky Embedded Systems Security для Windows в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security для Windows из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.
- **Применение шаблонов**. Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security для Windows.
- **Управление правами доступа к функциям Kaspersky Embedded Systems Security для Windows**. Вы можете настраивать права на управление Kaspersky Embedded Systems Security для Windows и службами Windows, которые регистрирует программа, для пользователей и групп пользователей.
- **Запись событий в журнал событий Windows**. Kaspersky Embedded Systems Security для Windows записывает в журнал событий информацию о параметрах функциональных компонентов программы, текущем состоянии задач, событиях, возникших за время их выполнения, а также о событиях, связанных с управлением Kaspersky Embedded Systems Security для Windows, и информацию, необходимую для диагностики сбоев в работе программы.
- **Доверенная зона**. Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Embedded Systems Security для Windows будет применять в задачах проверки по требованию и постоянной защиты компьютера.
- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

# Что нового

В новой версии Kaspersky Embedded Systems Security для Windows появились следующие возможности и улучшения:

- В задаче Защита от сетевых угроз добавлена функциональность защиты от атак MAC-спуфинга.
- В задаче Управление сетевым экраном добавлена возможность выбора режима взаимодействия с брандмауэром Windows - Отслеживать статус работы брандмауэра Windows или Контролировать работу брандмауэра Windows.
- Для задачи Мониторинг файловых операций добавлена возможность экспорта правил во внешний файл и импорта правил из внешнего файла.
- Для задачи Мониторинг доступа к реестру добавлена возможность экспорта правил во внешний файл и импорта правил из внешнего файла.
- Правила доверенных процессов теперь можно применять к задаче Контроль запуска программ. Задачи Мониторинг доступа к реестру и Мониторинг файловых операций всегда применяют параметры доверенной зоны. Параметры применимости правил доверенных процессов в задачах Мониторинг файловых операций и Мониторинг доступа к реестру более недоступны. Параметры применимости правил доверенных процессов теперь размещены в параметрах доверенной зоны.
- В задаче Контроль запуска программ при создании правил на основе событий журнала Kaspersky Security Center добавлен фильтр по имени групп устройств.
- В Kaspersky Security Center Web Console в параметрах правил задачи Контроль запуска программ стало возможным добавление разрешающих правил на основе событий журнала Kaspersky Security Center.
- В плагине управления программой через Kaspersky Security Center в параметрах правил и задач Контроль запуска программ, Контроль устройств, Мониторинг файловых операций и Мониторинг доступа к реестру расширен список источников информации о пользователях. Теперь администратор может указывать пользователей не только из списков Active Directory, но также выбирать пользователей из списков учетных записей Kaspersky Security Center или указать имя пользователя или группы пользователей вручную.
- События обнаружения угроз в режиме "Только уведомлять об обнаруженных атаках" для задачи Защита от сетевых угроз теперь публикуются с уровнем важности "Предупреждение" вместо "Критический".
- Оптимизировано количество событий задач Мониторинг доступа к реестру и Мониторинг файловых операций. Повторные события не отправляются в Kaspersky Security Center, а отправляются только в журналы выполнения задач.
- Реализована поддержка новых операционных систем: Windows 11 23H2, Windows 11 23H2 IoT.
- Программа уведомляет пользователя в случае завершения периода поддержки установленной версии программы.
- Плагин управления программой через Kaspersky Security Center больше не поддерживает создание политики с помощью экспорта свойств политики из KLP-файла. Но это по-прежнему можно сделать с помощью мастера создания политики в консоли администрирования Kaspersky Security Center.
- Исправлены ошибки предыдущих версий: данная версия программы включает исправления ошибок из более ранних версий.

# Источники информации о Kaspersky Embedded Systems Security для Windows

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

## В этом разделе


Источники для самостоятельного поиска информации ..... 23

Обсуждение программ "Лаборатории Касперского" на форуме ..... 24


## Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Embedded Systems Security для Windows:

- страница Kaspersky Embedded Systems Security для Windows на веб-сайте "Лаборатории Касперского";
- страница программы на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/.

Для использования источников информации на веб-сайтах требуется подключение к интернету.

**Страница Kaspersky Embedded Systems Security для Windows на веб-сайте "Лаборатории Касперского"**

На странице Kaspersky Embedded Systems Security для Windows http://www.kaspersky.ru/enterprise-security/embedded-systems можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Страница Kaspersky Embedded Systems Security для Windows содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

### Страница Kaspersky Embedded Systems Security для Windows в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Embedded Systems Security для Windows в Базе знаний https://support.kaspersky.ru/kess приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний содержат информацию, относящуюся не только к Kaspersky Embedded Systems Security для Windows, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

### Документация Kaspersky Embedded Systems Security для Windows

В Руководстве администратора Kaspersky Embedded Systems Security для Windows вы можете найти информацию об установке, удалении, настройке и использовании программы.

## Обсуждение программ "Лаборатории Касперского" на форуме

Вы можете обсудить вопросы, связанные с программами "Лаборатории Касперского", с другими пользователями и специалистами "Лаборатории Касперского" на нашем форуме https://community.kaspersky.com/.

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

# Kaspersky Embedded Systems Security для Windows

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security для Windows, перечень аппаратных и программных требований Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Комплект поставки ..... 25

Программные и аппаратные требования ..... 28

Функциональные требования и ограничения ..... 33


## Комплект поставки

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

- запустить мастер установки Kaspersky Embedded Systems Security для Windows;
- запустить мастер установки Консоли Kaspersky Embedded Systems Security для Windows;
- запустить мастер установки Плагина управления Kaspersky Embedded Systems Security для Windows, который позволяет управлять программой через Kaspersky Security Center;
- перейти на страницу Kaspersky Embedded Systems Security для Windows на веб-сайте "Лаборатории Касперского";
- перейти на веб-сайт Службы технической поддержки https://support.kaspersky.ru/;
- прочитать информацию о текущем выпуске Kaspersky Embedded Systems Security для Windows.

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

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

*Таблица 1. Файлы комплекта поставки Kaspersky Embedded Systems Security для Windows*

| Файл | Назначение |
|---|---|
| autorun.inf | Файл автозапуска мастера установки Kaspersky Embedded Systems Security для Windows при установке программы со съемных дисков. |
| release_notes.txt | Файл содержит информацию о версии. |
| migration.txt | Файл с описанием обновления с предыдущих версий программы. |
| setupui.exe | Файл запуска программы приветствия (запускает setup.hta). |

| Файл | Назначение |
|---|---|
| ess.kud | Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки программы через Kaspersky Security Center. |
| \console\esstools.msi | Пакет установщика Windows. Устанавливает Консоль программы на управляемое устройство. |
| \console\setup.exe | Файл запуска мастера установки для набора компонентов Средства администрирования (в него входит Консоль Kaspersky Embedded Systems Security для Windows). Запускается файл инсталляционного пакета esstools.msi с указанными в мастере параметрами установки. |
| \exec\bases.cab | Архив антивирусных баз, актуальных на момент выпуска программы. |
| \exec\config.ini | Конфигурационный файл, содержащий параметры установки для создания пакета установки Kaspersky Embedded Systems Security для Windows в Kaspersky Security Center. |
| \exec\ess.kud | Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center. |
| \exec\ess_x64.msi | Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security для Windows на управляемое устройство с 64-битной операционной системой. |
| \exec\ess_x86.msi | Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security для Windows на управляемое устройство с 32-битной операционной системой. |
| \exec\klcfginst.exe | Программа установки Плагина управления программой через Kaspersky Security Center. |
| \exec\license.txt | Файл с текстом Лицензионного соглашения и Политики конфиденциальности. |
| \exec\setup.exe | Файл для установки Kaspersky Embedded Systems Security для Windows на защищаемом устройстве с помощью мастера установки; запускает файл пакета установки ess.msi с указанными в мастере параметрами. |
| \product_long_term\config.ini | Конфигурационный файл, содержащий параметры установки для создания пакета установки Kaspersky Embedded Systems Security для Windows в Kaspersky Security Center. |
| \product_long_term\ess_light.kud | Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center. |
| \product_long_term\ess_x86.msi | Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security для Windows в конфигурации Защита компьютера с помощью технологии "запрет по умолчанию" на защищаемое устройство с 32-разрядной операционной системой. |
| \product_long_term\license.txt | Файл с текстом Лицензионного соглашения и Политики конфиденциальности. |

| Файл | Назначение |
| --- | --- |
| \product_long_term\setup.exe | Файл для установки Kaspersky Embedded Systems Security для Windows на защищаемом устройстве с помощью мастера установки; запускает файл пакета установки ess.msi с указанными в мастере параметрами. |
| \setup\images | Папка с файлами для запуска приветственного экрана программы. |
| \setup\setup.hta | Файл запуска программы-приветствия. |
| \setup\SETUP_STRINGS.JS | Файл со строковыми ресурсами программы. |

# Программные и аппаратные требования

Перед установкой Kaspersky Embedded Systems Security для Windows необходимо удалить с устройства другие антивирусные программы.

**Программные требования к защищаемым устройствам**

Вы можете установить Kaspersky Embedded Systems Security для Windows на компьютере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

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

Для установки и работы Kaspersky Embedded Systems Security для Windows на защищаемых устройствах со встроенными операционными системами необходим компонент Диспетчер фильтров (Filter Manager).
Для корректной работы Kaspersky Embedded Systems Security для Windows в Windows требуется поддержка SHA-2. Подробная информация приведена в статье https://support.kaspersky.ru/15728.

Вы можете установить Kaspersky Embedded Systems Security для Windows на устройство под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows (полный перечень поддерживаемых операционных систем можно уточнить в технической поддержке):

- Рабочие станции:
  - Windows XP Pro SP2.
  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11

- Встраиваемые системы:
  - Windows XP Embedded - -
  - Windows 7
  - Windows 8.0 - - .
  - Windows 8.1 - - .
  - Windows 10 - - .
  - Windows 11 - - .

- .

**Аппаратные требования к защищаемым устройствам**

*Таблица 1. Аппаратные требования к защищаемым устройствам*

| Тип ОС | Наименование ОС | Минимальные требования | Рекомендованные требования |
|---|---|---|---|
| Для рабочих станций | Windows XP x86 / x64 | • Процессор: 1.4 ГГц одноядерный Pentium III (x32), Pentium IV (x64).<br>• Оперативная память:<br>  • Для установки только Контроля запуска программ – 256 МБ.<br>  • Для установки всех компонентов программы – 512 МБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 50 МБ.<br>  • Для установки всех компонентов программы – 2 ГБ. | • Процессор: 2.4 ГГц четырехядерный.<br>• Оперативная память: 2ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ. |
| | Windows 7 / 8 / 10 x86 | • Процессор: 1.4 ГГц одноядерный Pentium III (x32), Pentium IV (x64).<br>• Оперативная память:<br>  • Для установки только Контроля запуска программ – 256 МБ.<br>  • Для установки всех компонентов программы – 1 ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 50 МБ.<br>  • Для установки всех компонентов программы – 2 ГБ. | • Процессор: 2.4 ГГц четырехядерный.<br>• Оперативная память: 2ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ. |

| Тип ОС | Наименование ОС | Минимальные требования | Рекомендованные требования |
|---|---|---|---|
| | Windows 7 / 8 / 10 / 11 x64 | • Процессор: 1.4 ГГц одноядерный Pentium IV (x64).<br>• Оперативная память:<br>  • Для установки только Контроля запуска программ – 1 ГБ.<br>  • Для установки всех компонентов программы – 2 ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 50 МБ.<br>  • Для установки всех компонентов программы – 2 ГБ. | • Процессор: 2.4 ГГц четырехядерный.<br>• Оперативная память:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ. |
| Встраиваемые | Windows XP Embedded<br><br>Windows Embedded POSReady 2009 | • Процессор: 1.4 ГГц одноядерный Pentium III (x32), Pentium IV (x64).<br>• Оперативная память:<br>  • Для установки только Контроля запуска программ – 256 МБ.<br>  • Для установки всех компонентов программы – 512 МБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 50 МБ.<br>  • Для установки всех компонентов программы – 2 ГБ. | • Процессор: 2.4 ГГц четырехядерный.<br>• Оперативная память: 2ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ. |

| Тип ОС | Наименование ОС | Минимальные требования | Рекомендованные требования |
|---|---|---|---|
| | Windows 7 / 8 Embedded<br>Windows 10 / 11 IoT | • Процессор: 1.4 ГГц одноядерный Pentium IV (x64).<br>• Оперативная память: 1 ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 50 МБ.<br>  • Для установки всех компонентов программы – 2 ГБ. | • Процессор: 2.4 ГГц четырехядерный.<br>• Оперативная память: 2ГБ.<br>• Объем свободного места на диске:<br>  • Для установки только Контроля запуска программ – 2 ГБ.<br>  • Для установки всех компонентов программы – 4 ГБ. |

kaspersky

# Функциональные требования и ограничения

В этом разделе приведено описание дополнительных функциональных требований и существующих ограничений компонентов Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Установка и удаление ..... 33

Мониторинг файловых операций ..... 34

Управление сетевым экраном ..... 35

Прочие ограничения ..... 35


## Установка и удаление

Ниже приведен список ограничений при установке и удалении:

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

Если указанные корневые сертификаты не установлены, программа может работать некорректно.

## Мониторинг файловых операций

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

Следующие папки и файлы исключены из области мониторинга:

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

Программа исключает папки верхнего уровня.

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

## Управление сетевым экраном

Ниже приведен список ограничений при управлении сетевым экраном:

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

## Прочие ограничения

Ограничения задач **Проверка по требованию** и **Постоянная защита файлов**:

- Проверка подключенных устройств, работающих по протоколу MTP, не поддерживается.
- Проверка архивов невозможна без проверки SFX-архивов: если проверка архивов включена в параметрах защиты Kaspersky Embedded Systems Security для Windows, программа автоматически проверяет объекты как в архивах, так и в SFX-архивах. Возможна проверка SFX-архивов без проверки архивов.
- Если одновременно установлен флажок **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)** и включено **Использование KSN**, все запущенные процессы, получившие в качестве аргумента веб-адрес, будут заблокированы, даже если был выбран режим "Только статистика". Чтобы избежать блокировки процесса, выберите один из вариантов:
  - Отключите **Использование KSN**.
  - Снимите флажок **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)**.

  Рекомендуемый вариант: снимите флажок "Более глубокий анализ запускаемых процессов".

**Лицензирование**:

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

**Обновления**:

- После установки критических обновлений модулей Kaspersky Embedded Systems Security для Windows, по умолчанию значок программы будет скрыт.
- KLRAMDISK не поддерживается на защищаемых устройствах с операционными системами Windows XP и Windows Server® 2003.

**Интерфейс**:

- При использовании фильтров в Консоли программы учитывается регистр для карантина, резервного хранилища, журнала системного аудита и журналов выполнения задач.
- При настройке области защиты и области проверки в Консоли программы можно использовать только одну маску и только в конце пути. Примеры использования маски: "C:\Temp\Temp*", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc". Это ограничение не распространяется на настройку доверенной зоны.

**Безопасность**:

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

**Интеграция с Kaspersky Security Center**:

- При получении пакетов обновлений Сервер администрирования проверяет обновления баз перед отправкой обновлений на защищаемые сетевые устройства. Сервер администрирования не проверяет обновления модулей программы.
- Убедитесь, что установлены необходимые флажки в окне параметров взаимодействия с Сервером администрирования, при использовании компонентов, передающих динамические данные в Kaspersky Security Center с помощью сетевых списков (карантин, резервное хранилище).

**Защита от эксплойтов**:

- Защита от эксплойтов недоступна, если библиотеки apphelp.dll не загружены в текущей конфигурации сетевого окружения. Библиотека располагается в директории SystemRoot%\System32\apphelp.dll
- Компонент Защита от эксплойтов несовместим с утилитой EMET от Microsoft на защищаемых устройствах с операционной системой Microsoft Windows 10. Kaspersky Embedded Systems Security для Windows блокирует EMET, если компонент Защита от эксплойтов установлен на защищаемом устройстве с установленной утилитой EMET.
- Компонент Защита от эксплойтов несовместим с ядром базы данных SQL Server® 2012. Если Kaspersky Embedded Systems Security для Windows устанавливается на компьютер с MS SQL Server 2012, необходимо добавить библиотеку sqlos.dll сервера баз данных в список исключений в задаче Защита от эксплойтов.
- Наличие библиотеки apphelp.dll проверяется продуктом на этапе установки. В случае её отсутствия, установщик продукта отображает предупреждение. Загрузка библиотеки осуществляется операционной системой без участия продукта.  Если файл библиотеки присутствует в каталоге операционной системы, он будет загружен загрузчиком операционной системы.

kaspersky

# Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Об обновлении Kaspersky Embedded Systems Security для Windows ..... 37

Миграция значений параметров обновляемой версии программы ..... 38

Об обновлении средств администрирования Kaspersky Embedded Systems Security для Windows . 40

Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows ..... 41

Изменения в системе после установки Kaspersky Embedded Systems Security для Windows ..... 45

Процессы Kaspersky Embedded Systems Security для Windows ..... 48

Параметры установки и удаления и ключи командной строки для службы установщика Windows .. 49

Журналы установки и удаления Kaspersky Embedded Systems Security для Windows ..... 53

Планирование установки ..... 54

Установка и удаление программы с помощью мастера ..... 57

Установка и удаление программы из командной строки ..... 72

Установка и удаление программы с помощью Kaspersky Security Center ..... 79

Установка и удаление программы через групповые политики Active Directory ..... 84

Проверка функций Kaspersky Embedded Systems Security для Windows. Использование тестового вируса EICAR ..... 87


# Об обновлении Kaspersky Embedded Systems Security для Windows

Обновление до Kaspersky Embedded Systems Security для Windows версии 3.3 доступно для программы версии 2.1 и выше. Обновление выполняется путем установки новой версии программы поверх установленной версии программы и не требует перезагрузки компьютера.

По умолчанию программа создает новую папку установки с именем новой версии программы на основе пути к существующей папке установки программы. Вы можете вручную задать новый путь для папки установки программы.

В процессе обновления Kaspersky Embedded Systems Security для Windows до версии 3.3 установленная раннее версия программы автоматически удаляется.

Если у вас установлена Kaspersky Embedded Systems Security для Windows версии ниже 2.1, перед установкой новой версии программы необходимо сначала удалить установленную программу.

При обновлении Kaspersky Embedded Systems Security для Windows версии 2.1 и выше, защищенной паролем, необходимо передать установщику этот пароль.

При обновлении программы действующая лицензия автоматически применяется к Kaspersky Embedded Systems Security для Windows версии 3.3, и использование новых компонентов и задач программы доступно в полном объеме. Срок действия лицензии остается без изменений.

При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности (например, недоступно обновление баз программы).

# Миграция значений параметров обновляемой версии программы

Во время обновления программы остаются неизмененными:

- параметры программы и задач;
- журналы выполнения задач и системного аудита;
- содержимое карантина и резервного хранилища;
- учетные записи, с правами которых запускаются задачи;
- права на управление программой;
- параметры уведомлений о работе задач программы;
- служба KAVFS продолжает работать с признаком PPL, если этот признак был присвоен ей в предыдущей версии программы.

Во время обновления программы сбрасываются или изменяются до значений по умолчанию для новой версии программы:

- все счетчики, в том числе статусы состояния антивирусных баз;
- данные об установленных обновлениях программных модулей и антивирусных баз;
- статусы выполнения задач;
- параметры программы и задач, настроенные через реестр;
- параметры программы и задач, измененные в процессе установки критических исправлений.

### Миграция списка заблокированных сетевых сессий

Во время обновления программы не переносится список заблокированных сетевых сессий клиентских компьютеров.

Параметры автоматической разблокировки доступа к заблокированным сетевым файловым ресурсам остаются неизмененными во время обновления программы.

### Миграция значений параметров и правил Контроля запуска программ

Во время обновления программы правила контроля запуска программ переносятся без изменений.

Во время обновления программы рекомендуем остановить задачу Контроль запуска программ, если она выполняется в активном режиме, или изменить режим работы задачи на *Только статистика*.

После завершения обновления программы рекомендуем проверить перенесенные правила контроля запуска программ и их работу в режиме *Только статистика*.

### Миграция значений параметров и правил Управления сетевым экраном

Во время обновления программы правила задачи управления сетевым экраном переносятся без изменений.

Если компонент Управление сетевым экраном не был установлен в предыдущей версии программы, после обновления программы задача Управление сетевым экраном работает в режиме Отслеживать статус работы брандмауэра Windows.

Если компонент Управление сетевым экраном был установлен в предыдущей версии программы, после обновления программы задача Управление сетевым экраном работает в режиме Контролировать работу брандмауэра Windows.

### Обновление с изменением конфигурации программы

При установке программы в конфигурации "Защита компьютера с помощью антивирусных баз" (из папки /exec) поверх версии программы, в которой не используются сигнатурный анализ и антивирусные базы для защиты компьютера (конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию""), набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов:

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

Архив с антивирусными базами распаковывается автоматически.

Если вы не хотите использовать эти компоненты и задачи для защиты устройства, перезапустите установку программы из папки /product_long_term.

При установке программы в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию"" (из папки /product_long_term) поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера (конфигурация "Защита компьютера с помощью антивирусных баз"), набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

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

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

### Положение о Kaspersky Security Network и Kaspersky Managed Protection

Задача Использование KSN будет остановлена после обновления программы до версии 3.3. Чтобы продолжить использование KSN и службы KMP после обновления программы, необходимо прочитать и принять условия Положения о KSN и Положения о KMP.

# Об обновлении средств администрирования Kaspersky Embedded Systems Security для Windows

Обновление Консоли Kaspersky Embedded Systems Security для Windows до версии 3.3 доступно для Консоли программы любой версии.

При этом:

- Значения параметров обновленной Консоли программы остаются неизмененными.
- Консоль программы версии 3.3 может управлять Kaspersky Embedded Systems Security для Windows любой предыдущей версии.
- Консоль программы любой предыдущей версии может управлять Kaspersky Embedded Systems Security для Windows версии 3.3.

Обновление Плагина управления до версии 3.3 доступно для Плагина управления следующих версий:

- 2.1.0.xxx;
- 2.3.0.xxx;
- 3.0.0.xxx;
- 3.1.0.xxx;
- 3.2.0.xxx.

При этом:

- Значения параметров Плагина управления любой из перечисленных выше версий остаются неизмененными после обновления до версии 3.3.
- Плагин управления версии 3.3 может управлять Kaspersky Embedded Systems Security для Windows следующих версий: 2.1.0.441, 2.3.0.754, 3.0.0.102, 3.1.0.461, 3.2.0.200.
- Плагин управления любой из перечисленных выше версий может управлять Kaspersky Embedded Systems Security для Windows версии 3.3.

Обновление выполняется путем установки новой версии Плагина управления или Консоли программы поверх установленной версии и не требует перезагрузки компьютера.

# Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows

Файлы \product_long_term\ess_x86.msi и \product_long_term\ess_x64.msi предназначены для установки Kaspersky Embedded Systems Security для Windows в конфигурации Защита компьютера с помощью технологии "запрет по умолчанию", а файлы \product\ess_x86.msi и \product\ess_x64.msi предназначены для установки Kaspersky Embedded Systems Security для Windows в конфигурации Защита компьютера с помощью антивирусных баз.

Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию".

Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты:

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

При установке программы в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

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

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

Файлы \console\esstools_x86.msi и \console\esstools_x64.msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приведены коды компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Embedded Systems Security для Windows из командной строки.

kaspersky

## В этом разделе

Программные компоненты Kaspersky Embedded Systems Security для Windows ..... 42
Программный компонент "Средства администрирования" ..... 45

# Программные компоненты Kaspersky Embedded Systems Security для Windows

В следующей таблице приведены коды и описания программных компонентов Kaspersky Embedded Systems Security для Windows.

*Таблица 2. Описание программных компонентов Kaspersky Embedded Systems Security для Windows*

| Компонент | Идентификатор | Функции компонента |
|---|---|---|
| Основная функциональность | Core | Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.<br>Если, устанавливая Kaspersky Embedded Systems Security для Windows из командной строки, вы укажете другие компоненты Kaspersky Embedded Systems Security для Windows, не указывая компонент Core, компонент Core будет установлен автоматически. |
| Контроль запуска программ | AppCtrl | Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает запуск в соответствии с заданными правилами контроля запуска программ.<br>Компонент реализуется в задаче Контроль запуска программ. |
| Контроль устройств | DevCtrl | Этот компонент отслеживает попытки подключения внешних устройств к защищаемому устройству и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств.<br>Компонент реализуется в задаче Контроль устройств. |
| Антивирусная защита | AVProtection | Этот компонент обеспечивает антивирусную защиту. |

| Компонент | Идентификатор | Функции компонента |
|---|---|---|
| Защита от сетевых угроз | IDS | Этот компонент выполняет проверку входящего сетевого трафика на наличие активности, характерной для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Embedded Systems Security для Windows блокирует сетевую активность со стороны атакующего компьютера. |
| Проверка по требованию | Ods | Этот компонент устанавливает системные файлы Kaspersky Embedded Systems Security для Windows и выполняет задачи проверки по требованию (проверка объектов защищаемого устройства, выполняемая по команде). |
| Постоянная защита файлов | Oas | Этот компонент выполняет антивирусную проверку файлов на защищаемом устройстве при обращении к этим файлам.<br>Компонент реализует задачу Постоянная защита файлов. |
| Использование Kaspersky Security Network | Ksn | Этот компонент обеспечивает защиту на основе облачных технологий "Лаборатории Касперского".<br>Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network). |
| Мониторинг файловых операций | Fim | Этот компонент позволяет регистрировать операции, производимые над файлами в выбранной области мониторинга.<br>Компонент реализует задачу Мониторинг файловых операций. |
| Мониторинг доступа к реестру | RegMonitor | Этот компонент позволяет контролировать действия, выполненные с указанными ветвями и разделами реестра, в областях мониторинга, заданных в параметрах задачи.<br>Компонент реализует Мониторинг доступа к реестру. |
| Защита от эксплойтов | AntiExploit | Этот компонент обеспечивает управление параметрами защиты процессов в памяти устройства. |

| Компонент | Идентификатор | Функции компонента |
|---|---|---|
| Управление сетевым экраном | Firewall | Этот компонент предоставляет возможность управления брандмауэром Windows через графический интерфейс Kaspersky Embedded Systems Security для Windows.<br>Компонент реализует задачу Управление сетевым экраном. |
| Модуль интеграции с Агентом администрирования Kaspersky Security Center | AKIntegration | Этот компонент обеспечивает связь Kaspersky Embedded Systems Security для Windows с Агентом администрирования Kaspersky Security Center.<br>Вы можете установить этот компонент на защищаемом устройстве, 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. |
| Набор счетчиков производительности программы Системный монитор | PerfMonCounters | Компонент устанавливает набор счетчиков производительности программы Системный монитор. Счетчики производительности позволяют измерять производительность Kaspersky Embedded Systems Security для Windows и находить возможные узкие места при совместной работе Kaspersky Embedded Systems Security для Windows с другими программами. |
| Поддержка SNMP-протокола | SnmpSupport | Компонент публикует счетчики и ловушки Kaspersky Embedded Systems Security для Windows через Simple Network Management Protocol (протокол SNMP) в Microsoft Windows. Этот компонент можно установить на защищаемое устройство, только если на нем уже установлена служба SNMP. |
| Значок Kaspersky Embedded Systems Security для Windows в области уведомлений | TrayApp | Компонент отображает значок Kaspersky Embedded Systems Security для Windows в области уведомлений панели задач защищаемого устройства. Значок Kaspersky Embedded Systems Security для Windows показывает состояние защиты устройства и позволяет открыть Консоль программы с помощью Microsoft Management Console, если она установлена, и окно **О программе**. |

## Программный компонент "Средства администрирования"

В следующей таблице содержится код и описание программного компонента набора "Средства администрирования".

*Таблица 3. Описание программного компонента "Средства администрирования"*

| Компонент | Код | Функции компонента |
|---|---|---|
| Оснастка Kaspersky Embedded Systems Security для Windows | MmcSnapin | Компонент устанавливает оснастку Консоли управления Microsoft (MMC) для управления программой с помощью Консоли Kaspersky Embedded Systems Security для Windows.<br>Если при установке набора "Средства администрирования" из командной строки, вы укажете другие компоненты набора, но не укажите компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически. |

# Изменения в системе после установки Kaspersky Embedded Systems Security для Windows

При совместной установке Kaspersky Embedded Systems Security для Windows и набора "Средства администрирования", включающего Консоль программы, служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Embedded Systems Security для Windows на защищаемом устройстве и на устройстве, на котором установлена Консоль программы;
- регистрирует службы Kaspersky Embedded Systems Security для Windows;
- создает группу пользователей Kaspersky Embedded Systems Security для Windows;
- регистрирует в системном реестре ключи Kaspersky Embedded Systems Security для Windows;
- создает системную задачу Kaspersky Embedded Systems Security OS Upgrade Detect, которая отображается в Планировщике задач Windows.

Эти изменения описаны ниже.

### Папки Kaspersky Embedded Systems Security для Windows на защищаемом устройстве

При установке Kaspersky Embedded Systems Security для Windows на защищаемом устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Embedded Systems Security для Windows, содержащая исполняемые файлы Kaspersky Embedded Systems Security для Windows в зависимости от разрядности операционной системы. По умолчанию используются следующие папки установки:
  - В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security

- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Embedded Systems Security для Windows по протоколу SNMP.
  - %Kaspersky Embedded Systems Security%\mibs
- 64-разрядные версии исполняемых файлов Kaspersky Embedded Systems Security для Windows (папка создается только при установке Kaspersky Embedded Systems Security для Windows в 64-разрядной версии Microsoft Windows).
  - %Kaspersky Embedded Systems Security%\x64
- Служебные файлы Kaspersky Embedded Systems Security для Windows:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Dskm

  Для Windows XP путь к папке Kaspersky Lab – %ALLUSERSPROFILE%\Application Data

- Файлы с параметрами источников обновлений:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update
- Обновления баз и программных модулей, загруженные с помощью задачи Копирование обновлений (папка создается при первой загрузке обновлений с помощью задачи Копирование обновлений).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update\Distribution
- Журналы выполнения задач и журнал системного аудита.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports
- Набор используемых баз данных.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Current
- Резервные копии баз; перезаписываются при каждом обновлении баз.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Backup
- Временные файлы, создаваемые при выполнении задач обновления.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Temp
- Объекты на карантине (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Quarantine
- Объекты в резервном хранилище (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Backup
- Объекты, восстановленные из резервного хранилища и карантина (папка по умолчанию для восстановленных объектов).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored

### Папка, создаваемая при установке Консоли программы

Заданная по умолчанию папка установки Консоли программы, содержащая файлы набора "Средства администрирования", зависит от разрядности операционной системы. По умолчанию используются следующие папки установки:

- В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

### Службы Kaspersky Embedded Systems Security для Windows

Следующие службы Kaspersky Embedded Systems Security для Windows запускаются под системной учетной записью Локальная система (SYSTEM).

- Kaspersky Security Service (KAVFS) – это основная служба Kaspersky Embedded Systems Security для Windows, которая управляет задачами и рабочими процессами Kaspersky Embedded Systems Security для Windows.
- Служба Kaspersky Security Management (KAVFSGT) – это служба, предназначенная для управления Kaspersky Embedded Systems Security для Windows через Консоль программы.
- Служба Kaspersky Security Exploit Prevention (KAVFSSLP)– это служба, исполняющая роль посредника при передаче параметров безопасности внешним агентам безопасности и при получении данных о событиях безопасности.

### Группа Kaspersky Embedded Systems Security для Windows

ESS Administrators – это группа на защищаемом устройстве, пользователи которой имеют полный доступ к службе Kaspersky Security Management и ко всем функциям Kaspersky Embedded Systems Security для Windows.

### Ключи системного реестра

При установке Kaspersky Embedded Systems Security для Windows создаются следующие ключи системного реестра:

- Свойства Kaspersky Embedded Systems Security для Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Параметры журнала событий Kaspersky Embedded Systems Security для Windows (Kaspersky Event Log): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Свойства службы управления Kaspersky Embedded Systems Security для Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Параметры счетчиков производительности:
  - В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - В Microsoft Windows 64-разрядной версии: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]

- Параметры компонента Поддержка SNMP-протокола:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\SnmpAgent]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\SnmpAgent]
- Параметры файла дампа:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\CrashDump]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\CrashDump]
- Параметры файла трассировки:
  - В Microsoft Windows 32-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\Trace]
  - В Microsoft Windows 64-разрядной версии:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\Trace]
- Параметры задач и функций программы:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\Environment]

**Системная задача Kaspersky Embedded Systems Security OS Upgrade Detect**

Служба установщика Windows создает задачу Kaspersky Embedded Systems Security OS Upgrade Detect во время установки программы. Задача запускается сразу после ее создания и далее при каждой загрузке ОС. Задача проверяет версию используемых программой драйверов: если выполнено обновление версии операционной системы, программа обновляет драйверы для соответствующей версии операционной системы.

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

# Процессы Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows запускает процессы, описанные в таблице ниже.

*Таблица 4. Процессы Kaspersky Embedded Systems Security для Windows*

| Имя файла | Назначение |
|---|---|
| kavfswp.exe | Рабочий процесс Kaspersky Embedded Systems Security для Windows |
| kavtray.exe | Процесс значка области уведомлений |
| kavfsmui.exe | Процесс компонента Диагностическое окно |
| kavshell.exe | Процесс утилиты командной строки |

| Имя файла | Назначение |
|---|---|
| kavfsrcn.exe | Процесс удаленного управления Kaspersky Embedded Systems Security для Windows |
| kavfs.exe | Процесс службы Kaspersky Security |
| kavfsgt.exe | Процесс службы Kaspersky Security Management |
| kavfswh.exe | Процесс службы Kaspersky Security Exploit Prevention |

# Параметры установки и удаления и ключи командной строки для службы установщика Windows

В этом разделе описаны параметры установки и удаления Kaspersky Embedded Systems Security для Windows, их значения по умолчанию, указаны ключи для изменения параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Embedded Systems Security для Windows из командной строки.

**Параметры установки и ключи командной строки для установщика Windows**

- Согласие с условиями Лицензионного соглашения: необходимо принять условия для установки Kaspersky Embedded Systems Security для Windows.

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

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

- Согласие с условиями Политики конфиденциальности: необходимо принять условия для установки Kaspersky Embedded Systems Security для Windows.

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

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

- Разрешить установку Kaspersky Embedded Systems Security для Windows, если не установлено обновление KB4528760. Дополнительная информация об обновлении KB4528760 приведена на веб-сайте Microsoft https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760.

  Возможны следующие значения ключа командной строки `SKIPCVEWINDOWS10=<значение>`:

  - `0` – отменить установку Kaspersky Embedded Systems Security для Windows, если не установлено обновление KB4528760 (значение по умолчанию).
  - `1` – разрешить установку Kaspersky Embedded Systems Security для Windows, если не установлено обновление KB4528760.

Обновление KB4528760 исправляет уязвимость безопасности CVE-2020-0601. Дополнительная информация об уязвимости в системе безопасности CVE-2020-0601 приведена на веб-сайте Microsoft https://support.microsoft.com/ru-ru/help/4528760/windows-10-update-kb4528760.

- Установка Kaspersky Embedded Systems Security для Windows с восстановленными параметрами предыдущей версии при обновлении.

  Возможны следующие значения ключа командной строки RESTOREDEFSETTINGS=<значение>:

  - 0 – все данные из предыдущей версии переносятся в новую версию при обновлении (значение по умолчанию).
  - 1 – только файл с данными активации и закрытыми ключами переносится в новую версию при обновлении ([диск]:\ProgramData\Kaspersky Lab\<продукт>\<версия>\Data\product.dat). Все остальные данные из предыдущей версии, такие как настройки, антивирусные базы, отчеты, объекты карантина и резервного хранилища, удаляются.

- Установка Kaspersky Embedded Systems Security для Windows с сохранением отчетов из предыдущих версий при обновлении.

  Возможны следующие значения ключа командной строки KEEP_REPORTS=<значение>:

  - 0 – все данные из предыдущей версии, кроме отчетов ([диск]:\ProgramData\Kaspersky Lab\<продукт>\<версия>\Reports), переносятся в новую версию при обновлении. Отчеты удаляются.
  - 1 – все данные из предыдущей версии, такие как настройки, антивирусные базы, отчеты, объекты карантина и резервного хранилища, переносятся в новую версию при обновлении (значение по умолчанию).

- Установка Kaspersky Embedded Systems Security для Windows с предварительной проверкой активных процессов и загрузочных секторов локальных дисков.

  Возможны следующие значения ключа командной строки PRESCAN=<значение>:

  - 0 – не выполнять предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки (значение по умолчанию).
  - 1 – выполнить предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки.

- Папка, в которую будут сохранены файлы Kaspersky Embedded Systems Security для Windows при установке. Вы можете указать другую папку.

  Значение по умолчанию для ключа командной строки INSTALLDIR=<полный путь к папке>:

  - Kaspersky Embedded Systems Security для Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%

- Запуск задачи Постоянная защита файлов сразу после запуска Kaspersky Embedded Systems Security для Windows.

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

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

- Режим работы задачи Постоянная защита файлов.

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

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

- Объекты, исключаемые из области защиты в соответствии с рекомендациями корпорации Microsoft. В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать корпорация Microsoft. Некоторые программы на защищаемом устройстве могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, используемые этими программами. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.

  Возможны следующие значения ключа командной строки `ADDMSEXCLUSION=<значение>`:

  - `1` – исключить (значение по умолчанию).
  - `0` – не исключать.

- Объекты, исключаемые из области защиты в соответствии с рекомендациями "Лаборатории Касперского". В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать "Лаборатория Касперского".

  Возможны следующие значения ключа командной строки `ADDKLEXCLUSION=<значение>`:

  - `1` – исключить (значение по умолчанию).
  - `0` – не исключать.

- Разрешить удаленное подключение к Консоли программы По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом устройстве, не разрешено. Во время установки можно разрешить подключение. Kaspersky Embedded Systems Security для Windows создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.

  Возможны следующие значения ключа командной строки `ALLOWREMOTECON=<значение>`:

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Путь к файлу ключа (`LICENSEKEYPATH`). По умолчанию установщик Windows пытается найти файл с расширением .key в папке \exec комплекта поставки. Если в папке \exec имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Можно предварительно сохранить файл ключа в папке \exec или указать другой путь к файлу ключа с помощью параметра **Добавить ключ**. Вы можете добавить ключ после установки Kaspersky Embedded Systems Security для Windows с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ во время установки программы, после установки Kaspersky Embedded Systems Security для Windows не будет функционировать.

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

  Значение по умолчанию для параметра `CONFIGPATH=<имя конфигурационного файла>` не указано.

- Режим задачи **Проверка при старте операционной системы** (SCANSTARTUP_BLOCKING). Если установка Kaspersky Embedded Systems Security для Windows выполнялась без ключа SCANSTARTUP_BLOCKING, параметру **Область проверки** в задаче **Проверка при старте операционной системы** назначаются следующие значения:

  - **Действия над зараженными и другими обнаруженными объектами: Только уведомлять**
  - **Действия над возможно зараженными объектами: Только уведомлять**

  Если установка Kaspersky Embedded Systems Security для Windows выполнялась с использованием ключа SCANSTARTUP_BLOCKING, параметру **Область проверки** в задаче **Проверка при старте операционной системы** назначаются следующие значения:

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

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

- Параметр включения сетевых соединений для Консоли программы используется для установки Консоли Kaspersky Embedded Systems Security для Windows на другое устройство. Вы можете удаленно управлять защитой устройства с другого устройства, на котором установлена Консоль Kaspersky Embedded Systems Security для Windows. В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла kavfsrcn.exe для удаленного управления Kaspersky Embedded Systems Security для Windows и предоставлен доступ к DCOM-программам. После завершения установки добавьте пользователей в ESS Administrators группу KAVWSEE Administrators, чтобы разрешить им управлять программой удаленно, а также разрешите на защищаемом устройстве сетевые подключения к службе Kaspersky Security Management (файл kavfsgt.exe). Можно более детально ознакомиться с дополнительной настройкой при установке Kaspersky Embedded Systems Security для Windows на другое устройство (см. раздел "Дополнительная настройка после установки Консоли программы на другое устройство" на стр. 62).

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

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Отключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на защищаемое устройство в фоновом режиме. Независимо от значения данного параметра, при установке Kaspersky Embedded Systems Security для Windows программа всегда предупреждает о других версиях программы, установленных на этом же защищаемом устройстве.

  Возможны следующие значения ключа командной строки `SKIPINCOMPATIBLESW=<значение>`:

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

**Параметры удаления и ключи командной строки для установщика Windows**

- Восстановление содержимого карантина.

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

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

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

  - `0` – удалить содержимое резервного хранилища (значение по умолчанию).
  - `1` – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную папку \Backup.
- Ввод текущего пароля для подтверждения операции удаления (при включенной функции защиты паролем).

  Значение по умолчанию для ключа `UNLOCK_PASSWORD=<указанный пароль>` не задано.
- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

  Значение по умолчанию для ключа командной строки `RESTOREPATH=<полный путь к папке>` – %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored

# Журналы установки и удаления Kaspersky Embedded Systems Security для Windows

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security для Windows с помощью мастера установки (удаления), служба установщика Windows создает журнал установки (удаления). Файл журнала с именем ess_v3.3_install_<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала) сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление** для Консоли программы или для Kaspersky Embedded Systems Security для Windows, в папке %temp% будет автоматически создан файл журнала с именем ess_3.3_maintenance.log.

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security для Windows из командной строки, по умолчанию файл журнала установки не создается.

► *Чтобы установить Kaspersky Embedded Systems Security для Windows и создать файл журнала на диске C:\, выполните одну из следующих команд:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

# Планирование установки

В этом разделе описаны средства администрирования Kaspersky Embedded Systems Security для Windows, особенности установки и удаления Kaspersky Embedded Systems Security для Windows с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. 57), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. 72), с помощью Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. 79) и через групповые политики Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 84).

Перед началом установки Kaspersky Embedded Systems Security для Windows составьте план основных этапов установки.

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Embedded Systems Security для Windows и для настройки программы.
2. Определите, какие программные компоненты требуется установить (см. раздел "Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows" на стр. 41).
3. Выберите способ установки.

## В этом разделе

Выбор средств администрирования ..... 54
Выбор способа установки ..... 56

## Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров и управления Kaspersky Embedded Systems Security для Windows. В качестве средств администрирования Kaspersky Embedded Systems Security для Windows вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

### Консоль Kaspersky Embedded Systems Security для Windows

Консоль Kaspersky Embedded Systems Security для Windows представляет собой самостоятельную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security для Windows в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security для Windows.

Консоль программы входит в набор компонентов "Средства администрирования".

### Утилита командной строки

Вы можете управлять Kaspersky Embedded Systems Security для Windows из командной строки защищаемого устройства.

Утилита командной строки входит в набор программных компонентов Kaspersky Embedded Systems Security для Windows.

### Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств в вашей организации, вы можете управлять Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows. Он позволяет Kaspersky Embedded Systems Security для Windows взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемое устройство.
- **Агент администрирования Kaspersky Security Center**. Установите его на каждом защищаемом устройстве. Этот компонент будет обеспечивать взаимодействие между программой Kaspersky Embedded Systems Security для Windows, установленной на защищаемом устройстве, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин управления Kaspersky Embedded Systems Security 3.3 для Windows**. Дополнительно на защищаемом устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Embedded Systems Security для Windows для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления \exec\klcfginst.exe входит в комплект поставки Kaspersky Embedded Systems Security для Windows.

# Выбор способа установки

После определения программных компонентов для установки Kaspersky Embedded Systems Security для Windows (см. раздел "Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows" на стр. 41), необходимо выбрать способ установки программы.

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

- Потребуется ли вам задать специальные параметры установки Kaspersky Embedded Systems Security для Windows или вы будете использовать рекомендуемые параметры установки (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 49).
- Будут ли параметры установки едиными для всех защищаемых устройств или индивидуальными для каждого защищаемого устройства.

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

Вы можете установить и настроить Kaspersky Embedded Systems Security для Windows на отдельном защищаемом устройстве и сохранить его параметры в конфигурационный файл, чтобы затем использовать созданный файл для установки Kaspersky Embedded Systems Security для Windows на другие защищаемые устройства. Однако это невозможно при установке программы через групповые политики Active Directory.

### Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Embedded Systems Security для Windows (см. раздел "Программные компоненты Kaspersky Embedded Systems Security для Windows" на стр. 42) из файла \exec\setup.exe, входящего в комплект поставки, на защищаемом устройстве.
- Консоль Kaspersky Embedded Systems Security для Windows (см. раздел "Установка Консоли Kaspersky Embedded Systems Security для Windows" на стр. 60) из файла \console\setup.exe, входящего в комплект поставки, на защищаемом устройстве или другом устройстве в локальной сети.

### Запуск из командной строки файла пакета установки с параметрами установки

Запустив файл пакета установки без ключей, вы установите Kaspersky Embedded Systems Security для Windows с параметрами установки по умолчанию. С помощью ключей Kaspersky Embedded Systems Security для Windows вы можете изменять параметры установки.

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

Вы также можете использовать команды для установки Kaspersky Embedded Systems Security для Windows и Консоли программы (см. раздел "Установка и удаление программы из командной строки" на стр. 72).

### Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой устройств в сети, вы можете установить Kaspersky Embedded Systems Security для Windows на несколько устройств с помощью задачи удаленной установки.

Защищаемые устройства, на которых вы хотите установить Kaspersky Embedded Systems Security для Windows с помощью Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. 79), могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене, а также вообще не принадлежать ни к одному домену.

**Централизованная установка через групповые политики Active Directory**

С помощью групповых политик Active Directory вы можете устанавливать Kaspersky Embedded Systems Security для Windows на защищаемом устройстве. Вы можете установить Консоль программы на защищаемом устройстве или рабочем месте администратора.

Вы можете установить Kaspersky Embedded Systems Security для Windows, используя только параметры установки по умолчанию.

Защищаемые устройства, на которых программа Kaspersky Embedded Systems Security для Windows была установлена с помощью групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 84), должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске защищаемого устройства, перед входом в Microsoft Windows.

# Установка и удаление программы с помощью мастера

В этом разделе описана установка и удаление Kaspersky Embedded Systems Security для Windows и Консоли программы с помощью мастера установки, а также приведена информация о дополнительных параметрах Kaspersky Embedded Systems Security для Windows и действиях при установке.

## В этом разделе


Установка с помощью мастера установки ..... 57

Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security для Windows ..... 68

Удаление с помощью мастера установки ..... 70


## Установка с помощью мастера установки

В следующих разделах содержится информация об установке Kaspersky Embedded Systems Security для Windows и Консоли программы.

► *Чтобы установить и начать использовать Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. Установите Kaspersky Embedded Systems Security для Windows на защищаемое устройство.
2. На устройства, с которых вы планируете управлять Kaspersky Embedded Systems Security для Windows, установите Консоль программы.
3. Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку, чтобы пользователи Консоли программы могли удаленно управлять Kaspersky Embedded Systems Security для Windows.
4. Выполните действия после установки Kaspersky Embedded Systems Security для Windows.

kaspersky

## В этом разделе

Установка Kaspersky Embedded Systems Security для Windows ..... 58
Установка Консоли Kaspersky Embedded Systems Security для Windows ..... 60
Дополнительная настройка после установки Консоли программы на другое устройство ..... 62
Действия после установки Kaspersky Embedded Systems Security для Windows ..... 65

## Установка Kaspersky Embedded Systems Security для Windows

Перед установкой Kaspersky Embedded Systems Security для Windows выполните следующие действия:

1. Убедитесь, что на защищаемом устройстве не установлены другие антивирусные программы.
2. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом устройстве.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Embedded Systems Security для Windows. Вы можете прервать установку Kaspersky Embedded Systems Security для Windows на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Можно более детально ознакомиться с параметрами установки (удаления) (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 49).

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с помощью мастера установки, выполните следующие действия:*

1. На защищаемом устройстве запустите файл setupui.exe.
2. В открывшемся окне в разделе **Установка** перейдите по ссылке **Установить защиту на основе разрешенных списков** или **Установить защиту на основе антивирусных баз**.

Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию".

Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты:

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

При установке программы в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

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

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

3. В открывшемся окне приветствия мастера установки Kaspersky Embedded Systems Security для Windows нажмите на кнопку **Далее**.

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

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы принимаете условия и положения Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

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

6. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

7. Выберите компоненты, которые вы хотите установить.

   Компонент Поддержка SNMP-протокола Kaspersky Embedded Systems Security для Windows отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба Microsoft Windows SNMP.

8. Чтобы отменить все изменения, в окне **Сбросить** нажмите на кнопку **Выборочная установка**. Нажмите на кнопку **Далее**.
9. В окне **Выбор папки назначения** выполните следующие действия:
   - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Embedded Systems Security для Windows.
   - Если требуется, нажмите на кнопку **Диск** для просмотра информации о доступном пространстве на локальных жестких дисках.

   Нажмите на кнопку **Далее**.

10. В окне **Дополнительные параметры установки** настройте следующие параметры установки:
    - **Включить Постоянную защиту файлов после установки программы**
    - **Добавить к исключениям файлы, рекомендованные Microsoft**
    - **Добавить к исключениям файлы, рекомендованные «Лабораторией Касперского»**

      Нажмите на кнопку **Далее**.

11. В окне **Импорт параметров из конфигурационного файла** выполните следующие действия:
    a. Если вы хотите импортировать параметры Kaspersky Embedded Systems Security для Windows из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.
    b. Нажмите на кнопку **Далее**.
12. В окне **Активация программы** выполните одно из следующих действий:
    - Если вы хотите активировать программу, укажите файл ключа Kaspersky Embedded Systems Security для Windows для активации программы.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
    - Если вы предварительно сохранили файл ключа в папке \exec комплекта поставки, имя этого файла отобразится в поле **Ключ**.

      Чтобы добавить ключ с помощью файла ключа из другой папки, укажите путь к этому файлу.

      После добавления файла ключа в окне отобразится информация о лицензии. В Kaspersky Embedded Systems Security для Windows отображается расчетная дата истечения срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, а истекает не позднее даты окончания срока действия файла ключа.

      Нажмите на кнопку **Далее**, чтобы добавить файл ключа в программу.
13. В окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Embedded Systems Security для Windows.
14. По завершении установки откроется окно **Установка завершена**.
15. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. По завершении установки программа Kaspersky Embedded Systems Security для Windows готова к работе, если вы добавили ключ активации.

## Установка Консоли Kaspersky Embedded Systems Security для Windows

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

► *Чтобы установить Консоль программы, выполните следующие действия:*

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.
2. На защищаемом устройстве запустите файл setupui.exe.

   Откроется окно программы-приветствия.
3. Перейдите по ссылке **Установить Консоль Kaspersky Embedded Systems Security для Windows**.

   Откроется окно приветствия мастера установки.
4. Нажмите на кнопку **Далее**.

5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности и, чтобы продолжить установку, установите флажки под заголовком **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры установки**.
7. В окне **Дополнительные параметры установки** выполните следующие действия:
   - Если вы планируете с помощью Консоли программы управлять программой Kaspersky Embedded Systems Security для Windows, установленной на удаленном устройстве, установите флажок **Разрешить удаленный доступ**.
   - Чтобы открыть окно **Выборочная установка** и выбрать компоненты, выполните следующие действия:
     a. Нажмите на кнопку **Дополнительно**.

        Откроется окно **Выборочная установка**.

     b. В списке выберите набор компонентов «Средства администрирования».

        По умолчанию устанавливаются все компоненты.

     c. Нажмите на кнопку **Далее**.

   Можно ознакомиться с более подробной информацией о компонентах Kaspersky Embedded Systems Security для Windows (см. раздел "Коды программных компонентов Kaspersky Embedded Systems Security для Windows для службы установщика Windows" на стр. 41).
8. В окне **Выбор папки назначения** выполните следующие действия:
   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
   b. Нажмите на кнопку **Далее**.
9. В окне **Готовность к установке** нажмите на кнопку **Установить**.

   Мастер приступит к установке выбранных компонентов.
10. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. Консоль программы будет установлена на защищаемом устройстве.

Если вы установили набор Средства администрирования не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли программы на другое устройство" на стр. 62).

## Дополнительная настройка после установки Консоли программы на другое устройство

Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните следующие действия для того, чтобы пользователи могли удаленно управлять Kaspersky Embedded Systems Security для Windows:

- На защищаемом устройстве добавьте пользователей Kaspersky Embedded Systems Security для Windows в группу ESS Administrators.
- Включите сетевые соединения для службы Kaspersky Security Management Service (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 295), если на защищаемом устройстве используется брандмауэр Windows или сетевой экран стороннего поставщика.
- Если во время установки Консоли программы на устройство под управлением Microsoft Windows не был установлен флажок **Разрешить удаленный доступ**, вручную включите сетевые соединения для Консоли программы через сетевой экран устройства.

Консоль программы на удаленном устройстве использует протокол DCOM для получения информации о событиях Kaspersky Embedded Systems Security для Windows, например, о проверенных объектах или о завершении задач, от службы Kaspersky Security Management на защищаемом устройстве. Необходимо разрешить сетевые соединения для Консоли программы в параметрах брандмауэра Windows, чтобы устанавливать соединения между Консолью программы и службой Kaspersky Security Management.

На удаленном устройстве, на котором установлена Консоль программы, выполните следующие действия:

- Убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM).
- В параметрах брандмауэра Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security для Windows – kavfsrcn.exe.

  Устройство, на котором установлена Консоль программы, обменивается информацией с защищаемым устройством через порт TCP 135.
- Чтобы разрешить подключение, настройте правило исходящего подключения для брандмауэра Windows.

  В отличие от стандартных служб TCP/IP и UDP/IP, где для каждого протокола имеется фиксированный порт, DCOM динамически назначает порты удаленным COM-объектам. Если между клиентским устройством (на котором установлена Консоль программы) и DCOM-устройством (защищаемым устройством) находится сетевой экран, нужно открыть широкий диапазон портов.

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

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

1. Закройте Консоль программы.
2. Дождитесь завершения процесса удаленного управления Kaspersky Embedded Systems Security для Windows – kavfsrcn.exe.
3. Перезапустите Консоль программы.

   Будут применены новые параметры соединения.

## В этом разделе

Разрешение анонимного удаленного доступа к программам COM ..... 63

Разрешение сетевых соединений для процесса удаленного управления Kaspersky Embedded Systems Security для Windows ..... 64

Добавление правила исходящего подключения для брандмауэра Windows..... 65

## Разрешение анонимного удаленного доступа к программам COM

Названия параметров могут отличаться в разных операционных системах Windows.

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

1. На удаленном устройстве, на котором установлена Консоль Kaspersky Embedded Systems Security для Windows, откройте консоль Службы компонентов.
2. Выберите **Пуск** → **Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **OK**.
5. В консоли **Службы компонентов** защищаемого устройства разверните узел **Компьютеры**.
6. Откройте контекстное меню узла **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в блоке параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.
10. Нажмите на кнопку **OK**.

## Разрешение сетевых соединений для процесса удаленного управления Kaspersky Embedded Systems Security для Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы открыть TCP-порт 135 в брандмауэре Windows и разрешить сетевые соединения для процесса удаленного управления Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. На удаленном устройстве закройте Консоль Kaspersky Embedded Systems Security для Windows.
2. Выполните одно из следующих действий:
   - В Microsoft Windows XP с пакетом обновлений 2 и выше:
     a. Выберите **Пуск** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** (или Параметры брандмауэра Windows) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
     c. В поле **Имя** укажите имя порта RPC (TCP/135) или задайте другое имя, например, DCOM Kaspersky Embedded Systems Security для Windows, а в поле **Номер порта** укажите номер порта: 135.
     d. Выберите протокол **TCP**.
     e. Нажмите на кнопку **OK**.
     f. На закладке **Исключения** нажмите на кнопку **Добавить**.
   - В Microsoft Windows 7 и выше:
     a. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
     c. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.
3. В окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Embedded Systems Security для Windows с помощью Microsoft Management Console.
4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **OK** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

## Добавление правила исходящего подключения для брандмауэра Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы добавить правило исходящего подключения для брандмауэра Windows, выполните следующие действия:*

1. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
2. В окне **Брандмауэр Windows** перейдите по ссылке **Дополнительные параметры**.

   Откроется окно **Брандмауэр Windows в режиме повышенной безопасности**.
3. Выберите вложенный узел **Правила для исходящего подключения**.
4. На панели **Действия** выберите пункт **Создать правило**.
5. В открывшемся окне **Мастер создания правила для нового исходящего подключения** выберите параметр **Порт** и нажмите на кнопку **Далее**.
6. Выберите протокол **TCP**.
7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.
8. В окне **Действие** выберите пункт **Разрешить подключение**.
9. Сохраните созданное правило и закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Брандмауэр Windows не разрешает установку сетевых соединений между Консолью программы и службой Kaspersky Security Management.

## Действия после установки Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security для Windows был установлен флажок **Включить Постоянную защиту файлов после установки программы** (по умолчанию), программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security для Windows выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security для Windows рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз программы. После установки Kaspersky Embedded Systems Security для Windows проверяет объекты с использованием баз, которые входили в состав программы при поставке.

  Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security для Windows, так как базы могли устареть.

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

- Выполнить Проверку важных областей, если перед установкой Kaspersky Embedded Systems Security для Windows на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security для Windows.

## В этом разделе

Запуск и настройка задачи Обновление баз программы ..... 66
Проверка важных областей ..... 68

## Запуск и настройка задачи Обновление баз программы

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

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

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

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

1. Откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
3. Выберите закладку **Параметры соединения**.
4. В разделе **Параметры прокси-сервера** установите флажок **Использовать указанный прокси-сервер**.
5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.
6. В разделе **Параметры аутентификации на прокси-сервере** выберите требуемый метод аутентификации из раскрывающегося списка:
   - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Embedded Systems Security для Windows будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи. По умолчанию задача запускается под учетной записью **Локальная система** (**SYSTEM**).

- **Использовать NTLM-аутентификацию с именем пользователя и паролем**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Embedded Systems Security для Windows будет использовать указанную учетную запись для доступа к прокси-серверу. Введите имя и пароль пользователя или выберите пользователя в списке.
- **Использовать имя пользователя и пароль**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.

7. В окне **Параметры программы** нажмите на кнопку **OK**.

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

1. Запустите Консоль программы одним из следующих способов:
   - Откройте Консоль программы на защищаемом устройстве. Для этого в меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security для Windows** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security 3.3 для Windows**.
   - Если Консоль программы запущена не на защищаемом устройстве, подключитесь к защищаемому устройству:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
     b. Выберите пункт **Подключиться к другому компьютеру**.
     c. В диалоговом окне **Выбор защищаемого устройства** выберите вариант **Другое устройство** и в поле ввода укажите сетевое имя защищаемого устройства.

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

   Откроется окно Консоли программы.
2. В дереве Консоли программы разверните узел **Обновление**.
3. Выберите вложенный узел **Обновление баз программы**.
4. В панели результатов перейдите по ссылке **Свойства**.
5. В открывшемся окне **Параметры задачи** выберите закладку **Параметры соединения**.
6. Выберите **Использовать параметры прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского»**.
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Параметры соединения с источником обновлений в задаче Обновление баз программы будут сохранены.

► *Чтобы запустить задачу Обновление баз программы, выполните следующие действия:*

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

Задача Обновление баз программы будет запущена.

После того как задача успешно завершится, вы сможете посмотреть дату выпуска последних установленных обновлений баз в панели результатов узла **Kaspersky Embedded Systems Security для Windows**.

### Проверка важных областей

После того как вы обновили базы Kaspersky Embedded Systems Security для Windows, проверьте защищаемое устройство на наличие вредоносных программ с помощью задачи Проверка важных областей.

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

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

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

► *Чтобы просмотреть журнал выполнения задачи,*

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

## Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security для Windows

Вы можете добавлять или удалять компоненты Kaspersky Embedded Systems Security для Windows. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу Постоянная защита файлов или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security для Windows запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► *Чтобы изменить состав компонентов Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security для Windows** > **Изменение или удаление Kaspersky Embedded Systems Security для Windows**.

   Откроется окно мастера установки программы **Восстановление или удаление**.
2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

3. В списке доступных компонентов в окне **Выборочная установка** выберите компоненты, которые требуется добавить или удалить из состава Kaspersky Embedded Systems Security для Windows. Для этого выполните следующие действия:
   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:
     - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;
     - пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если требуется установить группу компонентов.
   - Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

   Нажмите на кнопку **Далее**.
4. В окне **Готовность к установке** подтвердите изменение состава компонентов программы, нажав на кнопку **Установить**.
5. В окне, открывшемся по завершении установки, нажмите на кнопку **OK**.

Состав компонентов Kaspersky Embedded Systems Security для Windows будет изменен в соответствии с заданными параметрами.

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

► *Чтобы восстановить Kaspersky Embedded Systems Security для Windows после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security для Windows**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security для Windows**.

   Откроется окно мастера установки программы **Восстановление или удаление**.
4. Выберите вариант **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

   Откроется окно **Восстановление установленных компонентов**.
5. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если вы хотите сбросить параметры программы и восстановить Kaspersky Embedded Systems Security для Windows с параметрами по умолчанию. Нажмите на кнопку **Далее**.
6. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
7. В окне, открывшемся по завершении операции восстановления, нажмите на кнопку **OK**.

Программа Kaspersky Embedded Systems Security для Windows будет восстановлена с указанными параметрами.

kaspersky

# Удаление с помощью мастера установки

В этом разделе приведены инструкции по удалению Kaspersky Embedded Systems Security для Windows и Консоли программы с защищаемого устройства с помощью мастера установки / удаления.

## В этом разделе


Удаление Kaspersky Embedded Systems Security для Windows ..... 70

Удаление Консоли Kaspersky Embedded Systems Security для Windows ..... 71


## Удаление Kaspersky Embedded Systems Security для Windows

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security для Windows. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 215).
Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Embedded Systems Security для Windows с защищаемого устройства с помощью мастера установки / удаления.

После удаления Kaspersky Embedded Systems Security для Windows с защищаемого устройства может потребоваться перезагрузка. Перезагрузку можно отложить.

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

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security для Windows запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► *Чтобы удалить Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security для Windows**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security для Windows**.

   Откроется окно мастера установки программы **Восстановление или удаление**.

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

   Откроется окно **Дополнительные параметры удаления программы**.

5. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:

   a. Установите флажок **Экспортировать объекты на карантине**, чтобы программа Kaspersky Embedded Systems Security для Windows экспортировала объекты, помещенные на карантин. По умолчанию флажок снят.

   b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы экспортировать объекты из резервного хранилища Kaspersky Embedded Systems Security для Windows. По умолчанию флажок снят.

   c. Нажмите на кнопку **Сохранить в** и укажите папку, в которую требуется экспортировать объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security для Windows\Uninstall.

      Нажмите на кнопку **Далее**.

6. В окне **Готовность к удалению** подтвердите удаление, нажав на кнопку **Удалить**.

7. В окне, открывшемся по завершении удаления, нажмите на кнопку **OK**.

Программа Kaspersky Embedded Systems Security для Windows будет удалена с защищаемого устройства.

## Удаление Консоли Kaspersky Embedded Systems Security для Windows

Названия параметров могут отличаться в разных операционных системах Windows.

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

После удаления Консоли программы перезагрузка защищаемого устройства не требуется.

► *Чтобы удалить Консоль программы, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security для Windows**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security для Windows**.

   Откроется окно мастера **Восстановление или удаление**.

4. Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.
5. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление завершено**.

6. Нажмите на кнопку **OK**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

kaspersky

# Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Embedded Systems Security для Windows из командной строки, примеры команд для установки и удаления Kaspersky Embedded Systems Security для Windows из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Embedded Systems Security для Windows из командной строки.

## В этом разделе


Об установке и удалении Kaspersky Embedded Systems Security для Windows из командной строки ..... 72

Примеры команд установки Kaspersky Embedded Systems Security для Windows ..... 73

Действия после установки Kaspersky Embedded Systems Security для Windows ..... 75

Добавление и удаление компонентов. Примеры команд ..... 76

Удаление Kaspersky Embedded Systems Security для Windows. Примеры команд ..... 77

Коды возврата ..... 78


## Об установке и удалении Kaspersky Embedded Systems Security для Windows из командной строки

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security для Windows. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 215).

Вы можете установить или удалить Kaspersky Embedded Systems Security для Windows, а также добавить или удалить его компоненты, запустив файл инсталляционного пакета \exec\ess_x86.msi или \exec\ess_x64.msi из командной строки и указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом устройстве или на другом устройстве в сети, чтобы работать с Консолью программы локально или удаленно. Для этого используйте пакет установки \console\esstools.msi

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

Если вы запустите на защищаемом устройстве один из файлов \exec\ess_x86.msi или \exec\ess_x64.msi без дополнительных ключей, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows

В этом разделе приведены примеры команд для установки Kaspersky Embedded Systems Security для Windows.

На защищаемом устройстве под управлением 32-разрядной версии Microsoft Windows запускайте файлы с суффиксом x86 из комплекта поставки. На защищаемом устройстве под управлением 64-разрядной версии Microsoft Windows запускайте файлы с суффиксом x64 из комплекта поставки.

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

**Примеры установки Kaspersky Embedded Systems Security для Windows из файла setup.exe**

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

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

Kaspersky Embedded Systems Security для Windows можно установить со следующими параметрами:

- Установить только компоненты Постоянная защита файлов и Проверка по требованию.
- Не запускать Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security для Windows.
- Не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

► *Чтобы установить компоненты, например Контроль устройств, выполните следующую команду:*

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

При установке Kaspersky Embedded Systems Security для Windows на компьютеры с сетевыми устройствами и SCSI-устройствами, вызывающими сбой системы после установки <RPODUCT_NAME_NOM_FULL>, с этой командой можно использовать следующие дополнительные ключи:

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

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

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

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

**Список команд для установки: запуск msi-файла**

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с параметрами по умолчанию и показать интерфейс установки, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с рекомендованными параметрами установки и включить ротацию файлов трассировки при достижении ими заданного максимального количества, выполните следующую команду:*

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

Параметр `TRACE_FOLDER` является обязательным.

Для параметра `TRACE_MAX_ROLL_COUNT` действуют следующие правила:

- Если параметр указан, включается ротация файлов трассировки при достижении ими максимального количества, указанного в параметре. Доступный диапазон значений параметра: от 1 до 999.
- Если в качестве максимального количества файлов трассировки указано значение 0, ротация файлов трассировки будет отключена.
- Если параметр указан, но его значение недопустимо или превышает диапазон допустимых значений от 1 до 999 файлов, ротация файлов трассировки включается с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.
- Если параметр не указан:
  - Если на устройстве уже настроена ротация файлов трассировки, ее параметры не изменяются. Программа будет игнорировать вводимые параметры.
  - Если ротация файлов трассировки на устройстве не настроена, параметр ротации будет включен с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.

► *Чтобы установить Kaspersky Embedded Systems Security для Windows и активировать его с помощью файла ключа C:\0000000A.key, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с предварительной проверкой активных процессов и загрузочных секторов локальных дисков, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows в папку установки C:\ESS, выполните следующую команду:*

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

► *Чтобы установить Kaspersky Embedded Systems Security для Windows и сохранить файл журнала установки с именем ess.log в папку, где хранится msi-файл Kaspersky Embedded Systems Security для Windows, выполните следующую команду:*

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

► *Чтобы установить Консоль Kaspersky Embedded Systems Security для Windows, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows и активировать программу с помощью файла ключа C:\0000000A.key, а также настроить Kaspersky Embedded Systems Security для Windows в соответствии с параметрами в конфигурационном файле C:\settings.xml, выполните следующую команду:*

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

► *Чтобы установить исправление, если программа Kaspersky Embedded Systems Security для Windows защищена паролем, выполните следующую команду:*

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

## Действия после установки Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security для Windows был установлен флажок **Включить Постоянную защиту файлов после установки программы**, программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security для Windows выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security для Windows рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Embedded Systems Security для Windows. После установки Kaspersky Embedded Systems Security для Windows проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security для Windows. Для этого вам нужно запустить задачу Обновление баз программы. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию.

  Например, вы можете запустить задачу Обновление баз программы, выполнив следующую команду:

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

При этом обновления баз Kaspersky Embedded Systems Security для Windows будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080) с использованием для доступа к серверу встроенной в Windows проверки подлинности NTLM с учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить Проверку важных областей, если перед установкой Kaspersky Embedded Systems Security для Windows на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.

► *Чтобы выполнить задачу Проверка важных областей с помощью командной строки, выполните следующую команду:*

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

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

- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security для Windows.

## Добавление и удаление компонентов. Примеры команд

► *Компонент Контроль запуска программ устанавливается автоматически.*

► *Чтобы установить компонент Проверка по требованию, выполните следующую команду:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

или

```
\exec\setup.exe /s /p ADDLOCAL=Oas,Ods
```

После добавления компонентов в список Kaspersky Embedded Systems Security для Windows переустанавливает существующие компоненты и устанавливает указанные компоненты.

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

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

► *Чтобы установить новые компоненты, выполните следующую команду:*

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,Lo
gInspector,Oas,Ods,SnmpSupport,TrayApp,IDS,RegMonitor EULA=1
PRIVACYPOLICY=1 /qn
```

После того, как вы перечислили компоненты, которые требуется установить и удалить, Kaspersky Embedded Systems Security для Windows установит и удалит соответствующие компоненты.

## Удаление Kaspersky Embedded Systems Security для Windows. Примеры команд

► *Чтобы удалить Kaspersky Embedded Systems Security для Windows с защищаемого устройства, выполните следующую команду:*

- Для 32-разрядной операционной системы:

```
msiexec /x ess_x86.msi /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x ess_x64.msi /qn
```

или

- Для 32-разрядной операционной системы:

```
msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} /qn
```

► *Чтобы удалить Консоль Kaspersky Embedded Systems Security для Windows, выполните следующую команду:*

```
msiexec /x esstools.msi /qn
```

или

```
msiexec /x {4A79347C-BAE9-4A94-BF5D-16CDA5085084} /qn
```

► *Чтобы удалить Kaspersky Embedded Systems Security для Windows с устройства, на котором установлена защита паролем, выполните следующую команду:*

- Для 32-разрядной операционной системы:

```
msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} UNLOCK_PASSWORD=*** /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} UNLOCK_PASSWORD=*** /qn
```

## Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

*Таблица 5. Коды возврата*

| Код | Описание |
|---|---|
| 1324 | Имя папки назначения содержит недопустимые символы. |
| 25001 | Недостаточно прав для установки Kaspersky Embedded Systems Security для Windows. Чтобы установить программу, запустите мастер установки с правами локального администратора. |
| 25003 | Не удается установить Kaspersky Embedded Systems Security для Windows на устройство под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows. |
| 25004 | Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующее программное обеспечение: <список несовместимого программного обеспечения>. |
| 25010 | Указанный путь не может быть использован для сохранения объектов на карантине. |
| 25011 | Имя папки для сохранения объектов на карантине содержит недопустимые символы. |
| 26251 | Не удалось загрузить DLL для Счетчиков производительности. |
| 26252 | Не удалось загрузить DLL для Счетчиков производительности. |
| 27300 | Драйвер не может быть установлен. |
| 27301 | Драйвер не может быть удален. |
| 27302 | Невозможно установить сетевой компонент. Достигнуто максимальное пороговое значение поддерживаемого количества устройств фильтрации. |
| 27303 | Антивирусные базы не найдены. |

# Установка и удаление программы с помощью Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Embedded Systems Security для Windows с помощью Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center, а также описание действий после установки Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Общие сведения об установке через Kaspersky Security Center ..... 79

Права для установки или удаления Kaspersky Embedded Systems Security для Windows ..... 80

Установка Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center ..... 80

Действия после установки Kaspersky Embedded Systems Security для Windows ..... 82

Установка Консоли программы через Kaspersky Security Center ..... 83

Удаление Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center..... 84


## Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки программа Kaspersky Embedded Systems Security для Windows будет установлена с одинаковыми параметрами на несколько защищаемых устройств.

Можно объединить все защищаемые устройства в одну группу администрирования и создать групповую задачу установки Kaspersky Embedded Systems Security для Windows на защищаемые устройства этой группы.

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

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

## Права для установки или удаления Kaspersky Embedded Systems Security для Windows

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

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

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

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

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

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

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

## Установка Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center

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

Если вы планируете в дальнейшем управлять Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На защищаемом устройстве с установленным Сервером администрирования Kaspersky Security Center также установлен Плагин управления (файл \exec\klcfginst.exe комплекта поставки Kaspersky Embedded Systems Security для Windows).

- На защищаемых устройствах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых устройствах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Embedded Systems Security для Windows с помощью задачи удаленной установки.

Можно также объединить устройства в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

► *Чтобы установить Kaspersky Embedded Systems Security для Windows с помощью задачи удаленной установки, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Дополнительно**.
3. Разверните вложенный узел **Удаленная установка**.
4. В панели результатов вложенного узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.
5. Выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. Введите имя инсталляционного пакета.
7. Выберите файл ess.kud из комплекта поставки Kaspersky Embedded Systems Security для Windows в качестве файла инсталляционного пакета.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
8. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

   Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.
9. Чтобы изменить набор устанавливаемых компонентов (см. раздел "Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security для Windows" на стр. 68) Kaspersky Embedded Systems Security для Windows и настроить параметры по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 49) в инсталляционном пакете, выполните следующие действия:
   a. В Kaspersky Security Center разверните узел **Удаленная установка**.
   b. В панели результатов вложенного узла **Инсталляционные пакеты** откройте контекстное меню созданного инсталляционного пакета Kaspersky Embedded Systems Security для Windows и выберите пункт **Свойства**.
   c. В окне **Свойства: <название инсталляционного пакета>** перейдите раздел **Настройка**.
   d. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Embedded Systems Security для Windows, которые вы хотите установить.

e. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.

   Путь к папке назначения может содержать системные переменные окружения. Если указанной папки не существует на защищаемом устройстве, она будет создана.

f. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:

   - **Выполнить антивирусную проверку защищаемого устройства перед началом установки**
   - **Включить постоянную защиту после установки программы**
   - **Добавить к исключениям файлы, рекомендованные Microsoft**
   - **Добавить к исключениям файлы, рекомендованные Лабораторией Касперского**
   - **Включить отложенный запуск Kaspersky Security Service при старте операционной системы**

g. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.

10. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Embedded Systems Security для Windows на защищаемые устройства (группу администрирования). Настройте параметры задачи.

    Подробная информация о создании и настройке задачи удаленной установки приведена в *Справке Kaspersky Security Center*.

11. Запустите задачу удаленной установки Kaspersky Embedded Systems Security для Windows.

Программа Kaspersky Embedded Systems Security для Windows будет установлена на указанные в задаче защищаемые устройства.

## Действия после установки Kaspersky Embedded Systems Security для Windows

После установки Kaspersky Embedded Systems Security для Windows рекомендуется обновить базы Kaspersky Embedded Systems Security для Windows на устройствах, а также выполнить Проверку важных областей устройств, если до установки Kaspersky Embedded Systems Security для Windows на устройствах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если защищаемые устройства, на которых установлена программа Kaspersky Embedded Systems Security для Windows, объединены в одну группу администрирования в Kaspersky Security Center, можно выполнить эти задачи следующими способами:

1. Создать задачу Обновление баз программы для группы защищаемых устройств, на которых установлена программа Kaspersky Embedded Systems Security для Windows. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
2. Создать групповую задачу проверки по требованию со статусом Проверка важных областей. Kaspersky Security Center оценивает состояние безопасности каждого защищаемого устройства группы по результатам выполнения этой задачи, а не по результатам задачи Проверка важных областей.

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

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security для Windows.

## Установка Консоли программы через Kaspersky Security Center

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

► *Чтобы установить Консоль программы с помощью задачи удаленной установки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.
2. Разверните вложенный узел **Удаленная установка**.
3. В панели результатов вложенного узла Инсталляционные пакеты нажмите на кнопку **Создать инсталляционный пакет**. При создании нового инсталляционного пакета:
   a. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет для указанного исполняемого файла** в качестве типа пакета.
   b. Введите имя инсталляционного пакета.
   c. В папке комплекта поставки Kaspersky Embedded Systems Security для Windows выберите файл \console\setup.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.
   d. Чтобы установить Консоль программы, в поле **Параметры запуска исполняемого файла (необязательно)** укажите ключ командной строки ADDLOCAL. Консоль программы устанавливается в папку установки по умолчанию. Укажите параметр "EULA=1". В противном случае установка компонентов невозможна.

      ```
      /s /p "ADDLOCAL=MmcSnapin EULA=1"
      ```

      При необходимости в поле **Параметры запуска исполняемого файла (необязательно)** можно указать параметр командной строки ADDLOCAL, чтобы изменить набор устанавливаемых компонентов, и параметр командной строки INSTALLDIR, чтобы указать папку назначения, отличную от заданной по умолчанию. Например, чтобы выполнить автономную установку Консоли программы в папку C:\KasperskyConsole, используйте следующие ключи командной строки:

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

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

   Подробная информация о создании и настройке задач удаленной установки приведена в Справке Kaspersky Security Center.

5. Запустите задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче защищаемые устройства.

## Удаление Kaspersky Embedded Systems Security для Windows через Kaspersky Security Center

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security для Windows. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 215).
Если доступ к управлению Kaspersky Embedded Systems Security для Windows на устройствах сети защищен паролем, введите пароль при создании задачи удаления нескольких программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, программа Kaspersky Embedded Systems Security для Windows будет успешно удалена с устройств, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Программа Kaspersky Embedded Systems Security для Windows не будет удалена с других защищаемых устройств.

► *Чтобы удалить Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программы.
2. В задаче выберите метод удаления (аналогично выбору метода установки, см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к защищаемым устройствам. Вы можете удалить Kaspersky Embedded Systems Security для Windows только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 49).

# Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory, а также информацию о действиях, которые требуется выполнить после установки Kaspersky Embedded Systems Security для Windows через групповые политики.

### В этом разделе

Установка Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory ..... 85

Действия после установки Kaspersky Embedded Systems Security для Windows ..... 86

Удаление Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory ..... 86

kaspersky

# Установка Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory

Вы можете установить Kaspersky Embedded Systems Security для Windows на несколько защищаемых устройств с помощью групповой политики Active Directory. Консоль программы можно установить аналогичным образом.

Защищаемые устройства, на которые вы хотите установить Kaspersky Embedded Systems Security для Windows или Консоль программы, должны находиться в одном домене и в одной организационной единице.

Операционные системы защищаемых устройств, на которые вы хотите установить Kaspersky Embedded Systems Security для Windows с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Embedded Systems Security для Windows, используйте пакет установки ess_x86.msi или ess_x64.msi. Чтобы установить Консоль программы, используйте пакет установки esstools.msi

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

► *Чтобы установить Kaspersky Embedded Systems Security для Windows (Консоль программы), выполните следующие действия:*

1. Сохраните msi-файл, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папку общего доступа на контроллере домена.
2. Сохраните файл ключа (см. раздел "О файле ключа" на стр. 95) в эту же общую папку на контроллере домена.
3. В этой же папке общего доступа на контроллере домена создайте файл install_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

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

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

Программа Kaspersky Embedded Systems Security для Windows будет установлена на защищаемые устройства группы после их перезагрузки.

## Действия после установки Kaspersky Embedded Systems Security для Windows

После установки Kaspersky Embedded Systems Security для Windows на защищаемых устройствах рекомендуется сразу обновить базы программы и выполнить проверку важных областей компьютера. Эти действия (см. раздел "Действия после установки Kaspersky Embedded Systems Security для Windows" на стр. 65) можно выполнить из Консоли программы.

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security для Windows.

## Удаление Kaspersky Embedded Systems Security для Windows через групповые политики Active Directory

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security для Windows. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 215).

Если вы установили Kaspersky Embedded Systems Security для Windows или Консоль программы в группе защищаемых устройств, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Embedded Systems Security для Windows или Консоль программы.

Вы можете удалить программу 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 Embedded Systems Security для Windows через групповые политики Active Directory невозможно.

► *Чтобы удалить Kaspersky Embedded Systems Security для Windows (или Консоль программы), выполните следующие действия:*

1. На контроллере домена выберите организационную единицу, с защищаемых устройств которой вы хотите удалить Kaspersky Embedded Systems Security для Windows или Консоль программы.
2. Выберите политику, созданную для установки Kaspersky Embedded Systems Security для Windows, и в **Редакторе объектов групповых политик**, в узле **Установка программ** (**Конфигурация компьютеров** > **Параметры программ** > **Установка программ**) откройте контекстное меню пакета установки Kaspersky Embedded Systems Security для Windows (Консоли программы) и выберите команду **Все задачи** > **Удалить**.

3. Выберите метод удаления **Немедленно удалить программы из учетных записей пользователей и компьютеров**.
4. Примените изменения с помощью команды `gpupdate /force`.

Программа Kaspersky Embedded Systems Security для Windows будет удалена с защищаемых устройств после их перезагрузки, перед входом в Microsoft Windows.

# Проверка функций Kaspersky Embedded Systems Security для Windows. Использование тестового вируса EICAR

В этом разделе описан тестовый вирус EICAR и его использование для проверки функций постоянной защиты файлов и проверки по требованию Kaspersky Embedded Systems Security для Windows.

## В этом разделе

О тестовом вирусе EICAR ..... 87
Проверка функций постоянной защиты файлов и проверки по требованию ..... 88

## О тестовом вирусе EICAR

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

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

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

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

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Embedded Systems Security для Windows обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный или обнаруживаемый** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы и в журнале выполнения задачи.

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

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

*Таблица 6. Префиксы в файлах EICAR*

| Префикс | Статус файла после проверки и действие Kaspersky Embedded Systems Security для Windows |
|---|---|
| Без префикса | Kaspersky Embedded Systems Security для Windows присваивает объекту статус **Зараженный или обнаруживаемый** и удаляет его. |
| SUSP– | Kaspersky Embedded Systems Security для Windows присваивает статус **Возможно зараженный** объекту, обнаруженному с помощью эвристического анализатора, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению. |
| WARN– | Kaspersky Embedded Systems Security для Windows присваивает статус **Возможно зараженный** объекту, если код объекта частично совпадает с кодом известной угрозы, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению. |
| CURE– | Kaspersky Embedded Systems Security для Windows присваивает объекту статус **Зараженный или обнаруживаемый** и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE". |

## Проверка функций постоянной защиты файлов и проверки по требованию

После установки Kaspersky Embedded Systems Security для Windows вы можете убедиться, что Kaspersky Embedded Systems Security для Windows обнаруживает объекты, содержащие вредоносный код. Для этого можно использовать тестовый вирус EICAR (см. раздел "О тестовом вирусе EICAR" на стр. 87).

► *Чтобы проверить функцию постоянной защиты файлов, выполните следующие действия:*

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

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

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что Служба сообщений Microsoft Windows включена на защищаемом устройстве и на устройстве, на котором сохранен файл eicar.com.
3. Открыть Консоль программы на защищаемом устройстве.
4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого устройства одним из следующих способов:
   - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на защищаемое устройство, подключившись к защищаемому устройству с помощью программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).
   - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с устройства, на котором вы его сохранили, через сетевое окружение этого устройства.

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

- Файл eicar.com удален с защищаемого устройства.
- В Консоли программы журналу выполнения задачи (см. раздел "О журналах выполнения задач" на стр. 261) присвоен статус *Критический*. В журнале появилась строка с информацией об угрозе в файле eicar.com.
- На устройстве, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: `Программа Kaspersky Embedded Systems Security для Windows заблокировала доступ к <путь к файлу eicar.com на устройстве>\eicar.com на компьютере <сетевое имя устройства> в <время возникновения события>. Причина: обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <имя пользователя>. Имя компьютера: <сетевое имя устройства, с которого вы скопировали файл>.`

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

► *Чтобы проверить функцию проверки по требованию, выполните следующие действия:*

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

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

2. Откройте Консоль программы (см. раздел "Запуск Консоли Kaspersky Embedded Systems Security для Windows из меню Пуск" на стр. 284) и разверните узел **Проверка по требованию** в дереве Консоли программы.
3. Выберите вложенный узел **Проверка важных областей**.
4. На закладке **Настройка области проверки** откройте контекстное меню узла **Сетевое окружение** и выберите пункт **Добавить сетевой файл**.
5. Введите сетевой путь к файлу eicar.com на удаленном устройстве в формате UNC (Universal Naming Convention).
6. Установите флажок **Путь к объекту**, чтобы включить добавленный сетевой путь в область проверки.
7. Запустите задачу Проверка важных областей.

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

- Файл eicar.com удален с жесткого диска устройства.
- В Консоли программы журналу выполнения задачи (см. раздел "О журналах выполнения задач" на стр. 261) присвоен статус *Критический*. В журнале выполнения задачи проверки важных областей появилась строка с информацией об угрозе в файле eicar.com.

# Интерфейс программы

Программой Kaspersky Embedded Systems Security для Windows можно управлять с помощью следующих интерфейсов:

- Локальная Консоль программы.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

### Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Embedded Systems Security для Windows, а также настраивать параметры программы, изменять набор доступных компонентов программы, добавлять ключи, запускать и останавливать задачи.

Программой можно управлять из Kaspersky Security Center с помощью плагина управления Kaspersky Embedded Systems Security для Windows. Подробная информация об интерфейсе Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

### Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (далее также Веб-консоль) – это веб-приложение, предназначенное для централизованного выполнения основных задач по управлению и поддержке системы безопасности сети организации. Веб-консоль – это компонент Kaspersky Security Center, обеспечивающий пользовательский интерфейс. Подробная информация о Kaspersky Security Center Web Console приведена в *справке Kaspersky Security Center*.

Kaspersky Security Center Cloud Console (далее также Облачная консоль) – это облачное решение для защиты и управления сетью организации. Подробная информация о Kaspersky Security Center Cloud Console приведена в *справке Kaspersky Security Center Cloud Console*.

Веб-консоль и Облачная консоль позволяют выполнять следующие действия:

- Контролировать состояние системы безопасности организации.
- Устанавливать программы "Лаборатории Касперского" на устройства в сети.
- Управлять установленными приложениями.
- Просматривать отчеты о состоянии системы безопасности.

# Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

## В этом разделе


О Лицензионном соглашении ... 92
О лицензии ... 93
О Лицензионном сертификате ... 94
О ключе ... 94
О файле ключа ... 95
О коде активации ... 95
О предоставлении данных ... 95
Активация программы с помощью файла ключа ... 101
Активация программы с помощью кода активации ... 102
Просмотр информации о действующей лицензии ... 103
Функциональные ограничения после окончания срока действия лицензии ... 106
Продление срока действия лицензии ... 106
Удаление ключа ... 107


## О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности, описывающих обработку и передачу данных, следующими способами:

- Во время установки Консоли Kaspersky Embedded Systems Security для Windows (см. раздел "Установка Kaspersky Embedded Systems Security для Windows" на стр. 58).
- Из меню **Пуск** (**Все программы** > **Kaspersky Embedded Systems Security для Windows** > **Лицензионное соглашение и Политика конфиденциальности**) после установки.
- Во время установки Kaspersky Fraud Prevention Cloud.

- Ознакомившись с документом license.txt, входящим в комплект поставки (на стр. 25).
- На сайте "Лаборатории Касперского" (https://www.kaspersky.ru/business/eula https://www.kaspersky.ru/business/eula).

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

# О лицензии

*Лицензия* – это ограниченное по времени право на использование программы, предоставляемое на основе Лицензионного соглашения.

Действующая лицензия дает право на использование программы в соответствии с условиями Лицензионного соглашения, а также на получение технической поддержки при необходимости.

Объем услуг и срок использования программы зависит от типа лицензии, используемой для активации программы.

Программу можно активировать двумя способами:

- С помощью файла ключа, дающего право на использование программы в рамках коммерческой лицензии.
- С помощью кода активации для приобретения коммерческой лицензии.

Можно приобрести стандартную лицензию Kaspersky Embedded Systems Security для Windows или расширенную лицензию Kaspersky Embedded Systems Security для Windows Compliance Edition, распространяющуюся на два дополнительных компонента системы: Мониторинг файловых операций и Анализ журналов.

По истечении срока действия коммерческой лицензии программа продолжает работать, но следующие функции становятся недоступными:

- Интеграция с Kaspersky Security Network.
- Обновление баз Kaspersky Embedded Systems Security для Windows.

Если удалить лицензионный ключ, программа продолжит работать. Задачи **Проверка по требованию** и **Постоянная защита файлов** останутся доступными, а все остальные задачи и обновление баз Kaspersky Embedded Systems Security для Windows станут недоступны. То же самое произойдет, если "Лаборатория Касперского" добавит вашу лицензию в список запрещенных.

Чтобы продолжить использование Kaspersky Embedded Systems Security для Windows в режиме полной функциональности, вам нужно продлить срок действия вашей лицензии.

Рекомендуется продлевать срок действия лицензии до истечения срока ее действия, чтобы обеспечить максимальную защиту устройства.

Убедитесь, что срок действия дополнительного ключа длиннее, чем у активного.

# О Лицензионном сертификате

*Лицензионный сертификат* – это документ, который передается вам вместе с файлом ключа или кодом активации (если применимо).

В Лицензионном сертификате содержится следующая информация о текущей лицензии:

- номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройства, на которых можно использовать программу с предоставленной лицензией);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- Тип лицензии.

# О ключе

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

Вы можете добавить ключ в программу с помощью файла ключа. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Специалисты "Лаборатории Касперского" могут поместить ключ в список запрещенных ключей из-за нарушения Лицензионного соглашения. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

Ключ может быть активным и дополнительным.

*Активный ключ* – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для коммерческой или пробной лицензии. В программе не может быть больше одного активного ключа.

*Дополнительный ключ* – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

# О файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Embedded Systems Security для Windows или после заказа пробной версии Kaspersky Embedded Systems Security для Windows.

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

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

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

# О коде активации

*Код активации* – уникальная последовательность из 20 символов (букв и цифр). Вам нужно ввести код активации, чтобы добавить ключ для активации Kaspersky Embedded Systems Security для Windows. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Embedded Systems Security для Windows или при заказе пробной версии Kaspersky Embedded Systems Security для Windows.

Чтобы активировать программу с помощью кода активации, необходим доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Можно восстановить утерянный после установки программы код активации. Код активации может понадобиться, например, чтобы зарегистрировать Kaspersky CompanyAccount. Чтобы восстановить код активации, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

# О предоставлении данных

Лицензионное соглашение для Kaspersky Embedded Systems Security для Windows, в частности, раздел "Условия обработки данных", определяет условия, ответственность и порядок передачи и обработки данных, указанных в настоящем Руководстве. Внимательно ознакомьтесь с условиями Лицензионного соглашения, а также со всеми документами, ссылки на которые содержит Лицензионное соглашение, перед тем, как принять его.

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

Условия Лицензионного соглашения и Политики конфиденциальности доступны при установке Kaspersky Embedded Systems Security для Windows (см. раздел "Установка Kaspersky Embedded Systems Security для Windows" на стр. 58) в составе комплекта поставки (см. раздел "Комплект поставки" на стр. 25), а также из меню **Пуск** после установки программы (**Все программы** > **Kaspersky Embedded Systems Security для Windows** > **Лицензионное соглашение и Политика конфиденциальности**).

При удалении Kaspersky Embedded Systems Security для Windows будут удалены все данные Kaspersky Embedded Systems Security для Windows, хранящиеся на защищаемом устройстве.

Принимая условия Лицензионного соглашения, вы соглашаетесь отправлять в автоматическом режиме следующие данные в "Лабораторию Касперского":

- Для обеспечения механизма получения обновлений - информацию об установленной программе и активации программы: идентификатор устанавливаемой программы и ее полную версию, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, идентификатор задачи обновления.
- Для использования возможности перехода на статьи Базы знаний при возникновении ошибок в работе программы (служба Redirector) – данные о программе и ссылке: название, локализацию и полный номер версии программы, тип перенаправляющей ссылки, а также идентификатор возникшей ошибки.
- Для контроля получения согласий на обработку данных – информацию о статусе согласия с условиями Лицензионного соглашения и других документов, регламентирующих отправку данных: идентификатор и версия Лицензионного соглашения или другого документа, в рамках которого выполняется согласие с условиями обработки данных или отзыв согласия; признак, указывающий на действие пользователя (подтверждение согласия с условиями или отзыв согласия); дата и время изменения статуса согласия с условиями обработки данных.

**Локальная обработка данных**

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Embedded Systems Security для Windows локально обрабатывает и хранит набор данных на защищаемом устройстве.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security для Windows данных, содержащихся в отчетах.

*Таблица 7. Обработка и хранение данных, содержащихся в отчетах*

| | |
|---|---|
| Функциональная область | Запись событий (см. раздел "Запись событий. Журналы Kaspersky Embedded Systems Security для Windows" на стр. 257) |
| Тип использования | Kaspersky Embedded Systems Security для Windows хранит данные локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о событиях программы, произошедших на управляемых защищаемых устройствах. |
| Хранилище | • %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security для Windows\<версия продукта>\Reports<br>• %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx<br>• База данных Сервера администрирования |

| | |
|---|---|
| Меры безопасности | Список контроля доступа (Access-control list). |
| Период хранения | Kaspersky Embedded Systems Security для Windows хранит данные до момента удаления Kaspersky Embedded Systems Security для Windows.<br>При удалении Kaspersky Embedded Systems Security для Windows будут удалены все данные Kaspersky Embedded Systems Security для Windows, хранящиеся на защищаемом устройстве. |
| Назначение | Обеспечение основных функций. |

Kaspersky Embedded Systems Security для Windows не удаляет события в журнале событий Windows, в том числе события, произошедшие во время удаления Kaspersky Embedded Systems Security для Windows.

Чтобы обеспечить функцию регистрации событий, Kaspersky Embedded Systems Security для Windows локально обрабатывает следующие данные:

- Имена, контрольные суммы (MD5, SHA-256) и атрибуты обрабатываемых файлов и полные пути к ним на проверяемом носителе.
- Действия, выполняемые над проверяемыми файлами программой Kaspersky Embedded Systems Security для Windows.
- Действия, выполняемые пользователями над проверяемыми файлами на защищаемом устройстве.
- Информация об учетных записях пользователей, выполняющих действия в защищаемой сети или на защищаемом устройстве.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о процессах и скриптах, запущенных в системе: контрольные суммы (MD5, SHA-256) и полные пути к исполняемым файлам, информация о цифровых сертификатах.
- Параметры брандмауэра Windows.
- Записи журнала событий Windows.
- Имена учетных записей пользователей, выполняющих действия над проверяемыми файлами на защищаемом устройстве.
- Экземпляры запущенных исполняемых файлов, а также типы, имена, контрольные суммы и атрибуты этих файлов.

- Информация о сетевой активности:
  - IP-адреса заблокированных внешних устройств.
  - Обработанные IP-адреса.
- Информация о статусе USN-журнала Windows.

В следующей таблице приведена информация о служебных данных, обрабатываемых Kaspersky Embedded Systems Security для Windows. Служебные данные включают: параметры программы, файлы на карантине и в резервном хранилище, информацию в сервисных базах данных программы, данные лицензирования.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security для Windows данных о параметрах, указанных пользователями.

*Таблица 8. Обработка и хранение данных о параметрах, указанных пользователями*

| | |
|---|---|
| Функциональная область | Все функции Kaspersky Embedded Systems Security для Windows |
| Тип использования | Kaspersky Embedded Systems Security для Windows хранит данные локально и передает данные на Сервер администрирования. Данные хранятся в базе данных Сервера администрирования.<br>Данные, обрабатываемые программой локально, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы. |
| Хранилище | • %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security для Windows\<версия продукта>\<br>• База данных Сервера администрирования |
| Меры безопасности | Список контроля доступа (Access-control list). |
| Период обработки | Kaspersky Embedded Systems Security для Windows хранит данные до момента удаления Kaspersky Embedded Systems Security для Windows.<br>При удалении Kaspersky Embedded Systems Security для Windows будут удалены все данные Kaspersky Embedded Systems Security для Windows, хранящиеся на защищаемом устройстве.<br>Kaspersky Embedded Systems Security для Windows не удаляет данные о параметрах, экспортируемых в конфигурационный файл.<br>Kaspersky Embedded Systems Security для Windows не удаляет объекты на карантине и в резервном хранилище, если установлены флажки **Экспортировать объекты на карантине** и **Экспортировать объекты резервного хранилища** в мастере установки. |
| Назначение | Обеспечение основных функций. |

Для заявленных целей Kaspersky Embedded Systems Security для Windows локально обрабатывает следующие данные:

- Объекты, помещенные на карантин и в резервное хранилище.
- Информация об учетных записях пользователей (имена пользователей и пароли), с правами которых запускаются задачи Kaspersky Embedded Systems Security для Windows.
- Пароль Kaspersky Embedded Systems Security для Windows.

- IP-адреса и идентификаторы заблокированных сеансов входа.
- Параметры брандмауэра Windows и параметры правил брандмауэра Windows.
- Контрольные суммы (MD5, SHA-256) и пути к исполняемым файлам, добавленным в правила задачи Контроль запуска программ.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о файлах и папках, включенных в области задач Kaspersky Embedded Systems Security для Windows.
- IP-адреса, включенные или исключенные из области защиты.
- Информация о событиях в журнале событий Windows.
- Информация об объектах, обнаруженных с использованием технологий iSwift и iChecker.
- Контрольные суммы (MD5, SHA-256), полные пути и маски, указанные в параметрах исключений.
- Информация о процессах, добавленных в Доверенную зону.
- Информация о добавленных лицензионных ключах.
- Информация о цифровых сертификатах.
- Файлы, распакованные из архива или другого составного объекта во время проверки.

Kaspersky Embedded Systems Security для Windows обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий программы и получения диагностических данных. Защита локально обрабатываемых данных выполняется в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Embedded Systems Security для Windows позволяет настроить уровень защиты данных, обрабатываемых локально (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security для Windows" на стр. 291, "Запись событий. Журналы Kaspersky Embedded Systems Security для Windows" на стр. 257). Вы можете изменять права пользователей на доступ к обрабатываемым данным, изменять сроки хранения таких данных, частично или полностью отключать функциональность, в рамках которой выполняется регистрация данных, а также изменять путь к папке, в которую выполняется запись данных, и ее атрибуты.

Данные, обрабатываемые программой локально, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые программой в ходе работы, удаляются после удаления Kaspersky Embedded Systems Security для Windows с защищаемого устройства.

Исключение составляют файлы с диагностической информацией (файлы трассировки и файлы дампов), файлы журнала событий Windows с событиями программы и файлы с экспортированными параметрами Kaspersky Embedded Systems Security для Windows. Рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные программы, в соответствующих разделах настоящего Руководства.

Вы можете удалить файлы журнала Windows с программными событиями Kaspersky Embedded Systems Security для Windows стандартными средствами операционной системы.

**Локальная обработка данных вспомогательными компонентами программы**

В пакет установки Kaspersky Embedded Systems Security для Windows включены вспомогательные компоненты программы, которые могут быть установлены на устройстве, даже если на нем не установлена программа Kaspersky Embedded Systems Security для Windows. К таким вспомогательным компонентам относятся:

- Консоль локального управления программой. Компонент входит в состав Средств администрирования Kaspersky Embedded Systems Security для Windows и представляет собой оснастку Microsoft Management Console.
- Плагин управления. Компонент обеспечивает полноценную интеграцию с программой Kaspersky Security Center.

При выполнении основных функций программы, описанных в настоящем Руководстве, вспомогательные компоненты программы локально обрабатывают и хранят набор данных на защищаемом устройстве, на котором они установлены, даже если они установлены отдельно от Kaspersky Embedded Systems Security для Windows.

Компоненты программы локально обрабатывают и хранят следующие данные:

- Консоль программы: имя защищаемого устройства с установленной программой Kaspersky Embedded Systems Security для Windows (IP-адрес или доменное имя), к которому в последний раз выполнялось удаленное подключение через Консоль программы; настроенные параметры отображения в оснастке Microsoft Management Console; данные о последней папке, в которой пользователь выполнял выбор объектов посредством Консоли программы (через системный диалог, открывающийся по кнопке **Обзор**). Файлы трассировки Консоли программы могут содержать следующие данные: имя защищаемого устройства с установленной программой Kaspersky Embedded Systems Security для Windows, к которому выполнялось удаленное подключение; имя учетной записи, с правами которой выполнялось удаленное подключение.
- Плагин управления может обрабатывать и временно хранить данные, обрабатываемые Kaspersky Embedded Systems Security для Windows, например, настроенные параметры задач и компонентов программы, параметры политик Kaspersky Security Center, данные, передаваемые в сетевых списках.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security для Windows данных, записываемых в файлы дампов и файлы трассировки.

Kaspersky Embedded Systems Security для Windows локально обрабатывает и хранит следующие данные, записанные в файлы дампов и файлы трассировки:

- Информация о действиях, выполняемых программой Kaspersky Embedded Systems Security для Windows на защищаемом устройстве.
- Информация об объектах, обработанных программой Kaspersky Embedded Systems Security для Windows.
- Информация о действиях на защищаемом устройстве, обрабатываемая Kaspersky Embedded Systems Security для Windows.
- Информация об ошибках, возникших во время работы программы Kaspersky Embedded Systems Security для Windows.

Данные, обрабатываемые вспомогательными компонентами программы, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые вспомогательными компонентами программы в ходе работы, удаляются после удаления этих компонентов.

Исключение составляют файлы трассировки вспомогательных компонентов программы. Рекомендуется самостоятельно удалить эти файлы.

**Данные в файлах трассировки и файлах дампов**

Kaspersky Embedded Systems Security для Windows в соответствии с заданными параметрами может записывать отладочную информацию в файлы трассировки в целях предоставления технической поддержки во время работы Kaspersky Embedded Systems Security для Windows.

Файлы дампов программы Kaspersky Embedded Systems Security для Windows формируются операционной системой во время сбоев программы и перезаписываются при следующем сбое.

Файлы трассировки и дампов могут содержать персональные данные пользователей или конфиденциальные данные организации.

Не используйте Kaspersky Embedded Systems Security для Windows на устройствах, для которых передача данных запрещена политикой организации.

По умолчанию Kaspersky Embedded Systems Security для Windows не записывает отладочную информацию.

Файлы трассировки и дампов не отправляются автоматически за пределы устройства, на котором они были сформированы. Содержимое файлов трассировки можно просматривать с помощью стандартных средств просмотра текстовых файлов. Файлы трассировки и дампов хранятся неограниченное время и не удаляются при удалении Kaspersky Embedded Systems Security для Windows.

Отладочная информация может быть полезна для технической поддержки.

Для ограничения доступа к файлам трассировки и дампов никаких специальных механизмов не предусмотрено. Администратор может настроить запись этих данных в защищенную папку.

Путь к папке с файлами трассировки и дампов по умолчанию не задан. Администратор должен указать папку трассировки и дампов, чтобы использовать ее.

В файлах трассировки и дампов могут содержаться следующие данные:

- Информация о действиях, выполняемых программой Kaspersky Embedded Systems Security для Windows на защищаемом устройстве.
- Информация об объектах, обработанных Kaspersky Endpoint Agent.
- Информация об ошибках, возникающих при работе Kaspersky Endpoint Agent.

# Активация программы с помощью файла ключа

Вы можете активировать Kaspersky Embedded Systems Security для Windows с помощью файла ключа.

Если в Kaspersky Embedded Systems Security для Windows уже добавлен активный ключ и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее ключ будет удален.

Если в Kaspersky Embedded Systems Security для Windows уже добавлен дополнительный ключ и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее дополнительный ключ будет удален.

Если в Kaspersky Embedded Systems Security для Windows уже добавлены активный ключ и дополнительный ключ, а вы добавите новый ключ в качестве активного, то новый ключ заменит ранее добавленный активный ключ, а дополнительный ключ не будет удален.

► *Чтобы активировать Kaspersky Embedded Systems Security для Windows с помощью файла ключа, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор**.
4. Выберите файл ключа с расширением key.

   Вы также можете добавить ключ в качестве дополнительного. Для этого установите флажок **Использовать в качестве дополнительного ключа**.

5. Нажмите на кнопку **ОК**.

   Будет применен выбранный файл ключа. Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

# Активация программы с помощью кода активации

Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

Вы можете активировать Kaspersky Embedded Systems Security для Windows с помощью кода активации.

При активации этим способом Kaspersky Embedded Systems Security для Windows отправляет данные на сервер активации для проверки введенного кода:

- В случае успешной проверки кода активации программа будет активирована.
- При сбое проверки кода активации отобразится соответствующее уведомление. В этом случае обратитесь к поставщику, у которого была приобретена лицензия на программу Kaspersky Embedded Systems Security для Windows.
- В случае превышения количества активаций с помощью указанного кода активации, отображается соответствующее уведомление. Процесс активации программы будет прерван, и вам будет предложено обратиться в Службу технической поддержки.

Вы можете активировать Kaspersky Embedded Systems Security для Windows, используя код активации в Консоли программы или создав групповую задачу Активация программы с помощью Плагина управления (см. раздел "Настройка групповых задач в Kaspersky Security Center" на стр. 132) или Веб-плагина (см. раздел "Настройка групповых задач с помощью Веб-плагина" на стр. 201).

► *Чтобы активировать Kaspersky Embedded Systems Security для Windows с помощью кода активации в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить код активации**.
3. В открывшемся окне введите код активации в поле **Код активации**.
   - Чтобы применить код активации для добавления дополнительного ключа, установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы просмотреть информацию о лицензии, нажмите на кнопку **Показать информацию о лицензии**. Информация отобразится в блоке **Информация о лицензии**.
4. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security для Windows отправит информацию о примененном коде активации на сервер активации.

# Просмотр информации о действующей лицензии

**Просмотр информации о лицензии**

Информация о действующей лицензии отображается в панели результатов узла **Kaspersky Embedded Systems Security для Windows** Консоли программы. Ключ может иметь один из следующих статусов:

- **Выполняется проверка статуса лицензии** – программа Kaspersky Embedded Systems Security для Windows проверяет примененный файл ключа или код активации и ожидает ответа о текущем статусе ключа.
- **Дата окончания срока действия лицензии** – программа Kaspersky Embedded Systems Security для Windows активирована до указанной даты и времени. Статус ключа выделен желтым цветом в следующих случаях:
  - До истечения срока действия лицензии остается не более 14 дней, и не добавлен дополнительный ключ.
  - Добавленный ключ помещен в список запрещенных и будет заблокирован.
- **Срок действия лицензии истек** – программа Kaspersky Embedded Systems Security для Windows не активирована, поскольку истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – программа Kaspersky Embedded Systems Security для Windows не активирована, поскольку нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. 92). Статус выделен красным цветом.
- **Ключ добавлен в запрещенный список** – добавленный ключ заблокирован и помещен в список запрещенных ключей специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.

### Просмотр информации о действующей лицензии

► *Чтобы просмотреть информацию о действующей лицензии,*

в дереве Консоли программы разверните узел **Лицензирование**.

В панели результатов узла **Лицензирование** отобразится общая информация о действующей лицензии (см. таблицу ниже).

*Таблица 9. Общая информация о лицензии в узле Лицензирование*

| Поле | Описание |
|---|---|
| **Код активации** | Код активации. Поле заполняется, если вы активируете программу с помощью кода активации. |
| **Статус активации** | Информация о статусе активации программы. В графе **Статус активации** в панели результатов узла **Лицензирование** могут отображаться следующие значения:<br>• **Применено** – если вы активировали программу с помощью кода активации или файла ключа.<br>• **Активация** – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус изменяется на **Применено** после завершения активации программы и обновления содержимого панели результатов узла.<br>• **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач. |
| **Ключ** | Ключ, добавленный для активации программы. |
| **Тип лицензии** | Тип лицензии: коммерческая или пробная. |
| **Дата окончания срока действия** | Дата и время окончания срока действия лицензии, связанной с активным ключом. |
| **Статус кода активации или ключа** | Статус кода активации или ключа: *Активный* или *дополнительный*. |

► *Чтобы просмотреть подробную информацию о лицензии,*

в панели результатов узла **Лицензирование** в контекстном меню строки с информацией о лицензии, которую вы хотите просмотреть, выберите пункт **Свойства**.

В окне **Свойства ключа** на закладке **Общие** отображается подробная информация о действующей лицензии, а на закладке **Дополнительно** – информация о заказчике и контактная информация "Лаборатории Касперского" или партнера, у которого вы приобрели Kaspersky Embedded Systems Security для Windows (см. таблицу ниже).

*Таблица 10. Подробная информация о лицензии в окне Свойства: <Статус кода активации или ключа>*

| Поле | Описание |
|---|---|
| **Закладка** Общие | |
| **Ключ** | Ключ, добавленный для активации программы. |
| **Дата добавления ключа** | Дата добавления ключа в программу. |
| **Тип лицензии** | Тип лицензии: коммерческая или пробная. |
| **Истекает через (сут)** | Количество дней, оставшихся до окончания срока действия лицензии, связанной с активным ключом. |
| **Дата окончания срока действия** | Дата и время окончания срока действия лицензии, связанной с активным ключом. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если программе Kaspersky Embedded Systems Security для Windows не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*. |
| **Программа** | Название программы, активированной с помощью файла ключа или кода активации. |
| **Ограничение на использование ключа** | Ограничение на использование ключа (если есть). |
| **Осуществление технической поддержки** | Информация о том, оказывает ли "Лаборатория Касперского" или ее партнеры техническую поддержку по условиям Лицензионного соглашения. |
| **Закладка** Дополнительно | |
| **Информация о лицензии** | Текущий лицензионный ключ. |
| **Информация о поддержке** | Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется. |
| **Информация о владельце** | Информация о владельце лицензии: имя клиента и название организации, для которой приобретена лицензия. |

# Функциональные ограничения после окончания срока действия лицензии

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

- Останавливаются все задачи, за исключением задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы.
- Невозможно запустить ни одну задачу, кроме задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы. Эти задачи продолжат работать с использованием старых антивирусных баз.
- Функция Защита от эксплойтов ограничена:
  - Процессы защищаются до их перезапуска.
  - Новые процессы нельзя включить в область защиты.

Другие функции (хранилища, журналы, диагностические данные) по-прежнему доступны.

# Продление срока действия лицензии

По умолчанию Kaspersky Embedded Systems Security для Windows уведомляет вас о скором окончании срока действия лицензии за 14 дней до окончания срока действия лицензии. При этом поле **Дата окончания срока действия лицензии** в панели результатов узла **Kaspersky Embedded Systems Security для Windows** выделяется желтым цветом.

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью дополнительного ключа. Это позволяет не прерывать защиту устройства на период после окончания срока действия лицензии и до активации программы по новой лицензии.

► *Чтобы обновить лицензию, выполните следующие действия:*

1. Получите новый файл ключа или код активации.
2. В дереве Консоли программы выберите узел **Лицензирование**.
3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
   - Если вы хотите продлить срок действия лицензии с помощью файла ключа:
     a. Перейдите по ссылке **Добавить ключ**.
     b. В открывшемся окне нажмите на кнопку **Обзор**.
     c. Выберите новый файл ключа с расширением key.
     d. Установите флажок **Использовать в качестве дополнительного ключа**.

- Если вы хотите продлить срок действия лицензии с помощью кода активации:
  a. Перейдите по ссылке **Добавить код активации**.
  b. В открывшемся окне введите приобретенный код активации.
  c. Установите флажок **Использовать в качестве дополнительного кода активации**.

Для применения кода активации необходимо подключение к интернету.

4. Нажмите на кнопку **OK**.

Дополнительный ключ будет добавлен и автоматически станет активным по истечении срока действия текущей лицензии на Kaspersky Embedded Systems Security для Windows.

# Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Embedded Systems Security для Windows добавлен дополнительный ключ, и вы удалите активный ключ, дополнительный ключ автоматически станет активным.

Если вы удалите добавленный ключ, вы можете его восстановить, повторно применив файл ключа.

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

1. В дереве Консоли программы выберите узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** в таблице с информацией о добавленных ключах выберите ключ, который вы хотите удалить.
3. В контекстном меню строки с информацией о выбранном ключе выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

Выбранный ключ будет удален.

kaspersky

# Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Embedded Systems Security для Windows и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

## В этом разделе


Управление Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center ..... 108

Управление параметрами программы ..... 109

Создание и настройка политик ..... 119

Создание и настройка задач в Kaspersky Security Center ..... 128

Отчеты в Kaspersky Security Center ..... 148


## Управление Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security для Windows, объединенными в группу администрирования, с помощью Плагина управления Kaspersky Embedded Systems Security для Windows. Kaspersky Security Center также позволяет отдельно настраивать параметры каждого защищаемого устройства, входящего в группу администрирования.

*Группа администрирования* формируется вручную на стороне Kaspersky Security Center. Группа администрирования включает устройства с установленной программой Kaspersky Embedded Systems Security для Windows, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Embedded Systems Security для Windows на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center.

С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, и параметры запуска локальных системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

  С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- **С помощью окна свойств отдельного устройства**. В окне **Свойства: <Имя защищаемого устройства>** можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры программы, так и параметры всех задач Kaspersky Embedded Systems Security для Windows, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры для группы защищаемых устройств или для отдельных защищаемых устройств.

# Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security для Windows в Kaspersky Security Center Web Console.

## В этом разделе


Навигация ..... 109

Настройка общих параметров программы в Kaspersky Security Center ..... 111

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center ..... 118


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к общим параметрам из политики ..... 110

Переход к общим параметрам из окна свойств программы ..... 110

## Переход к общим параметрам из политики

► *Чтобы открыть параметры программы Kaspersky Embedded Systems Security для Windows из политики, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. Нажмите на кнопку **Настройка** для группы параметров, которую вы хотите настроить.

## Переход к общим параметрам из окна свойств программы

► *Чтобы открыть окно свойств Kaspersky Embedded Systems Security для Windows для отдельного защищаемого устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security 3.3 для Windows**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры Kaspersky Embedded Systems Security 3.3 для Windows**.
7. Перейдите в раздел **Параметры программы**.

kaspersky

# Настройка общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

## В этом разделе


Настройка параметров масштабируемости, интерфейса и проверки в Kaspersky Security Center . 111

Настройка параметров безопасности в Kaspersky Security Center ..... 113

Настройка параметров соединения в Kaspersky Security Center ..... 115

Настройка запуска по расписанию локальных системных задач ..... 116


## Настройка параметров масштабируемости, интерфейса и проверки в Kaspersky Security Center

► *Чтобы выполнить настройку параметров масштабируемости, интерфейса и проверки, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Параметры программы** в подразделе **Масштабируемость, интерфейс и настройки сканирования** нажмите на кнопку **Настройка**.
5. В окне **Дополнительные параметры программы** на закладке **Общие** настройте следующие параметры:
   - В разделе **Параметры масштабируемости** настройте параметры, определяющие количество процессов, которые использует Kaspersky Embedded Systems Security для Windows:
     - **Определять параметры масштабируемости автоматически**

       Kaspersky Embedded Systems Security для Windows автоматически регулирует количество используемых процессов.

       Это значение установлено по умолчанию.

- **Указать количество рабочих процессов вручную**

  Kaspersky Embedded Systems Security для Windows контролирует количество активных рабочих процессов в соответствии с указанными значениями.

  - **Количество процессов для постоянной защиты**

    Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

  - **Количество процессов для фоновых задач проверки по требованию**

    Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

- В разделе **Взаимодействие с пользователем** настройте отображение Значка области уведомлений в панели задач: снимите или установите флажок **Показывать Значок области уведомлений**.

6. На закладке **Сканирование** настройте следующие параметры:

- **Восстанавливать атрибуты файлов после сканирования**

  Когда Kaspersky Embedded Systems Security для Windows выполняет задачи Проверка по требованию и Постоянная защита файлов, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Embedded Systems Security для Windows возвращает исходное значение времени последнего обращения к файлу.

  Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.

  По умолчанию эта функция включена.

- **Ограничивать сканирующие потоки в использовании ЦП**

  Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.

  Включение этой опции может негативно сказаться на производительности Kaspersky Embedded Systems Security для Windows.

  По умолчанию эта опция выключена.

  - **Предельное значение (в процентах)**

    Максимально допустимое значение загрузки процессора программой Kaspersky Embedded Systems Security для Windows.

    Это поле доступно, если выбран параметр **Ограничивать сканирующие потоки в использовании ЦП**.

    Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.

    Включение этой опции может негативно сказаться на производительности Kaspersky

Embedded Systems Security для Windows.

По умолчанию эта опция выключена.

- **Папка для временных файлов, создаваемых при сканировании**

  Папка, в которую программа Kaspersky Embedded Systems Security для Windows распаковывает файлы архивов при проверке.

  По умолчанию используется папка C:\Windows\Temp.

7. На закладке **Иерархическое хранилище** выберите вариант доступа к иерархическому хранилищу.
8. Нажмите на кнопку **OK**.

Настроенные параметры программы будут сохранены.

## Настройка параметров безопасности в Kaspersky Security Center

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Параметры программы** в подразделе **Настройка** нажмите на кнопку **Безопасность и надежность**.
5. В окне **Параметры безопасности** настройте следующие параметры:
   - В разделе **Параметры применения пароля** включите или отключите функцию **Защищать процессы программы от внешних угроз**.
   - В разделе **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows.
   - В разделе **Самозащита** настройте параметры восстановления задач Kaspersky Embedded Systems Security для Windows в случае сбоев в работе программы или аварийного завершения работы программы.
     - **Выполнять восстановление задач**

       Флажок включает или выключает восстановление задач Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.

Если флажок установлен, Kaspersky Embedded Systems Security для Windows автоматически восстанавливает задачи Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.

Если флажок снят, Kaspersky Embedded Systems Security для Windows не восстанавливает задачи Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.

По умолчанию флажок установлен.

- **Параметры надежности**

  Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Embedded Systems Security для Windows. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.

- В разделе **Выполнять восстановление задач проверки по требованию не более (раз)** задайте ограничение нагрузки на защищаемое устройство со стороны Kaspersky Embedded Systems Security для Windows при переходе на источник бесперебойного питания:

  - **Не запускать задачи проверки по расписанию**

    Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.

    Если флажок установлен, Kaspersky Embedded Systems Security для Windows не запускает задачи проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.

    Если флажок снят, Kaspersky Embedded Systems Security для Windows запускает задачи проверки по расписанию вне зависимости от режима питания.

    По умолчанию флажок установлен.

  - **Остановить выполняемые задачи проверки**

    Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

    Если флажок установлен, Kaspersky Embedded Systems Security для Windows останавливает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

    Если флажок снят, Kaspersky Embedded Systems Security для Windows продолжает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.

    По умолчанию флажок установлен.

- В разделе **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows.

6. Нажмите на кнопку **OK**.

Настроенные параметры безопасности и надежности будут сохранены.

## Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security для Windows к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Параметры программы** в подразделе **Настройка** нажмите на кнопку **Параметры соединения**.

   Откроется окно **Параметры соединения**.
5. В окне **Параметры соединения** настройте следующие параметры:
   - В разделе **Параметры прокси-сервера** задайте параметры использования прокси-сервера:
     - **Не использовать прокси-сервер**;

       Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
     - Использовать указанный прокси-сервер;

       Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security для Windows использует параметры прокси-сервера, указанные вручную.
     - **IP-адрес или символьное имя прокси-сервера и номер порта**;
     - **Не использовать прокси-сервер для локальных адресов**.

       Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security для Windows.

       Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security для Windows, происходит напрямую. Прокси-сервер не используется.

       Если флажок снят, для подключения к локальным устройствам используется прокси-сервер.

       По умолчанию флажок установлен.

- В разделе **Параметры аутентификации на прокси-сервере** задайте параметры аутентификации:
  - Выберите параметры аутентификации в раскрывающемся списке.
    - **Не использовать аутентификацию** – проверка подлинности не производится. Этот режим выбран по умолчанию.
    - **Использовать NTLM-аутентификацию** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
    - **Использовать NTLM-аутентификацию с именем пользователя и паролем** – проверка подлинности по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
    - **Использовать имя пользователя и пароль** – проверка подлинности с помощью имени пользователя и пароля.
  - Если требуется, укажите имя пользователя и пароль.
- В разделе **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

6. Нажмите на кнопку **OK**.

Настроенные параметры соединения будут сохранены.

## Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещен политикой.

> Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике. Kaspersky Embedded Systems Security для Windows будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с параметрами расписания по умолчанию.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если защищаемое устройство исключено из группы администрирования, расписание локальных системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию локальных системных задач Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.
2. На закладке **Политики** в контекстном меню политики, для которой вы хотите настроить запуск по расписанию локальных системных задач Kaspersky Embedded Systems Security для Windows для группы защищаемых устройств, выберите пункт **Свойства**.
3. В окне **Свойства: <Имя политики>** выберите раздел **Параметры программы**. В разделе **Запуск локальных системных задач** нажмите на кнопку **Настройка** и выполните одно из следующих действий:
   - Установите флажки **Задачи проверки по требованию** и **Задачи обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
   - Снимите флажки **Задачи проверки по требованию** и **Задачи обновления и копирования обновлений**, чтобы запретить запуск по расписанию перечисленных задач.

   Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.
4. Убедитесь, что настраиваемая политика активна и применена к выбранной группе защищаемых устройств.
5. Нажмите на кнопку **OK**.

Настроенные параметры расписания выбранных задач будут применены.

## Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

► *Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.
5. В окне **Резервное хранилище** на закладке **Параметры хранилищ** настройте следующие параметры резервного хранилища:
   - Если вы хотите задать папку-местоположение резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого устройства или введите полный путь к ней.
   - Чтобы задать максимальный размер резервного хранилища, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.
   - Чтобы задать порог свободного места в резервном хранилище:
     - Укажите значение параметра **Максимальный размер резервного хранилища (МБ)**.
     - Установите флажок **Порог доступного пространства (МБ)**.
     - Укажите минимальное значение свободного места в папке резервного хранилища в мегабайтах.
   - Чтобы указать папку для восстановленных объектов, выполните одно из следующих действий:
     - В разделе **Параметры восстановления объектов** выберите нужную папку на локальном диске защищаемого устройства.
     - Введите имя папки и полный путь к ней в поле **Папка, в которую восстанавливаются объекты**.
6. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие параметры карантина:
   - Чтобы изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого устройства.
   - Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.

- Чтобы задать минимальный объем свободного места в карантине, установите флажки **Максимальный размер карантина (МБ)** и **Порог доступного пространства (МБ)**, затем в поле ввода укажите значение в мегабайтах.
- Чтобы изменить папку, в которую восстанавливаются объекты из карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого устройства.

7. Нажмите на кнопку **OK**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

# Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security для Windows на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security для Windows.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Embedded Systems Security для Windows на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *активная* в Консоли администрирования.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Embedded Systems Security для Windows. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Embedded Systems Security для Windows использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы установили значок 🔒. В этом случае Kaspersky Embedded Systems Security для Windows не использует значения параметров, действовавшие до применения политики. Kaspersky Embedded Systems Security для Windows не применяет значения параметров активной политики, для которых в свойствах политики установлен значок 🔓.

Если политика активна, то значения параметров, отмеченные в политике значком 🔒, отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком 🔓) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком 🔒, также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры задачи Постоянная защита компьютера, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

kaspersky

## В этом разделе

Создание политики ..... 120
Разделы параметров политики Kaspersky Embedded Systems Security для Windows ..... 122
Настройка политики ..... 127

# Создание политики

► *Чтобы создать политику для группы защищаемых устройств, на которых установлена и запущена программа:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для защищаемых устройств которой вы хотите создать политику.
2. В панели результатов выбранной группы администрирования выберите 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 Embedded Systems Security для Windows и нажмите на кнопку **Далее**.
4. В поле **Имя** укажите название групповой политики.

   Имя политики не должно содержать следующие символы: " * < : > ? \ | .
5. Чтобы применить параметры политики, используемые в предыдущей версии программы, выполните следующие действия:
   a. Установите флажок **Использовать параметры политики, созданной для предыдущей версии программы**.
   b. Нажмите на кнопку **Обзор**.
   c. Выберите политику, которую требуется применить.
   d. Нажмите на кнопку **Далее**.
6. В окне **Выбор типа операции** в блоке **Способ создания политики** выберите один из следующих вариантов:
   - **Создать**, чтобы создать политику с заданными по умолчанию параметрами.
   - **Импортировать политику, созданную с помощью Kaspersky Embedded Systems Security для Windows**, чтобы использовать импортированную версию политики в качестве шаблона.

7. В окне **Постоянная защита компьютера** настройте параметры компонентов программы:
   a. Если необходимо, измените заданные по умолчанию параметры компонентов постоянной защиты компьютера:
      i. Нажмите на кнопку **Настройка** в подразделе компонента программы.
      ii. В открывшемся окне настройте параметры компонента.
      iii. Нажмите на кнопку **OK**.
   b. Разрешите или запретите применение параметров компонентов постоянной защиты компьютера на защищаемых устройствах сети:
      - Нажмите на кнопку 🔒, чтобы разрешить настройку параметров компонента программы на защищаемых устройствах сети и запретить применение параметров компонента программы, настроенных в политике.
      - Нажмите на кнопку 🔓, чтобы запретить настройку параметров компонента программы на защищаемых устройствах сети и разрешить применение параметров компонента программы, настроенных в политике.
   c. Нажмите на кнопку **Далее**.
8. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:
   - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.
   - **Неактивная политика**, если 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. 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 Embedded Systems Security для Windows.

# Разделы параметров политики Kaspersky Embedded Systems Security для Windows

### Общие

В разделе **Общие** можно настроить следующие параметры политики:

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

### Уведомление о событиях

В разделе **Уведомление о событиях** можно настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** можно настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

*Таблица 11. Параметры в разделе Параметры программы*

| Раздел | Параметры |
|---|---|
| **Масштабируемость, интерфейс и настройки сканирования** | В подразделе **Масштабируемость, интерфейс и настройки сканирования** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• выбрать автоматическую или ручную настройку параметров масштабирования;<br>• настроить параметры отображения значка программы. |
| **Безопасность и надежность** | В подразделе **Безопасность и надежность** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• настроить параметры запуска задачи;<br>• указать действия программы при переходе защищаемого устройства на источник бесперебойного питания;<br>• включить или выключить защиту функций программы паролем. |
| **Параметры соединения** | В подразделе **Параметры соединения** по кнопке **Настройка** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN:<br>• указать параметры использования прокси-сервера;<br>• указать параметры аутентификации на прокси-сервере. |
| **Запуск локальных системных задач** | В подразделе **Запуск локальных системных задач** по кнопке **Настройка** можно разрешить или запретить запуск следующих локальных системных задач по расписанию, настроенному на защищаемых устройствах:<br>• задачи проверки по требованию;<br>• задачи обновления и копирования обновлений. |

Дополнительные возможности

*Таблица 12. Параметры в разделе Дополнительные возможности*

| Раздел | Параметры |
|---|---|
| **Доверенная зона** | В подразделе **Настройка** по кнопке **Доверенная зона** вы можете настроить следующие параметры применения доверенной зоны:<br>• сформировать список исключений доверенной зоны;<br>• включить или выключить проверку операций резервного копирования файлов;<br>• сформировать список доверенных процессов. |
| **Проверка съемных дисков** | В подразделе **Проверка съемных дисков** по кнопке **Настройка** вы можете настроить параметры проверки съемных дисков. |
| **Права пользователей на управление программой** | В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Embedded Systems Security для Windows. |
| **Права пользователей на управление службой Kaspersky Security Service** | В подразделе **Права пользователей на управление службой Kaspersky Security Service** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security. |
| **Хранилища** | В подразделе **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов:<br>• указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;<br>• настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;<br>• указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;<br>• настроить продолжительность блокировки узлов. |

Постоянная защита компьютера

*Таблица 13. Параметры в разделе Постоянная защита компьютера*

| Раздел | Параметры |
|---|---|
| **Постоянная защита файлов** | В подразделе **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• указать режим защиты объектов;<br>• настроить применение эвристического анализатора;<br>• настроить применение доверенной зоны;<br>• указать область защиты;<br>• задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;<br>• настроить параметры запуска задачи. |
| **Использование KSN** | В подразделе **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• указать действия над объектами, недоверенными в KSN;<br>• настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.<br>Нажмите на кнопку **Положение о KSN**, чтобы принять или отклонить Положение о KSN, а также настроить параметры передачи данных. |
| **Защита от эксплойтов** | В подразделе **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим защиты памяти процессов;<br>• указать действия для снижения рисков эксплуатации уязвимостей;<br>• дополнить и изменить список защищаемых процессов. |

Контроль активности на компьютерах

*Таблица 14. Параметры в разделе Контроль активности на компьютерах*

| Раздел | Параметры |
|---|---|
| **Контроль запуска программ** | В подразделе **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры контроля повторных запусков программ;<br>• указать область применения правил контроля запуска программ;<br>• настроить использование KSN;<br>• настроить параметры запуска задачи. |
| **Контроль устройств** | В подразделе **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры запуска задачи. |

Контроль активности в сети

*Таблица 15. Параметры в разделе Контроль активности в сети*

| Раздел | Параметры |
|---|---|
| **Управление сетевым экраном** | В подразделе **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• настроить правила сетевого экрана;<br>• настроить параметры запуска задачи. |

Диагностика системы

*Таблица 16. Параметры в разделе Диагностика системы*

| Раздел | Параметры |
|---|---|
| **Мониторинг файловых операций** | В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. |
| **Анализ журналов** | В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows. |

Журналы и уведомления

*Таблица 17. Параметры в разделе Журналы и уведомления*

| Раздел | Параметры |
|---|---|
| **Журналы выполнения задач** | В подразделе **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• указать уровень важности регистрируемых событий для выбранных компонентов программы;<br>• указать параметры хранения журналов выполнения задач;<br>• указать параметры интеграции SIEM-системы с Kaspersky Security Center. |
| **Уведомления о событиях** | В подразделе **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и запрещено недоверенное устройство* и *Сетевая сессия добавлена в список недоверенных*;<br>• указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**. |
| **Взаимодействие с Сервером администрирования** | В разделе **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, включая объекты карантина и резервного хранилища, информацию о которых Kaspersky Embedded Systems Security для Windows будет передавать на Сервер администрирования. |

Диагностика сбоев

*Таблица 18. Параметры в разделе Диагностика сбоев*

| Раздел | Параметры |
|---|---|
| **Параметры диагностики сбоев** | В разделе **Параметры диагностики сбоев** можно настроить следующие параметры:<br>• **Включить трассировку** или выключить ее.<br>• Задать **папку файлов трассировки**.<br>• Указать **уровень детализации**.<br>• Указать **максимальный размер файлов трассировки**.<br>• Указать, надо ли **удалять самые старые файлы трассировки**.<br>• Указать **максимальное количество файлов в журнале трассировки**.<br>Одни и те же параметры можно задать как с помощью групповой политики, так и локально. Подробнее о параметрах и их ограничениях см. в описании конфигурации локальных параметров (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 157).Вы можете установить разные значения параметров на локальном устройстве и в групповой политике для нескольких устройств, при этом будут действовать следующие правила:<br>• Параметры групповой политики, настроенные на сервере Kaspersky Security Center, имеют более высокий приоритет, чем локальные параметры.<br>• Параметры групповой политики, настроенные на локальном устройстве, имеют более низкий приоритет, чем локальные параметры. |
| **Параметры файла дампа** | В разделе **Параметры файла дампа** можно настроить следующие параметры:<br>• Указать, надо ли **создавать файл дампа**.<br>• Указать **папку файла дампа**.<br>Одни и те же параметры можно задать как с помощью групповой политики, так и локально. Подробнее о параметрах и их ограничениях см. в описании конфигурации локальных параметров (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 157).Вы можете установить разные значения параметров на локальном устройстве и в групповой политике для нескольких устройств, при этом будут действовать следующие правила:<br>• Параметры групповой политики, настроенные на сервере Kaspersky Security Center, имеют более высокий приоритет, чем локальные параметры.<br>• Параметры групповой политики, настроенные на локальном устройстве, имеют более низкий приоритет, чем локальные параметры. |

**История ревизий**

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

## Настройка политики

► *Чтобы настроить параметры политики, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:
   - Выберите параметр **Свойства** в контекстном меню политики.
   - Перейдите по ссылке **Настроить параметры политики** в панели результатов выбранной политики.
   - Дважды щелкните мышью по нужной политике.
4. На закладке **Общие** в разделе **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
   - **Активная политика**, если вы хотите, чтобы политика применялась на всех защищаемых устройствах, входящих в выбранную группу администрирования.
   - **Неактивная политика**, если вы хотите активировать политику позже на всех защищаемых устройствах, входящих в выбранную группу администрирования.

   Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Embedded Systems Security для Windows.

5. Измените конфигурацию приложения в других разделах политики.

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

6. Нажмите на кнопку **OK**.

Настроенные параметры будут применены в политике.

# Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security для Windows, их создании, настройке параметров выполнения, запуске и остановке.

## В этом разделе


О создании задач в Kaspersky Security Center ..... 128

Создание задачи в Kaspersky Security Center ..... 129

Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера ..... 131

Настройка групповых задач в Kaspersky Security Center ..... 132

Настройка параметров диагностики сбоев в Kaspersky Security Center ..... 143

Работа с расписанием задач ..... 145


## О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов в Kaspersky Security Center:

- Активация программы;
- Копирование обновлений;
- Обновление баз программы;
- Обновление модулей программы;
- Откат обновления баз программы;
- Проверка по требованию;
- Проверка целостности программы;
- Мониторинг целостности файлов на основе эталона;
- Формирование правил контроля запуска программ;
- Формирование правил контроля устройств.

Вы можете создать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**.
- Для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**.
- Для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 116) на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

## Создание задачи в Kaspersky Security Center

► *Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый сервер.
     b. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства и выберите пункт **Свойства**.
     c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, для которой требуется создать задачу.
     c. В панели результатов перейдите на закладку **Задачи** и выберите пункт **Создать задачу**.
   - Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, к которой принадлежат защищаемые устройства.
     c. Выберите защищаемое устройство или произвольный набор защищаемых устройств.
     d. В раскрывающемся списке **Выполнить действие** выберите **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security 3.3 для Windows** выберите тип создаваемой задачи.

3. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно **Настройка**. В зависимости от типа задачи параметры могут различаться.
   - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 572).
   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
     a. Выберите источник обновлений в окне **Источник обновлений**.
     b. Нажмите на кнопку **Настройка параметров соединения**. В окне **Настройка параметров соединения** настройте параметры доступа к прокси-серверу при подключении к источнику обновлений.
   - Для создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Параметры**.
     a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.
     b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Embedded Systems Security для Windows автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.
     c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Embedded Systems Security для Windows, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

        "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.
   - Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Настройка параметров копирования обновлений**.
   - Для создания задачи Активация программы:
     a. В окне **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу.
     b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
   - Создайте задачу Формирование правил контроля запуска программ (см. раздел "Создание задачи Формирование правил контроля запуска программ" на стр. 421).
   - Создайте задачу Формирование правил контроля устройств (см. раздел "Создание правил с помощью задачи Формирование правил контроля устройств" на стр. 468).
4. Настройте расписание задачи (см. раздел "Настройка расписания задач" на стр. 145).

   Вы можете настраивать расписание для всех типов задач, кроме задачи Откат обновления баз программы.
5. Нажмите на кнопку **OK**.

6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.
7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, которую вы хотите использовать для запуска задачи.
8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы " * < > ? \ | :).

   Рекомендуется включить в название задачи ее тип (например, Проверка по требованию общих папок).
9. В окне **Завершение создания задачи** выполните следующие действия:
   a. Установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите запустить задачу сразу после создания.
   b. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

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

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

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

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

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
4. Перейдите в раздел **Задачи**.
5. В списке задач выберите локальную задачу, параметры которой требуется настроить, одним из следующих способов:
   - двойным щелчком мыши на названии задачи;
   - выберите задачу в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени задачи выберите пункт **Свойства**.

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

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

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

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
4. Перейдите в раздел **Программы**.
5. В списке установленных программ выберите Kaspersky Embedded Systems Security для Windows одним из следующих способов:
   - двойным щелчком мыши на имени Kaspersky Embedded Systems Security для Windows;
   - выберите Kaspersky Embedded Systems Security для Windows в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени Kaspersky Embedded Systems Security для Windows выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Embedded Systems Security для Windows**.

## Настройка групповых задач в Kaspersky Security Center

При управлении Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center Cloud Console нельзя вручную добавлять пользовательские HTTP и FTP-серверы или сетевые папки.

► *Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     - В разделе **Область проверки** настройте область проверки.
     - В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
     - В разделе **Настройка** настройте параметры источника обновлений и оптимизации дисковой подсистемы.
     - По кнопке **Настройка параметров соединения** настройте параметры соединения с источником обновлений.
   - Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:
     - Перейдите в раздел **Параметры**.
     - Выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
   - Чтобы настроить задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку назначения.
   - Чтобы настроить задачу Активация программы, выполните следующие действия:
     - В разделе **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу.
     - Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
   - Чтобы настроить задачу автоматического формирования разрешающих правил контроля устройств, в разделе **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.
6. Настройте расписание задачи в разделе **Расписание**. Вы можете настраивать расписание для всех типов задач, кроме задачи Откат обновления баз программы.
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

Настроенные параметры групповых задач будут сохранены.

Настраиваемые параметры групповых задач приведены в следующей таблице.

*Таблица 19. Параметры групповых задач Kaspersky Embedded Systems Security для Windows*

| Типы задач Kaspersky Embedded Systems Security для Windows | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| Формирование правил контроля запуска программ | **Настройка** | При настройке параметров задачи Формирование правил контроля запуска программ вы можете выбрать способ создания разрешающих правил:<br>• **Создавать разрешающие правила на основе запущенных программ**<br>Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.<br>Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.<br>Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.<br>По умолчанию флажок снят.<br>Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.<br>• **Создавать разрешающие правила для программ из папок** |

| Типы задач Kaspersky Embedded Systems Security для Windows | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.<br>• | **Параметры** | Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ:<br>• **Использовать цифровой сертификат**<br>• **Использовать заголовок и отпечаток цифрового сертификата**<br>• **Если сертификат отсутствует, использовать**<br>• **Использовать хеш SHA256**<br>• **Формировать правила для пользователя или группы пользователей**<br>Вы можете настроить параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Embedded Systems Security для Windows создает по завершении задачи. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Формирование правил контроля устройств | **Настройка** | • Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.<br>• Настройте параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Embedded Systems Security для Windows создает по завершении задачи. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Активация программы (см. раздел "Задача Активация программы" на стр. 139) | **Параметры активации** | Вы можете применить файл ключа для активации программы или продления срока действия лицензии. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |

| Типы задач Kaspersky Embedded Systems Security для Windows | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| Копирование обновлений (см. раздел "Задачи обновления" на стр. 140) | **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.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. |
| | Окно **Параметры соединения** | В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами. |
| | **Настройка параметров копирования обновлений** | Вы можете указать состав обновлений для копирования.<br>В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Embedded Systems Security для Windows будет сохранять скопированные обновления. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Обновление баз программы (см. раздел "Задачи обновления" на стр. 140) | **Настройка** | В блоке параметров **Источник обновлений** можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.<br>В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:<br>• **Снизить нагрузку на дисковую подсистему**<br>• **Объем оперативной памяти, используемой для оптимизации (МБ)** |

| Типы задач Kaspersky Embedded Systems Security для Windows | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| • | Окно **Параметры соединения** | В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Обновление модулей программы (см. раздел "Задачи обновления" на стр. 140) | **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.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. |
| | Окно **Параметры соединения** | В блоке параметров **Параметры соединения с источниками обновлений** можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами. |
| | **Параметры** | Вы можете указать действия, которые Kaspersky Embedded Systems Security для Windows будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Embedded Systems Security для Windows получать информацию о доступных плановых обновлениях. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Параметры проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 572) | **Область проверки** | Вы можете сформировать область проверки для задачи проверки по требованию и настроить параметры уровня безопасности. |
| | Окно **Настройка проверки по требованию** | В окне **Настройка проверки по требованию**, доступном из раздела **Область проверки**, вы можете выбрать один из стандартных уровней безопасности или настроить уровень безопасности вручную. |

| Типы задач Kaspersky Embedded Systems Security для Windows | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| | **Параметры** | В блоке параметров **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка.<br>В блоке **Интеграция с другими компонентами** можно настроить следующие параметры:<br>• применение Доверенной зоны в задачах проверки по требованию;<br>• применение служб KSN в задачах проверки по требованию;<br>• указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей. |
| | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Проверка целостности программы (на стр. 142) | **Расписание** | Вы можете настроить расписание запуска задачи. |
| Мониторинг целостности файлов на основе эталона (см. раздел "Настройка задачи Мониторинг целостности файлов на основе эталона" на стр. 587) | **Расписание** | Вы можете настроить расписание запуска задачи. |

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**.

Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

kaspersky

## В этом разделе

Задача Активация программы ..... 139
Задачи обновления ..... 140
Проверка целостности программы ..... 142

## Задача Активация программы

► *Чтобы настроить задачу Активация программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

5. В разделе **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

## Задачи обновления

► *Чтобы настроить задачи Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

5. В разделе **Источник обновлений** выполните следующие действия:
   a. Выберите источник обновлений:
      - Сервер администрирования Kaspersky Security Center.
      - Серверы обновлений "Лаборатории Касперского".
      - Другие HTTP-,FTP-серверы и сетевые ресурсы.

      Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).

      Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

   b. Нажмите на кнопку **Настройка параметров соединения**.
   c. В открывшемся окне **Настройка параметров соединения** настройте использование прокси-сервера для подключения к серверам обновлений "Лаборатории Касперского" и другим серверам.

d. Для задачи Обновление баз программы в разделе **Оптимизация использования дисковой подсистемы** настройте параметры функции, снижающей нагрузку на дисковую подсистему:

> Раздел **Оптимизация использования дисковой подсистемы** доступен только для задачи Обновление баз программы.

- **Снизить нагрузку на дисковую подсистему**

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

  Если флажок установлен, функция активна.

  По умолчанию флажок снят.

- **Объем оперативной памяти, используемой для оптимизации (МБ)**

  Объем оперативной памяти (в МБ), используемый программой для хранения файлов обновлений. По умолчанию задан объем 600 МБ. Минимальный объем составляет 400 МБ.

  При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

  - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении). Это приведет к завершению задачи с ошибкой.

    В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

  - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. Функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

    В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

6. Для задачи Обновление модулей программы в разделе **Параметры** укажите действия, которые Kaspersky Embedded Systems Security для Windows будет совершать при наличии критических обновлений модулей программы или при наличии информации о плановых обновлениях.

   Можно также настроить действия программы Kaspersky Embedded Systems Security для Windows по завершении установки критических обновлений.

   > Раздел **Параметры** доступен только для задачи Обновление модулей программы.

7. Для задачи Копирование обновлений в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку, в которую будут сохранены обновления.

Раздел **Настройка параметров копирования обновлений** доступен только для задачи Копирование обновлений.

8. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
9. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

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

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, контролируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

## Проверка целостности программы

► *Чтобы настроить групповую задачу Проверка целостности программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

5. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу Проверка целостности программы.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

## Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security для Windows возникла проблема (например, аварийное завершение программы), ее можно диагностировать. Для этого можно включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security для Windows и отправить эти файлы на анализ в Службу технической поддержки.

Kaspersky Embedded Systems Security для Windows не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security для Windows. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 131).
2. Откройте раздел **Диагностика сбоев**.
3. Чтобы отладочная информация записывалась в файл, в разделе **Параметры диагностики сбоев** установите флажок **Включить трассировку**.
4. В поле **Папка файлов трассировки** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы трассировки.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

5. Настройте уровень детализации отладочной информации.

   В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки. Параметр доступен, если установлен флажок **Включить трассировку**.

   Вы можете выбрать один из следующих режимов работы задачи:

   - **Полная информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки всю отладочную информацию.
   - **Краткая информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файл трассировки только информацию о критических событиях.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

   По умолчанию установлен уровень детализации **Полная информация**.

6. Укажите **Максимальный размер файлов трассировки (МБ)**.

   Доступные значения: от 1 до 4095 МБ. По умолчанию максимальный размер файлов трассировки составляет 50 МБ.

7. Для удаления самых старых файлов трассировки при достижении максимального количества файлов установите флажок **Использовать вытеснение старых файлов журнала трассировки**.

8. Укажите значение **Максимальное количество файлов журнала трассировки**.

   Доступные значения: от 1 до 999. По умолчанию максимальное количество файлов составляет 5. Поле доступно, если установлен флажок **Использовать вытеснение старых файлов трассировки**.

9. Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.

10. В поле **Папка файлов дампа** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы дампа.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

11. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом устройстве.

kaspersky

# Работа с расписанием задач

Вы можете задать расписание для задач Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Настройка расписания задач ..... 145

Включение и выключение запуска задач по расписанию ..... 147


## Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Плагина управления, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
      - **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).

- **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security для Windows.
- **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату начала действия расписания.

> После того как вы укажете частоту, дату и время запуска задачи, отобразится расчетное время очередного запуска задачи.
> Перейдите на закладку **Расписание** и откройте окно **Параметры задачи**. В поле **Следующий запуск** в верхней части окна отображается расчетное время запуска. Расчетное время следующего запуска задачи обновляется каждый раз, когда вы открываете окно.
> В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 116) запрещен действующей политикой Kaspersky Security Center.

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

> Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131)".

## Включение и выключение запуска задач по расписанию

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

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. Выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

# Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Embedded Systems Security для Windows доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

**Отчет о статусе компонентов Kaspersky Embedded Systems Security для Windows components**

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. Выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 131).
3. Выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

► *Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:*

1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

**Отчеты о запрещенных программах в активном и в тестовом режимах**

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

► *Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 403).

   В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о запрещенных программах в режиме тестирования** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 403).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

kaspersky

# Работа с Консолью Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о Консоли Kaspersky Embedded Systems Security для Windows и об управлении программой через Консоль программы, установленную на защищаемом устройстве или другом устройстве.

## В этом разделе


О Консоли Kaspersky Embedded Systems Security для Windows ..... 151

Интерфейс Консоли Kaspersky Embedded Systems Security для Windows ..... 152

Управление Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на другом устройстве ..... 157

Настройка общих параметров программы в Консоли программы ..... 157

Управление задачами Kaspersky Embedded Systems Security для Windows ..... 163

Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security для Windows ..... 176


# О Консоли Kaspersky Embedded Systems Security для Windows

Консоль Kaspersky Embedded Systems Security для Windows представляет собой изолированную оснастку, которую можно добавить в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

После установки Консоли программы на другое устройство требуется дополнительная настройка.

Консоль программы и Kaspersky Embedded Systems Security для Windows можно установить на разных защищаемых устройствах, принадлежащих к разным доменам. В этом случае возможны ограничения при передаче информации от программы в Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Embedded Systems Security для Windows добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Embedded Systems Security для Windows или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Embedded Systems Security для Windows только в Microsoft Management Console 32-разрядной версии. Чтобы добавить оснастку Kaspersky Embedded Systems Security для Windows, откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security для Windows в Microsoft Management Console, открытую в авторском режиме. Можно управлять защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security для Windows.

# Интерфейс Консоли Kaspersky Embedded Systems Security для Windows

В этом разделе описаны основные элементы интерфейса программы.

## В этом разделе


Окно консоли Kaspersky Embedded Systems Security для Windows ..... 152

Значок области уведомлений в панели задач ..... 156


## Окно консоли Kaspersky Embedded Systems Security для Windows

Консоль Kaspersky Embedded Systems Security для Windows отображается в дереве Microsoft Management Console в виде узла.

После подключения к программе Kaspersky Embedded Systems Security для Windows, установленной на другом защищаемом устройстве, в название узла добавляется имя защищаемого устройства, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Embedded Systems Security <Имя защищаемого устройства> как <имя учетной записи>**. При подключении к программе Kaspersky Embedded Systems Security для Windows, установленной на том же защищаемом устройстве, что и Консоль программы, узел называется **Kaspersky Embedded Systems Security для Windows**.

### Дерево Консоли программы

В дереве Консоли программы отображается узел **Kaspersky Embedded Systems Security для Windows** и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Embedded Systems Security для Windows** содержит следующие вложенные узлы:

- **Постоянная защита компьютера**: управление задачами постоянной защиты компьютеров и службами KSN. Узел **Постоянная защита компьютера** позволяет управлять следующими задачами:
  - **Постоянная защита файлов**
  - **Использование KSN**
  - **Защита от эксплойтов**

- **Контроль компьютера**: контроль программ, запускаемых на защищаемом устройстве, и подключаемых устройств. Узел **Контроль компьютера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Управление сетевым экраном**
- **Автоматическое формирование правил**: настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ и Контроль устройств.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имена задач>** (если есть)

    Групповые задачи (см. раздел "Категории задач Kaspersky Embedded Systems Security для Windows" на стр. 163) создаются с помощью Kaspersky Security Center. Управлять групповыми задачами с помощью Консоли программы невозможно.
- **Диагностика системы**: настройка параметров контроля файловых операций и анализа журнала событий Windows.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка объектов на карантине**
  - **Проверка целостности программы**
  - Пользовательские задачи **<Имена задач>** (если есть)

  В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Embedded Systems Security для Windows" на стр. 163), созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Embedded Systems Security для Windows, а также копированием обновлений в папку локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также последней задачей **Откат обновления баз программы**:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

  В узле отображаются все пользовательские и групповые задачи обновлений (см. раздел "Категории задач Kaspersky Embedded Systems Security для Windows" на стр. 163), сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами карантина и резервного хранилища.
  - **Карантин**
  - **Резервное хранилище**
- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Embedded Systems Security для Windows.
  - **Журнал событий безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование**: добавление и удаление ключей Kaspersky Embedded Systems Security для Windows, просмотр информации о лицензиях.

### Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Embedded Systems Security**, в панели результатов отобразится информация о текущем состоянии защиты устройства (см. раздел "Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security для Windows" на стр. 176), информация о Kaspersky Embedded Systems Security для Windows, состояние защиты функциональных компонентов программы и дата истечения срока действия лицензии.

### Контекстное меню узла Kaspersky Embedded Systems Security

С помощью пунктов контекстного меню узла **Kaspersky Embedded Systems Security** можно выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключиться к другому устройству (см. раздел "Управление Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на другом устройстве" на стр. 157), чтобы управлять установленной на нем программой Kaspersky Embedded Systems Security для Windows. Для выполнения этой операции вы можете также воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security для Windows**.
- **Запустить программу** / **Остановить программу**. Запустить или остановить программу или выбранную задачу (см. раздел "Запуск, приостановка, возобновление, остановка задач вручную" на стр. 164). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настроить проверку съемных дисков**. Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. 563), подключенных к защищаемому устройству по USB.
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны (см. раздел "О доверенной зоне" на стр. 619).
- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Embedded Systems Security для Windows.
- **Изменить права пользователей на управление службой Kaspersky Security**. Просмотреть и настроить права пользователя на управление службой Kaspersky Security (см. раздел "Настройка прав доступа на управление Kaspersky Embedded Systems Security для Windows и службой Kaspersky Security" на стр. 302).
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел "Экспорт параметров" на стр. 170). Выполнение этой операции также доступно в контекстных меню задач программы.

- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла в формате XML (см. раздел "Импорт параметров" на стр. 171). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Embedded Systems Security для Windows и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Embedded Systems Security для Windows или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  Для выполнения этой операции также можно воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Embedded Systems Security для Windows** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Embedded Systems Security для Windows. Выполнение этой операции также доступно в контекстных меню задач программы.

**Панель инструментов и контекстное меню задач Kaspersky Embedded Systems Security для Windows**

Вы можете управлять задачами Kaspersky Embedded Systems Security для Windows с помощью пунктов контекстного меню каждой задачи в дереве Консоли программы.

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

- **Запустить** / **Остановить**. Запустить или остановить (см. раздел "Запуск, приостановка, возобновление, остановка задач вручную" на стр. 164) выполнение задачи. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Возобновить** / **Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел "Запуск, приостановка, возобновление, остановка задач вручную" на стр. 164). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты компьютера и задач проверки по требованию.
- **Добавить задачу**. Создать новую пользовательскую задачу (см. раздел "Создание и настройка задачи проверки по требованию" на стр. 589). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. 261). Операция доступна для всех задач.
- **Удалить задачу**. Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Шаблоны параметров**. Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. 172). Операция доступна для задачи Постоянная защита файлов и задач проверки по требованию.

## Значок области уведомлений в панели задач

Каждый раз, когда Kaspersky Embedded Systems Security для Windows автоматически запускается после перезагрузки защищаемого устройства, в области уведомлений панели задач отображается значок области уведомлений . Он отображается по умолчанию, если при установке программы вы установили компонент Значок области уведомлений.

Вид значка области уведомлений отражает текущее состояние защиты устройства. Возможно два типа состояния:

Активный (цветной значок), если работает минимум одна задача: Постоянная защита файлов, Контроль запуска программ.

Неактивный (серый значок), если не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ.

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

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

*Таблица 20. Команды контекстного меню, отображаемые с помощью значка области уведомлений*

| Команда | Описание |
|---|---|
| **Открыть Консоль управления** | Открывает Консоль Kaspersky Embedded Systems Security для Windows (если она установлена). |
| **Открыть Диагностическое окно** | Открывает Диагностическое окно программы. |
| **О программе** | Открывает окно **О программе** с информацией о Kaspersky Embedded Systems Security для Windows.<br>Для зарегистрированных пользователей Kaspersky Embedded Systems Security для Windows окно **О программе** содержит информацию об установленных срочных обновлениях. |
| **Скрыть** | Скрывает значок области уведомлений в панели задач. |

Скрытый значок области уведомлений можно отобразить в любое время.

► *Чтобы снова отобразить значок области уведомлений,*

в Microsoft Windows в меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security для Windows** > **Значок области уведомлений**.

Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

В общих параметрах Kaspersky Embedded Systems Security для Windows можно включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки защищаемого устройства.

# Управление Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на другом устройстве

Вы можете управлять Kaspersky Embedded Systems Security для Windows через Консоль программы, которая установлена на удаленном устройстве.

Чтобы управление программой с помощью Консоли Kaspersky Embedded Systems Security для Windows, установленной на удаленном устройстве, было доступно, убедитесь, что выполняются следующие условия:

- Пользователи Консоли программы на удаленном устройстве добавлены в группу ESS Administrators на защищаемом устройстве.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management kavfsgt.exe, если на защищаемом устройстве включен брандмауэр Windows.
- Во время установки Kaspersky Embedded Systems Security для Windows в окне мастера установки был установлен флажок **Разрешить удаленный доступ**.

Если программа Kaspersky Embedded Systems Security для Windows на удаленном устройстве защищена паролем, введите пароль для получения доступа к управлению программой с помощью Консоли программы.

# Настройка общих параметров программы в Консоли программы

Общие параметры и параметры диагностики сбоев Kaspersky Embedded Systems Security для Windows определяют общие условия работы программы. Эти параметры позволяют контролировать количество рабочих процессов, используемых Kaspersky Embedded Systems Security для Windows, включать восстановление задач Kaspersky Embedded Systems Security для Windows после их аварийного завершения, вести журнал, включать создание файлов дампов для процессов Kaspersky Embedded Systems Security для Windows при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров программы недоступна из Консоли программы, если изменение данных параметров запрещено активной политикой Kaspersky Security Center.

► *Чтобы настроить параметры Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security для Windows** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. В открывшемся окне настройте общие параметры Kaspersky Embedded Systems Security для Windows согласно вашим требованиям:
   - На вкладке **Масштабируемость и интерфейс** можно настроить следующие параметры:
     - В разделе **Параметры масштабируемости**:
       - Количество процессов для постоянной защиты компьютера

*Таблица 21. Количество процессов для постоянной защиты*

| Параметр | Количество процессов для постоянной защиты |
|---|---|
| **Описание** | Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Embedded Systems Security для Windows.<br>С помощью этого параметра можно задать фиксированное количество процессов, в которых Kaspersky Embedded Systems Security для Windows будет выполнять задачи постоянной защиты компьютера.<br>Более высокое значение повысит скорость проверки объектов в задачах постоянной защиты компьютера. Однако, чем больше процессов задействует Kaspersky Embedded Systems Security для Windows, тем больше будет влияние на общую производительность защищаемого устройства и потребление оперативной памяти.<br>В Консоли администрирования Kaspersky Security Center параметр **Количество процессов для постоянной защиты** можно настроить только для программы Kaspersky Embedded Systems Security для Windows, установленной на отдельном защищаемом устройстве (в окне **Параметры программы**). Нельзя изменить этот параметр в свойствах политики для группы защищаемых устройств. |
| **Возможные значения** | Возможные значения: 1-8.<br>Большее значение позволяет снизить влияние Kaspersky Embedded Systems Security для Windows на скорость обмена данными между устройствами и защищаемым устройством. Таким образом повысится быстродействие задачи постоянной защиты компьютеров. Однако задачи обновления и задачи проверки по требованию с приоритетом *Средний* будут выполняться в уже запущенных рабочих процессах Kaspersky Embedded Systems Security для Windows. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени.<br>Задачи проверки по требованию с приоритетом *Низкий* всегда выполняются в отдельных процессах. |

| | |
|---|---|
| **Значение по умолчанию** | Kaspersky Embedded Systems Security для Windows выполняет масштабирование автоматически в зависимости от количества процессоров защищаемого устройства:<br>**Количество процессоров** — **Количество процессов для постоянной защиты**<br>=1 — 1<br>>1 — 2 |

- Количество рабочих процессов для фоновых задач проверки по требованию

*Таблица 22. Количество процессов для фоновых задач проверки по требованию*

| **Параметр** | **Количество процессов для фоновых задач проверки по требованию** |
|---|---|
| **Описание** | Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Embedded Systems Security для Windows.<br>С помощью этого параметра можно указать максимальное количество процессов, для которых программа будет выполнять задачи проверки по требованию в фоновом режиме.<br>Количество процессов, определяемое этим параметром, не входит в общее количество процессов Kaspersky Embedded Systems Security для Windows, заданное параметром Количество процессов для постоянной защиты сервера.<br>Например, если вы установите следующие значения:<br>• количество процессов для задач постоянной защиты компьютера – 3;<br>• количество процессов для фоновых задач проверки по требованию – 1;<br>а затем запустите задачи постоянной защиты компьютера и одну задачу проверки по требованию в фоновом режиме, общее количество процессов kavfswp.exe для Kaspersky Embedded Systems Security для Windows составит 4.<br>В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию.<br>Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость. |
| **Возможные значения** | 1–4 |
| **Значение по умолчанию** | 1 |

- В разделе **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач при каждом запуске программы (см. раздел "Значок области уведомлений в панели задач" на стр. 156).

- На вкладке **Безопасность и надежность** можно настроить следующие параметры:
  - В разделе **Параметры применения пароля** настройте защиту процессов программы.

    Если функция **Защищать процессы программы от внешних угроз** включена, программа

защищает процессы от внедрения кода и доступа к данным процессов.

При включении или выключении этой функции нет необходимости перезапускать службы программы, чтобы изменения вступили в силу.

Функция включена по умолчанию.

- В разделе **Параметры применения пароля** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля" на стр. 304).
- В разделе **Самозащита** укажите количество попыток восстановления задачи проверки по требованию после ее аварийного завершения.

*Таблица 23. Восстановление задач*

| Параметр | Выполнять восстановление задач |
|---|---|
| **Описание** | Этот параметр относится к группе **Самозащита** Kaspersky Embedded Systems Security для Windows. Он включает восстановление задач в случае их аварийного завершения и устанавливает количество попыток восстановления задач проверки по требованию.<br>Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Embedded Systems Security для Windows пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения.<br>Если восстановление задач выключено, программа не восстанавливает задачи постоянной защиты компьютера и проверки по требованию.<br>Если включено восстановление задач, программа пытается восстановить задачи постоянной защиты компьютера, до тех пор, пока они не будут успешно запущены. Также программа пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром. |
| **Возможные значения** | Включено / выключено.<br>Количество попыток восстановления задач проверки по требованию: 1–10. |
| **Значение по умолчанию** | Восстановление задач включено. Количество попыток восстановления задач проверки по требованию: 2. |

- В разделе **Выполнять восстановление задач проверки по требованию не более (раз)** укажите действия Kaspersky Embedded Systems Security для Windows при переходе на источник бесперебойного питания.

*Таблица 24. Использование источника бесперебойного питания*

| Параметр | Выполнять восстановление задач проверки по требованию не более (раз) |
|---|---|
| **Описание** | Этот параметр определяет действия, которые Kaspersky Embedded Systems Security для Windows выполняет, когда защищаемое устройство переходит на работу от источника бесперебойного питания. |
| **Возможные значения** | Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию.<br>Выполнять или останавливать все выполняемые задачи проверки по требованию. |

| | |
|---|---|
| **Значение по умолчанию** | По умолчанию при работе защищаемого устройства от источника бесперебойного питания Kaspersky Embedded Systems Security для Windows работает в следующем режиме:<br>• не запускает задачи проверки по требованию, которые должны быть запущены по расписанию;<br>• автоматически останавливает все выполняемые задачи проверки по требованию. |

- На вкладке **Сканирование**:
  - **Восстанавливать атрибуты файлов после сканирования**

    Когда Kaspersky Embedded Systems Security для Windows выполняет задачи Проверка по требованию и Постоянная защита файлов, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Embedded Systems Security для Windows возвращает исходное значение времени последнего обращения к файлу.

    Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.

    По умолчанию эта функция включена.

  - **Ограничивать сканирующие потоки в использовании ЦП**

    Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.

    Включение этой опции может негативно сказаться на производительности Kaspersky Embedded Systems Security для Windows.

    По умолчанию эта опция выключена.

  - **Предельное значение (в процентах)**

    Максимально допустимое значение загрузки процессора программой Kaspersky Embedded Systems Security для Windows.

    Это поле доступно, если выбран параметр **Ограничивать сканирующие потоки в использовании ЦП**.

    Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.

    Включение этой опции может негативно сказаться на производительности Kaspersky Embedded Systems Security для Windows.

    По умолчанию эта опция выключена.

  - **Папка для временных файлов, создаваемых при сканировании**

    Папка, в которую программа Kaspersky Embedded Systems Security для Windows распаковывает файлы архивов при проверке.

    По умолчанию используется папка C:\Windows\Temp.

- На вкладке **Параметры соединения**:

- В разделе **Параметры прокси-сервера** укажите параметры прокси-сервера.
- В разделе **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и данные, необходимые для аутентификации на прокси-сервере.
- В разделе **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.

- На вкладке **Диагностика сбоев**:
  - Чтобы отладочная информация записывалась в файл, в разделе **Параметры диагностики сбоев** установите флажок **Включить трассировку**.
  - В поле **Папка трассировки** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы трассировки.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
  - Настройте уровень детализации отладочной информации.

    В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки. Параметр доступен, если установлен флажок **Включить трассировку**.

    Вы можете выбрать один из следующих режимов работы задачи:

    - **Полная информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки всю отладочную информацию.
    - **Краткая информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файл трассировки только информацию о критических событиях.

    Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

    По умолчанию установлен уровень детализации **Полная информация**.
  - Укажите **максимальный размер файлов трассировки**.

    Доступные значения: от 1 до 4095 МБ. По умолчанию максимальный размер файлов трассировки составляет 50 МБ.
  - Для удаления самых старых файлов трассировки при достижении максимального количества файлов установите флажок **Удалять самые старые файлы трассировки**.
  - Укажите **максимальное количество файлов в одном журнале трассировки**.

    Доступные значения: от 1 до 999. По умолчанию максимальное количество файлов составляет 5. Поле доступно, если установлен флажок **Удалять самые старые файлы трассировки**.
  - Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
  - В поле **Папка файлов дампа** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы дампа.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security для Windows. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Embedded Systems Security для Windows будут сохранены.

# Управление задачами Kaspersky Embedded Systems Security для Windows

В этом разделе приведена информация о создании, настройке, запуске и остановке задач Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Категории задач Kaspersky Embedded Systems Security для Windows ..... 163

Запуск, приостановка, возобновление, остановка задач вручную ..... 164

Работа с расписанием задач ..... 165

Использование учетных записей для запуска задач ..... 167

Импорт и экспорт параметров ..... 168

Использование шаблонов параметров безопасности ..... 172


## Категории задач Kaspersky Embedded Systems Security для Windows

Функции постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления Kaspersky Embedded Systems Security для Windows реализованы в виде задач.

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли программы, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Embedded Systems Security для Windows: *локальные* и *групповые*.

**Локальные задачи**

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

- **Локальные системные задачи**. Эти задачи создаются автоматически при установке Kaspersky Embedded Systems Security для Windows. Вы можете изменять параметры всех локальных системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Локальные системные задачи нельзя переименовывать или удалять. Вы можете запускать локальные системные и пользовательские задачи проверки по требованию одновременно.
- **Локальные пользовательские задачи**. В Консоли программы вы можете создавать задачи проверки по требованию. В Kaspersky Security Center можно создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

**Групповые задачи**

Групповыми задачами и задачами для наборов защищаемых устройств можно управлять из Kaspersky Security Center. Все групповые задачи являются пользовательскими. Групповые задачи также отображаются в Консоли программы. В Консоли программы можно только просматривать состояние групповых задач. С помощью Консоли программы нельзя управлять или настраивать групповые задачи.

## Запуск, приостановка, возобновление, остановка задач вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты компьютера и проверки по требованию. Никакие другие задачи нельзя приостановить или возобновить вручную.

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

1. В дереве Консоли программы откройте контекстное меню задачи.
2. Выберите одну из следующих команд: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 258).

После возобновления задачи проверки по требованию Kaspersky Embedded Systems Security для Windows продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

kaspersky

# Работа с расписанием задач

Вы можете задать расписание для задач Kaspersky Embedded Systems Security для Windows.

## В этом разделе

Настройка параметров расписания задач ..... 165
Включение и выключение запуска задач по расписанию ..... 166

## Настройка параметров расписания задач

В Консоли программы можно настроить расписание запуска локальных системных и пользовательских задач. Однако настроить расписание запуска групповых задач нельзя.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, для которой требуется настроить расписание.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Выполните следующие действия, чтобы настроить расписание:
   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась с периодичностью в заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, чтобы задача запускалась с периодичностью в заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, чтобы задача запускалась с периодичностью в заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security для Windows.
      - **После обновления баз программы**, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату первого запуска задачи.

> После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
> В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию запрещен действующей политикой Kaspersky Security Center.

5. На закладке **Дополнительно** настройте следующие параметры расписания:
   - В разделе **Параметры остановки задачи**:
     a. Установите флажок **Длительность**. В полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с**. В полях справа укажите, когда требуется приостановить и возобновить выполнение задачи (в рамках 24 часов).
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить с** и укажите дату прекращения действия расписания.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы запускать пропущенные задачи.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **OK**.

Параметры расписания задачи будут сохранены.

## Включение и выключение запуска задач по расписанию

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

► *Чтобы включить или выключить запуск задачи по расписанию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню настраиваемой задачи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, чтобы включить запуск задачи по расписанию.

- Снимите флажок **Запускать задачу по расписанию**, чтобы выключить запуск задачи по расписанию.

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

4. Нажмите на кнопку **OK**.

Параметры расписания задачи будут сохранены.

# Использование учетных записей для запуска задач

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

## В этом разделе

Об использовании учетных записей для запуска задач ..... 167
Указание учетной записи для запуска задачи ..... 168

## Об использовании учетных записей для запуска задач

Вы можете указать учетную запись для запуска следующих задач Kaspersky Embedded Systems Security для Windows:

- Формирование правил контроля запуска программ
- Формирование правил контроля устройств
- Проверка по требованию
- Обновление

По умолчанию указанные задачи выполняются с правами системной учетной записи.

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

- Для задачи **Обновление**: если в качестве источника обновления указана папка общего доступа на другом устройстве в сети.
- Для задачи **Обновление**: если для доступа к источнику обновлений используется прокси-сервер со встроенной в Windows проверкой подлинности NTLM.
- Для задач **Проверка по требованию**: если системная учетная запись не обладает правами доступа к проверяемым объектам (например, к файлам в папках общего доступа на защищаемом устройстве).
- Для задачи **Формирование правил контроля запуска программ**: если сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, находящийся в папке общего доступа на защищаемом устройстве).

Вы можете запускать задачи обновления, проверки по требованию и автоматического формирования разрешающих правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Embedded Systems Security для Windows обращается к папкам общего доступа на другом устройстве в сети, если это устройство зарегистрировано в то же домене, что и защищаемое устройство. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Embedded Systems Security для Windows обращается к устройству с правами учетной записи **<имя домена \ имя устройства>**.

### Указание учетной записи для запуска задачи

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

1. В дереве Консоли программы откройте контекстное меню задачи, которую вы хотите запустить с правами определенной учетной записи.
2. Выберите пункт **Свойства**.

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

      Выбранный вами пользователь должен быть зарегистрирован на защищаемом устройстве или в одном домене с ним.
   c. Подтвердите пароль.
4. Нажмите на кнопку **OK**.

Изменения параметров задачи будут сохранены.

## Импорт и экспорт параметров

В этом разделе приведена информация об экспорте параметров Kaspersky Embedded Systems Security для Windows. Также описан экспорт параметров определенных программных компонентов в конфигурационный файл в формате XML и импорт этих параметров из конфигурационного файла в программу.

### В этом разделе


Об импорте и экспорте параметров ..... 169

Экспорт параметров ..... 170

Импорт параметров ..... 171

## Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Embedded Systems Security для Windows в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security для Windows из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Embedded Systems Security для Windows, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Embedded Systems Security для Windows:

- Постоянная защита файлов
- Использование KSN
- Контроль устройств
- Контроль запуска программ
- Формирование правил контроля устройств
- Формирование правил контроля запуска программ
- Задачи проверки по требованию
- Мониторинг файловых операций
- Анализ журналов
- Обновление баз и модулей Kaspersky Embedded Systems Security для Windows
- Карантин
- Резервное хранилище
- Журналы
- Уведомления администратора и пользователей
- Доверенная зона
- Защита от эксплойтов
- Защита паролем

Также вы можете сохранять в файле общие параметры Kaspersky Embedded Systems Security для Windows и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Embedded Systems Security для Windows экспортирует все пароли, используемые в программе, например, параметры учетных записей для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Пароли можно импортировать только с помощью программы Kaspersky Embedded Systems Security для Windows, установленной на этом же защищаемом устройстве, если она не была переустановлена или обновлена.

Нельзя импортировать ранее сохраненные пароли с помощью программы Kaspersky Embedded Systems Security для Windows, установленной на другом защищаемом устройстве. После импорта параметров на другом защищаемом устройстве нужно ввести все пароли вручную.

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

Можно импортировать параметры из конфигурационного файла, содержащего параметры только отдельных компонентов Kaspersky Embedded Systems Security для Windows (например, созданного в программе Kaspersky Embedded Systems Security для Windows, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Embedded Systems Security для Windows изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

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

## Экспорт параметров

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

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Embedded Systems Security для Windows** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Embedded Systems Security для Windows.
   - В контекстном меню требуемой задачи выберите пункт **Экспортировать параметры**, чтобы экспортировать параметры отдельного функционального компонента программы.
   - Чтобы экспортировать параметры доверенной зоны, выполните следующие действия:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

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

     Откроется окно мастера экспорта параметров.
2. Выполните инструкции, которые предлагает **Мастер экспорта параметров программы**: задайте имя и путь конфигурационного файла, в который вы хотите сохранить параметры.

   При указании пути можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя.

   Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует параметры, используемые в политике.
3. В окне **Закрыть** нажмите на кнопку **Экспорт параметров программы завершен**.

Мастер экспорта параметров будет закрыт; экспортированные параметры будут сохранены.

## Импорт параметров

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

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Embedded Systems Security для Windows** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Embedded Systems Security для Windows.
   - В контекстном меню требуемой задачи выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента программы.
   - Чтобы импортировать параметры доверенной зоны, выполните следующие действия:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

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

        Откроется окно мастера импорта параметров.
2. Выполните инструкции, которые предлагает **Мастер импорта параметров программы**: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После импорта общих параметров или параметров функциональных компонентов Kaspersky Embedded Systems Security для Windows на защищаемое устройство, восстановить их прежние значения невозможно.
3. В окне **Закрыть** нажмите на кнопку **Импорт параметров программы завершен**.

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.
4. В панели инструментов Консоли программы нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли программы.

Kaspersky Embedded Systems Security для Windows не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом защищаемом устройстве или на этом же защищаемом устройстве, после того как на нем была переустановлена или обновлена программа Kaspersky Embedded Systems Security для Windows. После завершения импорта пароли необходимо ввести вручную.

kaspersky

# Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Embedded Systems Security для Windows.

## В этом разделе


О шаблонах параметров безопасности ..... 172

Создание шаблона параметров безопасности ..... 172

Просмотр параметров безопасности в шаблоне ..... 173

Применение шаблона параметров безопасности..... 173

Удаление шаблона параметров безопасности ..... 174


## О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security для Windows.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Embedded Systems Security для Windows:

- Постоянная защита файлов
- Проверка при старте операционной системы
- Проверка важных областей
- Задачи проверки по требованию

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

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел "Применение шаблона параметров безопасности" на стр. 173).
- Если вложенные узлы виртуальные. В этом случае необходимо применить шаблон для каждого виртуального узла отдельно.

## Создание шаблона параметров безопасности

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите создать шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.

3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите дополнительное описание шаблона.
7. Нажмите на кнопку **OK**.

Шаблон параметров безопасности сохранен.

## Просмотр параметров безопасности в шаблоне

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите просмотреть шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

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

Откроется окно **<Название шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне. На закладке **Параметры** приведен список параметров безопасности, сохраненных в шаблоне.

## Применение шаблона параметров безопасности

► *Чтобы применить параметры безопасности из шаблона к выбранному узлу, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства откройте контекстное меню узла или элемента, к которому вы хотите применить шаблон.
4. Выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов защищаемого устройства. Значение на закладке **Уровень безопасности** для выбранного узла изменится на **Другой**.

Если значения параметры безопасности из шаблона применяются к родительскому узлу в дереве файловых ресурсов защищаемого устройства, эти параметры распространяются на все вложенные узлы.

Можно настроить область защиты или область проверки вложенных узлов в дереве файловых ресурсов защищаемого устройства отдельно. В этом случае параметры безопасности из шаблона, примененного к родительскому узлу, не применяются автоматически к вложенным узлам.

► *Чтобы применить параметры безопасности из шаблона ко всем выбранным узлам, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите родительский узел, чтобы применить шаблон к этому узлу и к его вложенным узлам.
4. В контекстном меню выберите пункт **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов защищаемого устройства. Значение на закладке **Уровень безопасности** для выбранного узла изменится на **Другой**.

## Удаление шаблона параметров безопасности

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

1. В дереве Консоли программы выберите задачу, для которой вы хотите удалить шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.

   Вы можете просмотреть шаблоны параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

3. В списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения удаления.

5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Шаблон параметров безопасности можно применить для защиты или проверки узлов в дереве файловых ресурсов защищаемого устройства. В этом случае настроенные для этих узлов параметры безопасности сохраняются после удаления шаблона.

# Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security для Windows

► *Чтобы просмотреть информацию о состоянии защиты устройства в Kaspersky Embedded Systems Security для Windows,*

в дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security для Windows**.

По умолчанию информация в панели результатов Консоли программы обновляется автоматически:

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

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле **Kaspersky Embedded Systems Security для Windows**,*

в контекстном меню узла **Kaspersky Embedded Systems Security для Windows** выберите пункт **Обновить**.

В панели результатов Консоли программы отображается следующая информация о программе:

- статус использования Kaspersky Security Network;
- состояние защиты устройства;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля защищаемого устройства;
- данные о лицензии;
- статус интеграции с Kaspersky Security Center: данные сервера с установленной программой Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В разделе **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *Остановлена* или *Не выполнялась*. Индикатор может принимать следующие значения:

- Зеленый – задача Использование KSN выполняется и запросы о файловой репутации отправляются в KSN.
- Желтый – принято одно из Положений, но задача не выполняется, или задача выполняется, но запросы не отправляются в KSN.

Защита компьютера

В разделе **Защита компьютера** (см. таблицу ниже) отображается информация о текущем состоянии защиты устройства.

*Таблица 25. Информация о состоянии защиты устройства*

| Раздел Защита | Информация |
|---|---|
| **Индикатор состояния защиты устройства** | Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения:<br>• Зеленый – отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется.<br>• Желтый – компонент Постоянная защита файлов не установлен и задача Проверка важных областей не выполнялась в течение долгого времени.<br>• Красный – задача Постоянная защита файлов не выполняется. |
| **Постоянная защита файлов** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Обнаружено** – количество объектов, обнаруженных программой Kaspersky Embedded Systems Security для Windows. Например, если программа Kaspersky Embedded Systems Security для Windows обнаружила одну вредоносную программу в пяти файлах, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ больше 0, значение выделяется красным цветом. |
| **Проверка важных областей** | **Дата последней проверки** – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз безопасности.<br>*Не выполнялась* – событие, которое возникает, если задача Проверка важных областей выполнялась 30 и более дней назад (по умолчанию). Вы можете изменять порог формирования этого события. |
| **Защита от эксплойтов** | **Статус** – текущий статус функции защиты от эксплойтов, например, *Используется* или *Не применяется*.<br>**Режим работы** – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: **Завершать скомпрометированные процессы** или **Только статистика**.<br>**Процессов защищено** – общее количество процессов, которые были добавлены в область защиты и обрабатываются в соответствие с выбранным режимом. |

| Раздел Защита | Информация |
|---|---|
| **Объектов в резервном хранилище** | *Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если объем доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Embedded Systems Security для Windows при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом.<br>*Превышен максимальный размер резервного хранилища* – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Embedded Systems Security для Windows при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом.<br>**Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище.<br>**Используемое пространство** – объем используемого пространства в резервном хранилище. |

Обновление

В разделе **Обновление** (см. таблицу ниже) отображается информация об актуальности баз и модулей программы.

*Таблица 26. Информация о состоянии баз и модулей Kaspersky Embedded Systems Security для Windows*

| **Раздел** Обновление | **Информация** |
|---|---|
| **Индикатор состояния баз и модулей программы** | Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения:<br>• Зеленый – отображается по умолчанию и означает, что базы программы актуальны и последняя задача обновления баз программы завершена успешно.<br>• Желтый – базы программы устарели или последняя задача Обновление баз программы завершена с ошибкой.<br>• Красный – возникло событие *Базы программы сильно устарели* или *Базы программы повреждены*. |

| **Раздел** Обновление | **Информация** |
|---|---|
| **Обновление баз программы** и **Обновление модулей программы** | **Актуальность баз программы** – оценка статуса Обновления баз программы.<br>Параметр может принимать следующие значения:<br>• **Базы программы актуальны** – базы программы были обновлены не более чем 7 дней назад (по умолчанию).<br>• **Базы программы устарели** – базы программы были обновлены от 7 до 14 дней назад (по умолчанию).<br>• **Базы программы сильно устарели** – базы программы были обновлены более чем 14 дней назад (по умолчанию).<br>Вы можете изменять пороги формирования событий *Базы программы актуальны* и *Базы программы сильно устарели*.<br>**Дата выпуска баз программы** – дата и время выпуска последнего обновления баз программы. Дата и время указаны в UTC-формате.<br>**Статус последней запущенной задачи обновления баз программы** – дата и время последнего обновления баз программы. Дата и время указаны по местному времени защищаемого устройства. Поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*.<br>**Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Embedded Systems Security для Windows, доступных для загрузки и установки.<br>**Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Embedded Systems Security для Windows. |

Контроль

В разделе **Контроль** (см. таблицу ниже) отображается информация о задачах Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

*Таблица 27. Информация о состоянии контроля защищаемого устройства*

| **Раздел** Контроль | **Информация** |
|---|---|
| **Индикатор состояния контроля защищаемого устройства** | Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения:<br>• Зеленый – отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в режиме активном **Активный**.<br>• Желтый – задача Контроль запуска программ выполняется в режиме **Только статистика**.<br>• Красный – задача Контроль запуска программ не выполняется или завершена с ошибкой. |

| **Раздел** Контроль | **Информация** |
|---|---|
| **Контроль запуска программ** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Режим работы** – один из двух доступных режимов работы задачи Контроль запуска программ: **Активный** или **Только статистика**.<br>**Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Embedded Systems Security для Windows в ходе выполнения задачи Контроль запуска программ. Если количество заблокированных запусков программ превышает 0, поле окрашивается в красный цвет.<br>**Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Embedded Systems Security для Windows для обработки попытки запуска программ на защищаемом устройстве. |
| **Контроль устройств** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Режим работы** – один из двух доступных режимов работы задачи Контроль устройств: **Активный** или **Только статистика**.<br>**Заблокировано устройств** – количество попыток подключения внешних устройств, заблокированных Kaspersky Embedded Systems Security для Windows в ходе выполнения задачи Контроль устройств. Если количество заблокированных внешних устройств превышает 0, значение поля окрашивается в красный цвет. |
| **Управление сетевым экраном** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Заблокировано попыток подключения** – количество подключений к защищаемому устройству, которые не были разрешены заданными правилами сетевого экрана. |

Диагностика

В разделе **Диагностика** (см. таблицу ниже) отображается информация о задачах Мониторинг файловых операций и Анализ журналов.

*Таблица 28. Информация о состоянии диагностики системы*

| **Раздел** Диагностика | **Информация** |
|---|---|
| **Индикатор статуса диагностики** | Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения:<br>• Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задачи выполняются.<br>• Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие *Не выполняется*.<br>• Красный – одна из задач завершена с ошибкой. |
| **Мониторинг файловых операций** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Несанкционированных файловых операций** – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого устройства. |
| **Анализ журналов** | **Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*.<br>**Нарушения настроенных правил** – количество зафиксированных нарушений по данным журнала событий Windows. Это количество определяется на основе заданных правил задачи или применения эвристического анализатора. |

Информация о лицензии на Kaspersky Embedded Systems Security для Windows отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security для Windows**.

Вы можете настроить свойства Kaspersky Embedded Systems Security для Windows, перейдя по ссылке **Свойства программы** (см. раздел "**Настройка общих параметров программы в Консоли программы**" на стр. 157).

Вы можете подключиться к другому защищаемому устройству, перейдя по ссылке **Подключиться к другому компьютеру** (см. раздел "**Управление Kaspersky Embedded Systems Security для Windows через Консоль программы, установленную на другом устройстве**" на стр. 157).

kaspersky

# Работа с Веб-плагином из Веб-консоли и Облачной консоли

Этот раздел содержит информацию о Плагине управления Kaspersky Embedded Systems Security для Windows и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

## В этом разделе


Управление Kaspersky Embedded Systems Security для Windows из Веб-консоли и Облачной консоли ..... 182

Ограничения Веб-плагина ..... 183

Управление параметрами программы ..... 184

Создание и настройка политик ..... 192

Создание и настройка задач в Kaspersky Security Center ..... 199

Отчеты в Kaspersky Security Center ..... 208


## Управление Kaspersky Embedded Systems Security для Windows из Веб-консоли и Облачной консоли

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security для Windows, объединенными в группу администрирования, с помощью Веб-плагина Kaspersky Embedded Systems Security для Windows. Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console также позволяют отдельно настраивать параметры каждого защищаемого устройства, входящего в группу администрирования.

*Группа администрирования* формируется вручную на стороне Kaspersky Security Center Web Console. Группа администрирования включает устройства с установленной программой Kaspersky Embedded Systems Security для Windows, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Embedded Systems Security для Windows на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security для Windows из Kaspersky Security Center Web Console следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне свойств устройства в Kaspersky Security Center Web Console. С помощью политик можно настроить общие параметры программы, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, и параметры запуска локальных системных задач по расписанию.
- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств. С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.
- **С помощью окна свойств отдельного устройства**. В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры программы, так и параметры всех задач Kaspersky Embedded Systems Security для Windows, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console позволяют настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

# Ограничения Веб-плагина

Веб-плагин Kaspersky Embedded Systems Security для Windows имеет следующие ограничения по сравнению с Плагином управления Kaspersky Embedded Systems Security для Windows:

- Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
- Для задачи Постоянная защита файлов нельзя изменить стандартный уровень безопасности.
- Для задачи Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.
- Для задачи Контроль устройств нельзя сформировать правила на основе подключенных устройств или данных системы.

# Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security для Windows в Kaspersky Security Center Web Console.

## В этом разделе


Настройка общих параметров программы с помощью Веб-плагина ..... 184

Настройка параметров карантина и резервного хранилища с помощью Веб-плагина..... 191


# Настройка общих параметров программы с помощью Веб-плагина

С помощью Веб-плагина можно настроить общие параметры Kaspersky Embedded Systems Security для Windows для группы защищаемых устройств или для отдельного защищаемого устройства.

## В этом разделе


Настройка параметров масштабируемости, интерфейса и проверки с помощью Веб-плагина ..... 184

Настройка параметров безопасности с помощью Веб-плагина ..... 187

Настройка параметров соединения с помощью Веб-плагина ..... 188

Настройка запуска по расписанию локальных системных задач ..... 190


### Настройка параметров масштабируемости, интерфейса и проверки с помощью Веб-плагина

► *Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Масштабируемость, интерфейс, настройки сканирования**.

6. Настройте параметры, приведены в следующей таблице.

*Таблица 29. Параметры масштабируемости*

| Параметр | Описание |
|---|---|
| **Определять параметры масштабируемости автоматически** | Kaspersky Embedded Systems Security для Windows автоматически регулирует количество используемых процессов.<br>Это значение установлено по умолчанию. |
| **Указать количество рабочих процессов вручную** | Kaspersky Embedded Systems Security для Windows контролирует количество активных рабочих процессов в соответствии с указанными значениями. |
| **Количество процессов для постоянной защиты** | Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**. |
| **Количество процессов для фоновых задач проверки по требованию** | Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**. |
| **Показывать значок в панели задач** | Настройте, будет ли Значок области уведомлений отображаться в панели задач. |
| **Восстанавливать атрибуты файлов после сканирования** | Когда Kaspersky Embedded Systems Security для Windows выполняет задачи Проверка по требованию и Постоянная защита файлов, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Embedded Systems Security для Windows возвращает исходное значение времени последнего обращения к файлу.<br>Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.<br>По умолчанию эта функция включена.<br>Когда Kaspersky Embedded Systems Security для Windows выполняет задачи Проверка по требованию и Постоянная защита файлов, обновляется время последнего обращения к каждому проверяемому файлу. После проверки Kaspersky Embedded Systems Security для Windows возвращает исходное значение времени последнего обращения к файлу.<br>Такое поведение может повлиять на работу систем резервного копирования, поскольку приводит к созданию резервных копий файлов, которые не были изменены. Это также может вызывать ложные срабатывания в программах для отслеживания изменений файлов.<br>По умолчанию эта функция включена. |

| Параметр | Описание |
| --- | --- |
| Ограничивать сканирующие потоки в использовании ЦП | Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.<br><br>Включение этой опции может негативно сказаться на производительности Kaspersky Embedded Systems Security для Windows.<br><br>По умолчанию эта опция выключена. |
| Предельное значение (в процентах) | Максимально допустимое значение загрузки процессора программой Kaspersky Embedded Systems Security для Windows.<br><br>Это поле доступно, если выбран параметр **Ограничивать сканирующие потоки в использовании ЦП**. |
| Kaspersky Embedded Systems Security для Windows ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Предельное значение (в процентах)**.<br><br>Включение этой опции может негативно сказаться на производительности Kaspersky Embedded Systems Security для Windows.<br><br>По умолчанию эта опция выключена.<br><br>**Папка для временных файлов, создаваемых при сканировании** | Папка, в которую программа Kaspersky Embedded Systems Security для Windows распаковывает файлы архивов при проверке.<br><br>По умолчанию используется папка C:\Windows\Temp.<br><br>Папка, в которую программа Kaspersky Embedded Systems Security для Windows распаковывает файлы архивов при проверке.<br><br>По умолчанию используется папка C:\Windows\Temp. |
| **Параметры HSM-системы** | Выберите тип доступа к иерархическому хранилищу. |

## Настройка параметров безопасности с помощью Веб-плагина

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. Нажмите на кнопку **Настройка** в подразделе **Безопасность и надежность**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 30. Параметры безопасности*

| Параметр | Описание |
|---|---|
| **Защищать процессы программы от внешних угроз** | Если функция **Защищать процессы программы от внешних угроз** включена, программа защищает процессы от внедрения кода и доступа к данным процессов.<br>При включении или выключении этой функции нет необходимости перезапускать службы программы, чтобы изменения вступили в силу.<br>Функция включена по умолчанию. |
| Выполнять восстановление задач | Флажок включает или выключает восстановление задач Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows автоматически восстанавливает задачи Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не восстанавливает задачи Kaspersky Embedded Systems Security для Windows после сбоя в работе программы или аварийного завершения работы программы.<br>По умолчанию флажок установлен. |
| Выполнять восстановление задач проверки по требованию не более (раз), значение в диапазоне от 1 до 10 | Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Embedded Systems Security для Windows. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**. |

| Параметр | Описание |
|---|---|
| Не запускать задачи проверки по расписанию | Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows не запускает задачи проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows запускает задачи проверки по расписанию вне зависимости от режима питания.<br>По умолчанию флажок установлен. |
| Остановить выполняемые задачи проверки | Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows останавливает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows продолжает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания.<br>По умолчанию флажок установлен. |
| Использовать защиту паролем | Установить пароль для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows. |

## Настройка параметров соединения с помощью Веб-плагина

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security для Windows к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.

5. Нажмите на кнопку **Настройка** в подразделе **Масштабируемость, интерфейс, настройки сканирования**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 31. Параметры соединения*

| Параметр | Описание |
|---|---|
| Не использовать прокси-сервер | Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую. |
| Использовать параметры указанного прокси-сервера | Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security для Windows использует параметры прокси-сервера, указанные вручную. |
| Не использовать прокси-сервер для локальных адресов | Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security для Windows.<br>Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security для Windows, происходит напрямую. Прокси-сервер не используется.<br>Если флажок снят, для подключения к локальным устройствам используется прокси-сервер.<br>По умолчанию флажок установлен. |
| Параметры аутентификации на прокси-сервере | Укажите параметры аутентификации |
| **Не использовать аутентификацию** | Проверка подлинности не выполняется. Этот режим выбран по умолчанию. |
| **Использовать NTLM-аутентификацию** | Проверка подлинности выполняться с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft. |
| **Использовать NTLM-аутентификацию с именем пользователя и паролем** | Проверка подлинности выполняется по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля. |
| **Использовать имя пользователя и пароль** | Проверка подлинности выполняется с помощью имени пользователя и пароля. |

## Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления. Запуск осуществляется по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Embedded Systems Security для Windows будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если защищаемое устройство исключено из группы администрирования, расписание локальных системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию локальных системных задач Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.

5. Нажмите на кнопку **Настройка** в подразделе **Запуск локальных системных задач**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 32. Параметры запуска локальных системных задач по расписанию*

| Параметр | Описание |
|---|---|
| Разрешить запуск задач проверки по требованию | Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач проверки по требованию. |
| Разрешить запуск задач обновления и копирования обновлений | Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач обновления и копирования обновлений. |

## Настройка параметров карантина и резервного хранилища с помощью Веб-плагина

Чтобы настроить общие параметры карантина и резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Хранилища**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 33. Параметры карантина и резервного хранилища*

| Параметр | Описание |
|---|---|
| **Папка резервного хранилища** | Укажите папку резервного хранилища. |
| **Максимальный размер резервного хранилища (МБ)** | Укажите максимальный размер резервного хранилища. |
| **Порог доступного пространства (МБ)** | Укажите минимальное значение свободного места в папке резервного хранилища. |
| **Папка, в которую восстанавливаются объекты** | Укажите папку для восстановленных объектов. |
| **Папка карантина** | Укажите папку резервного хранилища. |

| Параметр | Описание |
| --- | --- |
| **Максимальный размер карантина (МБ)** | Укажите максимальный размер резервного хранилища. |
| **Порог доступного пространства (МБ)** | Укажите минимальное значение свободного места в папке резервного хранилища. |
| **Папка, в которую восстанавливаются объекты** | Укажите папку для восстановленных объектов. |
| **Условия блокировки сетевых сессий** | Укажите количество суток, часов и минут, по истечении которых заблокированные сетевые сеансы получат доступ к сетевым файловым ресурсам. |

# Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security для Windows на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security для Windows.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Embedded Systems Security для Windows на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *активная* в Консоли администрирования.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Embedded Systems Security для Windows. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Embedded Systems Security для Windows использует на защищаемых устройствах параметры, для которых в свойствах политики вы установили значок 🔒. В этом случае выбранные параметры используются вместо параметров, действовавших до применения политики. Kaspersky Embedded Systems Security для Windows не применяет параметры активной политики, для которых в свойствах политики установлен значок 🔓 .

Если политика активна, то значения параметров, отмеченные в политике значком 🔒, отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком 🔓 ) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком 🔒, также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры для любой задачи постоянной защиты компьютера, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

## В этом разделе


Создание политики ..... 193

Разделы параметров политики Kaspersky Embedded Systems Security для Windows ..... 194


# Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Нажмите на кнопку **Добавить**.
3. Откроется окно **Новая политика**.
4. В разделе **Выбор программы** выберите Kaspersky Embedded Systems Security для Windows и нажмите на кнопку **Далее**.
5. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.

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

   - Выбрать статус политики:
     - **Активный**. После следующей синхронизации политика будет использоваться на компьютере в качестве активной политики.
     - **Неактивный**. Резервная политика. При необходимости можно перевести неактивную политику в активный статус.
     - **Для автономных пользователей**. Эта политика активируется, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если включен этот переключатель, значения параметров политики наследуются из политики верхнего уровня. Параметры политики недоступны для изменения, если для родительской политики установлен 🔒.

- **Принудительное наследование параметров в дочерних политиках**. Если переключатель включен, значения параметров политики распространяются на дочерние политики. В параметрах дочерней политики автоматически устанавливается флажок **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, за исключением параметров, отмеченных . Параметры дочерней политики недоступны для изменения, если для родительской политики установлен .

6. На закладке **Параметры программы** настройте параметры политики в соответствии с вашими требованиями.
7. Нажмите на кнопку **Сохранить**.

Созданная политика отобразится в списке политик на закладке **Политики и профили** выбранной группы администрирования. В окне **<Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Embedded Systems Security для Windows.

## Разделы параметров политики Kaspersky Embedded Systems Security для Windows

### Общие

В разделе **Общие** можно настроить следующие параметры политики:

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

### Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** можно настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

*Таблица 34. Параметры в разделе Параметры программы*

| Раздел | Параметры |
|---|---|
| **Масштабируемость, интерфейс, настройки сканирования** | В подразделе **Масштабируемость, интерфейс, настройки сканирования** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• выбрать автоматическую или ручную настройку параметров масштабирования;<br>• настроить параметры отображения значка программы. |
| **Безопасность и надежность** | В подразделе **Безопасность и надежность** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• настроить параметры запуска задачи;<br>• указать действия программы при переходе защищаемого устройства на источник бесперебойного питания;<br>• включить или выключить защиту функций программы паролем. |
| **Параметры соединения** | В подразделе **Параметры соединения** по кнопке **Настройка** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN:<br>• указать параметры использования прокси-сервера;<br>• указать параметры аутентификации на прокси-сервере. |
| **Запуск локальных системных задач** | В подразделе **Запуск локальных системных задач** по кнопке **Настройка** можно разрешить или запретить запуск следующих локальных системных задач по расписанию, настроенному на защищаемых устройствах:<br>• задачи проверки по требованию;<br>• задачи обновления и копирования обновлений. |

Дополнительные возможности

*Таблица 35. Параметры в разделе Дополнительные возможности*

| Раздел | Параметры |
|---|---|
| **Доверенная зона** | В подразделе **Настройка** по кнопке **Доверенная зона** вы можете настроить следующие параметры применения доверенной зоны:<br>• сформировать список исключений доверенной зоны;<br>• включить или выключить проверку операций резервного копирования файлов;<br>• сформировать список доверенных процессов. |
| **Проверка съемных дисков** | В подразделе **Проверка съемных дисков** по кнопке **Настройка** вы можете настроить параметры проверки съемных дисков. |
| **Права пользователей на управление программой** | В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Embedded Systems Security для Windows. |

| Раздел | Параметры |
| --- | --- |
| **Права пользователей на управление службой Kaspersky Security Service** | В подразделе **Права пользователей на управление службой Kaspersky Security Service** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security. |
| **Хранилища** | В подразделе **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов:<br>• указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;<br>• настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;<br>• указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;<br>• настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования.<br>• настроить продолжительность блокировки узлов. |

Постоянная защита компьютера

*Таблица 36. Параметры в разделе Постоянная защита сервера*

| Раздел | Параметры |
| --- | --- |
| **Постоянная защита файлов** | В подразделе **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• указать режим защиты объектов;<br>• настроить применение эвристического анализатора;<br>• настроить применение доверенной зоны;<br>• указать область защиты;<br>• задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;<br>• настроить параметры запуска задачи. |
| **Использование KSN** | В подразделе **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• указать действия над объектами, недоверенными в KSN;<br>• настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN. |

| Раздел | Параметры |
| --- | --- |
| **Защита от эксплойтов** | В подразделе **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим защиты памяти процессов;<br>• указать действия для снижения рисков эксплуатации уязвимостей;<br>• дополнить и изменить список защищаемых процессов. |

Контроль активности на компьютерах

*Таблица 37. Параметры в разделе Контроль активности на компьютерах*

| Раздел | Параметры |
| --- | --- |
| **Контроль запуска программ** | В подразделе **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры контроля повторных запусков программ;<br>• указать область применения правил контроля запуска программ;<br>• настроить использование KSN;<br>• настроить параметры запуска задачи. |
| **Контроль устройств** | В подразделе **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры запуска задачи. |

Контроль активности в сети

*Таблица 38. Параметры в разделе Контроль активности в сети*

| Раздел | Параметры |
| --- | --- |
| **Управление сетевым экраном** | В подразделе **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• настроить правила сетевого экрана;<br>• настроить параметры запуска задачи. |

Диагностика системы

*Таблица 39. Параметры в разделе Диагностика системы*

| Раздел | Параметры |
|---|---|
| **Мониторинг файловых операций** | В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. |
| **Анализ журналов** | В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows. |

Журналы и уведомления

*Таблица 40. Параметры в разделе Журналы и уведомления*

| Раздел | Параметры |
|---|---|
| **Журналы выполнения задач** | В подразделе **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• указать уровень важности регистрируемых событий для выбранных компонентов программы;<br>• указать параметры хранения журналов выполнения задач;<br>• указать параметры интеграции SIEM-системы с Kaspersky Security Center. |
| **Уведомления о событиях** | В подразделе **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры:<br>• указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и заблокировано недоверенное запоминающее устройство* и *Недоверенный узел в списке*;<br>• указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**. |
| **Взаимодействие с Сервером администрирования** | В подразделе **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security для Windows будет передавать на Сервер администрирования. |

**История ревизий**

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

# Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security для Windows, их создании, настройке параметров выполнения, запуске и остановке.

## В этом разделе


О создании задач с помощью Веб-плагина ..... 199

Создание задачи с помощью Веб-плагина ..... 200

Настройка групповых задач с помощью Веб-плагина ..... 201

Настройка параметров диагностики сбоев с помощью Веб-плагина ..... 204

Работа с расписанием задач ..... 206


## О создании задач с помощью Веб-плагина

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Можно создавать задачи следующих типов:

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

Вы можете создать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**.
- Для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**.
- Для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 116) по требованию на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

## Создание задачи с помощью Веб-плагина

► *Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
     b. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
     c. Выберите название защищаемого устройства.
     d. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
     e. Нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
     b. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.
     c. Нажмите на кнопку **Добавить**.
   - Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
     a. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
     b. Выберите выборку устройств, для которой требуется создать задачу.
     c. Нажмите на кнопку **Запустить**.
     d. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.
     e. Нажмите на кнопку **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security для Windows**.
3. В раскрывающемся списке **Тип задачи** выберите тип создаваемой задачи.

   Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно параметров.
4. В зависимости от выбранного типа задачи выполните одно из следующих действий:
   - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 572).
   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
     a. Выберите источник обновлений в разделе **Источник обновления баз программы**.
     b. В окне **Настройка параметров соединения** настройте параметры прокси-сервера.
   - После создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Обновление модулей программы**:

a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.

b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Embedded Systems Security для Windows автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.

c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Embedded Systems Security для Windows, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Копирование обновлений**.
- Для создания задачи Активация программы:

  a. В окне **Список ключей в хранилище ключей Kaspersky Security Center** укажите файл ключа, с помощью которого вы хотите активировать программу.

  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
- Создайте задачу Формирование правил контроля запуска программ и настройте ее параметры.
- Создайте задачу Формирование правил контроля устройств и настройте ее параметры.

5. Нажмите на кнопку **Далее**.
6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.
7. Нажмите на кнопку **Далее**.
8. В окне **Завершение создания задачи** установите флажок **Перейти к параметрам задачи после создания**, чтобы настроить параметры задачи.
9. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

## Настройка групповых задач с помощью Веб-плагина

► *Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     a. В разделе **Область проверки** настройте область проверки.
     b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
     a. В разделе **Источники обновлений** настройте параметры источника обновлений и прокси-сервера.
     b. В разделе **Оптимизация** настройте параметры оптимизации дисковой подсистемы.
   - Чтобы настроить задачу Обновление модулей программы, в разделе **Дополнительные параметры** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
   - Чтобы настроить задачу Копирование обновлений, в разделе **Параметры копирования обновлений** укажите состав обновлений и папку назначения.
   - Чтобы настроить задачу Активация программы, примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
   - Чтобы настроить автоматическое формирование разрешающих правил контроля устройств, укажите параметры, на основе которых будет сформирован список разрешающих правил.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. На закладке **Параметры** в разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры групповых задач будут сохранены.

## В этом разделе

Настройка задачи Активация программы с помощью Веб-плагина ..... 202
Настройка задач обновления с помощью Веб-плагина ..... 203

## Настройка задачи Активация программы с помощью Веб-плагина

► *Чтобы настроить задачу Активация программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. В разделе **Общие** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
4. Настройте расписание задачи в разделе **Расписание**.
5. В окне **<Название задачи>** нажмите на кнопку **OK**.

## Настройка задач обновления с помощью Веб-плагина

► *Чтобы настроить задачи Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. В разделе **Источники обновлений** настройте параметры источника обновлений:
   - В разделе **Источник обновления баз программы** укажите Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновлений: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

     Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     > Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
     > При настройке задачи обновления с помощью Облачной консоли в качестве источника обновлений доступны только варианты **Точки распространения** и **Серверы обновлений «Лаборатории Касперского»**.

   - В разделе **Настройка параметров соединения** настройте использование прокси-сервера для подключения к серверам обновлений "Лаборатории Касперского" и другим серверам.
4. В разделе **Оптимизация** для задачи Обновление баз программы можно настроить функцию, снижающую нагрузку на дисковую подсистему:
   - **Оптимизация использования дисковой подсистемы**

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

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.

- **Объем оперативной памяти, используемой для оптимизации (400 - 9999 МБ)**

  Объем оперативной памяти (в МБ), используемый программой для хранения файлов обновлений. По умолчанию задан объем 600 МБ. Минимальный объем составляет 400 МБ.

  При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

  - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении). Это приведет к завершению задачи с ошибкой.

    В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

  - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. Функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

    В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В окне **<Название задачи>** нажмите на кнопку **OK**.

## Настройка параметров диагностики сбоев с помощью Веб-плагина

Если в работе Kaspersky Embedded Systems Security для Windows возникла проблема (например, аварийное завершение Kaspersky Embedded Systems Security для Windows), ее можно диагностировать. Для этого можно включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security для Windows и отправить эти файлы на анализ в Службу технической поддержки.

Kaspersky Embedded Systems Security для Windows не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security для Windows. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 131).
2. Откройте раздел **Диагностика сбоев**.
3. Чтобы отладочная информация записывалась в файл, в разделе **Параметры диагностики сбоев** установите флажок **Включить трассировку**.
4. В поле **Папка файлов трассировки** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы трассировки.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
5. Настройте уровень детализации отладочной информации.

   В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки. Параметр доступен, если установлен флажок **Включить трассировку**.

   Вы можете выбрать один из следующих режимов работы задачи:

   - **Полная информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файле трассировки всю отладочную информацию.
   - **Краткая информация** – Kaspersky Embedded Systems Security для Windows сохраняет в файл трассировки только информацию о критических событиях.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

   По умолчанию установлен уровень детализации **Полная информация**.
6. Укажите **Максимальный размер файлов трассировки (МБ)**.

   Доступные значения: от 1 до 4095 МБ. По умолчанию максимальный размер файлов трассировки составляет 50 МБ.
7. Для удаления самых старых файлов трассировки при достижении максимального количества файлов установите флажок **Использовать вытеснение старых файлов журнала трассировки**.
8. Укажите значение **Максимальное количество файлов журнала трассировки**.

   Доступные значения: от 1 до 999. По умолчанию максимальное количество файлов составляет 5. Поле доступно, если установлен флажок **Использовать вытеснение старых файлов журнала трассировки**.
9. Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать файл дампа**.
10. В поле **Папка файлов дампа** укажите абсолютный путь к локальной папке, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы дампа.

    Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
11. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом устройстве.

kaspersky

# Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Embedded Systems Security для Windows, а также настроить параметры запуска по расписанию.

## В этом разделе


Настройка расписания задач ..... 206

Включение и выключение запуска задач по расписанию ..... 207


## Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. В разделе **Расписание** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.
5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. В списке **Частота запуска** выберите одно из следующих значений:

      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
      - **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security для Windows.
      - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.

6. В разделе **Параметры остановки задачи**:
   a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
   b. Установите флажок **Приостановить задачу** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
7. В блоке **Дополнительные параметры расписания**:
   a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
   b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
   c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры запуска задачи.

## Включение и выключение запуска задач по расписанию

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

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

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. Выберите раздел **Расписание**.
5. Выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

# Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Embedded Systems Security для Windows доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

**Отчет о статусе компонентов Kaspersky Embedded Systems Security для Windows components**

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center Web Console присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть статус компонентов в параметрах программы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Выберите название защищаемого устройства.
3. На закладке **Общие** выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

   Информация о статусе компонента Защита от эксплойтов недоступна в этой таблице.

► *Чтобы просмотреть стандартный отчет Kaspersky Security Center Web Console, выполните следующие действия:*

1. Выберите **Мониторинг и отчетность** → **Отчеты**.
2. В списке выберите **Отчет о статусе компонентов программы** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
3. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

**Отчеты о запрещенных программах в активном и в тестовом режимах**

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

► *Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 403).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 403).
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

kaspersky

# Диагностическое окно

В этом разделе описано использование диагностического окна для просмотра статуса или текущей активности защищаемого устройства и настройка записи файлов дампов и файлов трассировки.

## В этом разделе


О диагностическом окне ..... 211

Просмотр состояния Kaspersky Embedded Systems Security для Windows с помощью диагностического окна ..... 212

Просмотр статистики событий безопасности ..... 213

Просмотр текущей активности программы ..... 214

Настройка записи файлов дампов и файлов трассировки ..... 215


## О диагностическом окне

Компонент Диагностическое окно (далее также CDI) устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы и может быть использован, даже если Консоль программы не установлена на защищаемом устройстве. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на защищаемом устройстве.

В диагностическом окне можно выполнять следующие действия:

- просматривать информацию об общем статусе программы (см. раздел "Просмотр состояния Kaspersky Embedded Systems Security для Windows с помощью диагностического окна" на стр. 212);
- просматривать произошедшие инциденты безопасности (см. раздел "Просмотр статистики событий безопасности" на стр. 213);
- просматривать текущую активность на защищаемом устройстве (см. раздел "Просмотр текущей активности программы" на стр. 214);
- запускать и останавливать запись файлов дампов и файлов трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 215);
- открывать Консоль программы;
- открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Embedded Systems Security для Windows защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

# Просмотр состояния Kaspersky Embedded Systems Security для Windows с помощью диагностического окна

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

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

   Откроется **Диагностическое окно**.

На закладке **Статус защиты** можно просмотреть текущий статус ключа, а также статус задач постоянной защиты компьютера и задач обновления. Для уведомления о состояниях защиты используется цветовая индикация (см. таблицу ниже).

*Таблица 41. Статус защиты в диагностическом окне*

| Раздел | Состояние |
|---|---|
| **Статус постоянной защиты** | Панель *зеленого* цвета отображается при любом из следующих сценариев (при выполнении любого из условий):<br>• Рекомендуемая конфигурация:<br>  • Задача Постоянная защита файлов запущена с параметрами по умолчанию.<br>  • Задача Контроль запуска программ запущена в режиме **Активный** с параметрами по умолчанию.<br>• Приемлемая конфигурация:<br>  • Задача Постоянная защита файлов настроена пользователем.<br>  • Параметры задачи Контроль запуска программ изменены. |
| | Панель *желтого* цвета отображается, если выполнено одно или несколько из следующих условий:<br>• Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию).<br>• Задача Контроль запуска программ запущена в режиме **Только статистика**.<br>• Защита от эксплойтов и задача Контроль запуска программ запущены в режиме **Только статистика**. |
| | Панель *красного* цвета отображается, если выполнены оба условия:<br>• Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена.<br>• Компонент Контроль запуска программ не установлен или задача запущена в режиме **Только статистика**. |

| Раздел | Состояние |
|---|---|
| **Лицензирование** | Панель *зеленого* цвета отображается при действующей лицензии. |
| | Панель *желтого* цвета отображается, если возникло одно из следующих событий:<br>• *Выполняется проверка статуса лицензии*.<br>• *До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации.*<br>• *Добавленный ключ помещен в список запрещенных и будет заблокирован.* |
| | Панель *красного* цвета отображается, если возникло одно из следующих событий:<br>• *Программа не активирована*<br>• *Срок действия лицензии истек*<br>• *Нарушено Лицензионное соглашение*<br>• *Ключ добавлен в запрещенный список* |
| **Обновление** | Панель *зеленого* цвета отображается, если базы программы актуальны. |
| | Панель *желтого* цвета отображается, если базы программы устарели. |
| | Панель *красного* цвета отображается, если базы программы сильно устарели. |

# Просмотр статистики событий безопасности

На закладке **Статистика** отображаются все события безопасности. Статистика каждой задачи защиты отображается в отдельном блоке, где указано количество инцидентов, а также дата и время возникновения последнего инцидента. При регистрации инцидента цвет блока меняется на красный.

► *Чтобы просмотреть статистику, выполните следующие действия:*

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

   Откроется **Диагностическое окно**.
3. Выберите закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

# Просмотр текущей активности программы

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

Для отображения статуса активности программы используется цветовая индикация:

- В разделе **Задачи**:
  - *Зеленый цвет*. Не выполнены условия, при которых требовалась бы индикация красным цветом.
  - *Желтый цвет*. Проверка важных областей не проводилась давно.
  - *Красный цвет*. Выполнено как минимум одно из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В разделе **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

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

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

   Откроется **Диагностическое окно**.
3. Выберите закладку **Текущая активность программы**.
4. В разделе **Задачи** ознакомьтесь со следующей информацией:
   - **Проверка важных областей давно не выполнялась**.

     Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
   - **Выполняется сейчас**.
   - **Завершены с ошибкой**.
   - **Следующий запуск определен по расписанию**.
5. В разделе **Kaspersky Security Network** ознакомьтесь со следующей информацией:
   - **Включено с запросами файловой репутации** или **Не используется**.
   - **Включено с запросами файловой репутации**, **включена отправка статистики KSN.**
6. В разделе **Интеграция с Kaspersky Security Center** ознакомьтесь со следующей информацией:
   - **Разрешено локальное управление**.
   - **Применяется политика: <Имя Сервера администрирования>**.

# Настройка записи файлов дампов и файлов трассировки

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

Вы можете также настроить диагностику сбоев в Консоли программы (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 157).

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

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

   Откроется **Диагностическое окно**.
3. Выберите закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
   a. Установите флажок **Записывать отладочную информацию в файл трассировки**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы трассировки.

      Трассировка будет включена для всех компонентов с параметрами по умолчанию: уровнем детализации *Отладка* и максимальным размером файла журнала 50 МБ.
5. Если требуется, настройте следующие параметры записи файлов дампов:
   a. Установите флажок **Создавать файл дампа во время сбоя в указанной папке**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файл дампа.
6. Нажмите на кнопку **Применить**.

   Новая конфигурация будет применена.

# Обновление баз и модулей Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Embedded Systems Security для Windows, о копировании обновлений и об откате обновлений баз Kaspersky Embedded Systems Security для Windows, а также инструкции по настройке задач обновления баз и модулей программы.

## В этом разделе


О задачах обновления ... 216

Об обновлении модулей программы ... 217

Об обновлении баз программы ... 218

Схемы обновления баз и модулей антивирусных программ в организации ... 219

Настройка задач обновления ... 223

Откат обновления баз Kaspersky Embedded Systems Security для Windows ... 229

Откат обновления программных модулей ... 230

Статистика задач обновления ... 230


## О задачах обновления

В Kaspersky Embedded Systems Security для Windows предусмотрено четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Embedded Systems Security для Windows соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского" – каждый час. Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. 223), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Embedded Systems Security для Windows применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

**Обновление баз программы**

По умолчанию Kaspersky Embedded Systems Security для Windows копирует базы из источника обновлений на устройство и сразу переходит к их использованию в выполняющейся задаче Постоянная защита компьютера. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Embedded Systems Security для Windows запускает задачу Обновление баз программы каждый час.

**Обновление модулей программы**

По умолчанию Kaspersky Embedded Systems Security для Windows проверяет доступность обновлений модулей программы в источнике обновлений. Для использования установленных программных модулей требуется перезагрузка защищаемого устройства и / или перезапуск Kaspersky Embedded Systems Security для Windows.

По умолчанию Kaspersky Embedded Systems Security для Windows запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого устройства). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Embedded Systems Security для Windows, не копируя их.

**Копирование обновлений**

По умолчанию в ходе выполнения задачи Kaspersky Embedded Systems Security для Windows загружает файлы обновлений баз программы и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

**Откат обновления баз программы**

В ходе выполнения задачи Kaspersky Embedded Systems Security для Windows возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

# Об обновлении модулей программы

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Embedded Systems Security для Windows. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные (критичные) пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Embedded Systems Security для Windows запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого устройства).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Embedded Systems Security для Windows с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника, копируя на него обновления без установки, а затем распределяя их на защищаемые устройства в сети. Чтобы копировать и сохранять обновления без установки, используйте задачу Копирование обновлений.

Перед установкой обновлений модулей, Kaspersky Embedded Systems Security для Windows создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Embedded Systems Security для Windows автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений.

На время установки полученных обновлений служба Kaspersky Security автоматически останавливается, а затем снова запускается.

# Об обновлении баз программы

Базы Kaspersky Embedded Systems Security для Windows, хранящиеся на защищаемом устройстве, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз программы представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения устройства к минимуму, рекомендуется регулярно получать обновления баз программы.

По умолчанию, если базы Kaspersky Embedded Systems Security для Windows не обновляются в течение недели с момента создания установленных обновлений баз, возникает событие *Базы программы устарели*. Если базы программы не обновляются в течение двух недель, возникает событие *Базы программы сильно устарели*. Информация об актуальности баз (см. раздел "Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security для Windows" на стр. 176) отображается в панели результатов узла **Kaspersky Embedded Systems Security для Windows** в дереве Консоли программы. Вы можете использовать общие параметры Kaspersky Embedded Systems Security для Windows, чтобы указать другое количество дней до возникновения этих событий. Вы можете также настроить уведомления администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. 281).

Kaspersky Embedded Systems Security для Windows загружает обновления баз и модулей программы с FTP- или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.

Можно загружать обновления на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника. На него будут копироваться обновления, а затем распространяться на защищаемые устройства. Если вы используете программу Kaspersky Security Center для централизованного управления защитой устройств в организации, можно использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз программы вручную или по расписанию (см. раздел "Настройка параметров расписания задач" на стр. 165). По умолчанию Kaspersky Embedded Systems Security для Windows запускает задачу Обновление баз программы каждый час.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Embedded Systems Security для Windows автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Embedded Systems Security для Windows можно вручную откатить (см. раздел "Откат обновления баз Kaspersky Embedded Systems Security для Windows" на стр. 229) базы до ранее установленных обновлений.

# Схемы обновления баз и модулей антивирусных программ в организации

Выбор источника обновлений в задачах обновления зависит используемой в организации схемы обновления баз и модулей программы.

Вы можете обновлять базы и модули Kaspersky Embedded Systems Security для Windows на защищаемых устройствах по следующим схемам:

- загружать обновления напрямую из интернета на каждое защищаемое устройство (схема 1);
- Загружать обновления из интернета на устройство-посредник и распределять обновления на защищаемые устройства с этого устройства.

  Посредником может служить любое устройство, на котором установлены следующие программы:

  - Kaspersky Embedded Systems Security для Windows (схема 2).
  - Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через устройство-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность защищаемых устройств в сети.

Перечисленные схемы обновлений описаны ниже.

**Схема 1. Обновление баз и модулей программы напрямую из интернета**

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security для Windows напрямую из интернета,*

на каждом защищаемом устройстве в параметрах задач Обновление баз программы и Обновление модулей программы укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.

Вы можете указать в качестве источников обновлений другие HTTP- или FTP-серверы, на которых имеется папка обновлений.

**Схема 2. Обновление баз и модулей программы через одно из защищаемых устройств**

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security для Windows через одно из защищаемых устройств, выполните следующие действия:*

1. Скопируйте обновления на выбранное защищаемое устройство. Для этого выполните следующие действия:
   - На выбранном защищаемом устройстве настройте параметры задачи Копирование обновлений:
     a. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».
     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.
2. Распределите обновления на остальные защищаемые устройства. Для этого выполните следующие действия:
   - На каждом из защищаемых устройств настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже):
     a. В качестве источника обновлений укажите папку на диске устройства-посредника, в которую будут загружаться обновления.

Kaspersky Embedded Systems Security для Windows будет получать обновления через одно из защищаемых устройств.

**Схема 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center**

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств, можно загружать обновления с помощью Сервера администрирования Kaspersky Security Center, установленного в локальной сети (см. рис. ниже).

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security для Windows через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с серверов обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора защищаемых устройств:
     a. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».

2. Распределите обновления на защищаемые устройства. Для этого выполните одно из следующих действий:
   - Настройте на Сервере администрирования Kaspersky Security Center групповую задачу обновления для распределения обновлений на защищаемые устройства:
     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

     Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

     Частоту запуска **После получения обновлений Сервером администрирования** нельзя указать в Консоли программы.

   - Настройте на каждом из защищаемых устройств задачи Обновление баз программы и Обновление модулей программы:
     a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.
     b. Если требуется, настройте расписание задачи.

     При редких обновлениях антивирусных баз Kaspersky Embedded Systems Security для Windows (от одного раза в месяц до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

   Kaspersky Embedded Systems Security для Windows будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых устройств Агент администрирования – программный компонент, входящий в комплект поставки Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Embedded Systems Security для Windows на защищаемом устройстве. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

kaspersky

# Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security для Windows ..... 223

Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы ..... 226

Настройка параметров задачи Копирование обновлений ..... 227

Настройка параметров задачи Обновление модулей программы ..... 228


## Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security для Windows

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, можно указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► *Чтобы указать тип источника обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Источник обновлений** выберите тип источника обновлений Kaspersky Embedded Systems Security для Windows:

   - **Сервер администрирования Kaspersky Security Center**

     Kaspersky Embedded Systems Security для Windows использует Сервер администрирования Kaspersky Security Center в качестве источника обновления.

     Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" осуществляется с помощью системы удаленного доступа Kaspersky Security Center и на защищаемом устройстве установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь защищаемых устройств с Сервером администрирования.

- **Серверы обновлений «Лаборатории Касперского»**

  Kaspersky Embedded Systems Security для Windows использует в качестве источников обновлений веб-сайты "Лаборатории Касперского". На этих веб-сайтах публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

  Этот вариант выбран по умолчанию.

- **Другие HTTP-, FTP-серверы или сетевые ресурсы**

  Kaspersky Embedded Systems Security для Windows использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы или папки на серверах локальной сети.

  Вы можете сформировать список источников, которые содержат актуальный набор обновлений, перейдя по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:

   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

      i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.

      ii. Нажмите на кнопку **OK**.

   b. В разделе **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны**.

      Флажок включает или выключает функцию использования серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные вами источники обновлений недоступны.

      Если флажок установлен, функция активна.

      По умолчанию флажок установлен.

      Вы можете установить флажок **Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны**, когда выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского»**.

     Флажок включает или выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского" или если установлен флажок **Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны**.

     Если флажок установлен, используются параметры прокси-сервера.

     По умолчанию флажок установлен.

- Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

  Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

  Если флажок установлен, используются параметры прокси-сервера.

  По умолчанию флажок снят.

Информация о настройке дополнительных параметров прокси-сервера и параметров аутентификации для доступа к прокси-серверу приведена в разделе Запуск и настройка задачи Обновление баз программы.

7. Нажмите на кнопку **OK**.

Настроенные параметры источника обновлений Kaspersky Embedded Systems Security для Windows будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Embedded Systems Security для Windows.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.
5. Выполните следующие действия:
   - Чтобы добавить новый пользовательский источник обновления, нажмите на кнопку **Добавить** и в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере. Укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

     По умолчанию добавленная папка используется в качестве источника обновлений.
   - Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
   - Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
   - Чтобы изменить очередность обращения Kaspersky Embedded Systems Security для Windows к пользовательским источникам обновлений, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, когда он должен использоваться: до или после других источников.

- Чтобы изменить путь к пользовательскому источнику обновлений, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
- Чтобы удалить пользовательский источник обновлений, выберите его в списке и нажмите на кнопку **Удалить**.

Вы не можете удалить единственный пользовательский источник из списка.

6. Нажмите на кнопку **OK**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

## Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Embedded Systems Security для Windows размещает файлы обновлений на локальном диске защищаемого устройства. Вы можете снизить нагрузку на дисковую подсистему защищаемого устройства за счет размещения файлов обновлений на виртуальном диске в оперативной памяти при выполнении задачи обновления.

Эта функция доступна для операционных систем Microsoft Windows 7 и выше.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

► *Чтобы снизить нагрузку на дисковую подсистему защищаемого устройства при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Обновление баз программы**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Оптимизация использования дисковой подсистемы** настройте следующие параметры:
   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

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

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.

- В поле **Объем оперативной памяти, используемой для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

  При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

  - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

    В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

  - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

    В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

## Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Копирование обновлений**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security для Windows" на стр. 223).
5. На закладке **Общие** в разделе **Параметры копирования обновлений** выполните следующие действия:

   - Укажите условия копирования обновлений программы:

     - **Копировать обновления баз программы**.

       Kaspersky Embedded Systems Security для Windows загружает только обновления баз Kaspersky Embedded Systems Security для Windows.

       Этот вариант выбран по умолчанию.

- **Копировать критические обновления модулей программы**.

  Kaspersky Embedded Systems Security для Windows загружает только срочные обновления программных модулей Kaspersky Embedded Systems Security для Windows.

- **Копировать обновления баз программы и критические обновления модулей программы**.

  Kaspersky Embedded Systems Security для Windows загружает обновления баз и срочные обновления программных модулей Kaspersky Embedded Systems Security для Windows.

- Укажите локальную или сетевую папку, в которую Kaspersky Embedded Systems Security для Windows будет копировать полученные обновления.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

## Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Обновление модулей программы**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security для Windows" на стр. 223).
5. На закладке **Общие** в разделе **Параметры обновления** настройте параметры обновления модулей программы:

   - **Только проверять наличие доступных критических обновлений модулей программы**

     Kaspersky Embedded Systems Security для Windows отображает уведомление об имеющихся срочных обновлениях программных модулей без загрузки обновлений. Уведомление отображается, если включено оповещение о событиях этого типа.

     Этот вариант выбран по умолчанию.

   - **Копировать и устанавливать критические обновления модулей программы**

     Kaspersky Embedded Systems Security для Windows загружает и устанавливает критические обновления программных модулей.

- **Разрешать перезагрузку компьютера**

  Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows выполняет перезагрузку операционной системы после установки обновлений, требующих перезагрузки.

  Флажок активен, если выбран вариант **Копировать и устанавливать критические обновления модулей программы**.

  По умолчанию флажок снят.

- **Получать информацию о доступных плановых обновлениях модулей программы**

  Отображаются уведомления обо всех плановых обновлениях программных модулей Kaspersky Embedded Systems Security для Windows, доступных в источнике обновлений. Программа отображает уведомление, если для данного типа событий включены уведомления.

  Если флажок установлен, отображается уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165). По умолчанию Kaspersky Embedded Systems Security для Windows запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого устройства).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступны критические и плановые обновления*, в котором будет содержаться адрес веб-страницы, откуда можно загрузить плановые обновления.

# Откат обновления баз Kaspersky Embedded Systems Security для Windows

Перед обновлением баз Kaspersky Embedded Systems Security для Windows создает резервные копии баз, которые использовались ранее. Если обновление было прервано или завершилось с ошибкой, Kaspersky Embedded Systems Security для Windows автоматически возвращается к использованию ранее установленных баз.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз программы.

► *Чтобы запустить задачу Откат обновления баз программы,*

В панели результатов узла **Откат обновления баз программы** нажмите на ссылку **Запустить**.

# Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Embedded Systems Security для Windows создает резервные копии модулей, используемых в текущий момент. Если обновление модулей было прервано или завершилось с ошибкой, Kaspersky Embedded Systems Security для Windows автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте функцию Microsoft Windows **Установка и удаление программ**.

# Статистика задач обновления

Во время выполнения задачи обновления вы отображается актуальная информация об объеме данных, загруженных с момента запуска задачи, а также прочая информация о выполнении задачи.

После завершения или остановки задачи эта информация доступна в журнале выполнения задачи.

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

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

Если вы просматриваете задачу Обновление баз программы или Копирование обновлений, в разделе **Статистика** отображается объем данных, загруженных Kaspersky Embedded Systems Security для Windows на текущий момент (**Полученные данные**).

В следующей таблице приведена подробная информация о задаче Обновление модулей программы.

*Таблица 42. Информация о задаче Обновление модулей программы*

| Поле | Описание |
|---|---|
| **Полученные данные** | Общий объем полученных данных |
| **Доступно критических обновлений** | Количество критических обновлений, доступных для установки |
| **Доступно плановых обновлений** | Количество плановых обновлений, доступных для установки |
| **Ошибок применения обновлений** | Если значение этого поля отличается от нуля, обновление не было применено. Название обновления, вызвавшего ошибку, можно посмотреть в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач" на стр. 263). |

kaspersky

# Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

## В этом разделе


Изолирование возможно зараженных объектов. Карантин ..... 232

Резервное копирование объектов. Резервное хранилище ..... 243

Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы ..... 250


# Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

## В этом разделе


Об изолировании возможно зараженных объектов ..... 232

Просмотр объектов на карантине ..... 233

Проверка объектов на карантине ..... 235

Восстановление содержимого карантина ..... 236

Помещение объектов на карантин ..... 238

Удаление объектов с карантина ..... 239

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского" ..... 239

Настройка параметров карантина ..... 241

Статистика карантина ..... 242


## Об изолировании возможно зараженных объектов

Kaspersky Embedded Systems Security для Windows перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.

kaspersky

# Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов на карантине,*

отсортируйте объекты (см. раздел "Сортировка объектов на карантине" на стр. 233) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. 234).

## В этом разделе


Сортировка объектов на карантине ..... 233

Фильтрация объектов на карантине..... 234


## Сортировка объектов на карантине

По умолчанию объекты на карантине отсортированы в таблице по дате помещения на карантин в обратном хронологическом порядке. Чтобы найти нужный объект, можно отсортировать объекты по столбцам с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок столбца, по которому вы хотите отсортировать объекты в таблице.

Объекты в таблице писке будут отсортированы по выбранному параметру.

## Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, можно отфильтровать объекты в таблице – отобразить только те объекты, которые удовлетворяют заданным критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать фильтры, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в таблице могут различаться в зависимости от значения, выбранного в списке **Название поля**.
   c. В поле **Значение поля** введите или выберите в списке значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:
   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
   - Чтобы изменить фильтр, выберите фильтр в списке в окне **Параметры фильтра**. Отредактируйте требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.
5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы вернуть отображение всех объектов на карантине,*

в контекстном меню узла **Снять фильтр** выберите пункт **Карантин**.

## Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Embedded Systems Security для Windows выполняет локальную системную задачу Проверка объектов на карантине. Параметры задачи приведены в следующей таблице. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Можно настраивать расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Embedded Systems Security для Windows может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Embedded Systems Security для Windows может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

*Таблица 43. Параметры задачи Проверка объектов на карантине*

| Параметр задачи Проверка объектов на карантине | Значение |
|---|---|
| Область проверки. | Папка карантина |
| Параметры безопасности. | Единые для всей области проверки (значения приводятся в следующей таблице) |

*Таблица 44. Параметры безопасности в задаче Проверка объектов на карантине*

| Параметр безопасности | Значение |
|---|---|
| **Проверять объекты** | Все объекты области проверки |
| **Оптимизация** | Выключено |
| **Действия над зараженными и другими обнаруженными объектами** | Лечить, удалять, если лечение невозможно |
| **Действия над возможно зараженными объектами** | Пропускать |
| **Исключать файлы** | Нет |
| **Не обнаруживать** | Нет |
| **Останавливать проверку, если она длится более (сек.)** | Не задано |
| **Не проверять объекты размером более (МБ)** | Не задано |

| Параметр безопасности | Значение |
|---|---|
| **Альтернативные потоки NTFS** | Включено |
| **Загрузочные секторы дисков и MBR** | Выключено |
| **Использовать технологию iChecker** | Выключено |
| **Использовать технологию iSwift** | Выключено |
| **Проверять составные объекты** | • **Архивы***<br>• **SFX-архивы***<br>• **Упакованные объекты***<br>• **Вложенные OLE-объекты***<br>* **Проверка только новых и измененных файлов** выключена. |
| **Проверять подпись Microsoft у файлов** | Не выполняется |
| **Использовать эвристический анализатор** | Включено с уровнем анализа **Глубокий** |
| **Доверенная зона** | Не применяется |

## Восстановление содержимого карантина

Kaspersky Embedded Systems Security для Windows помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстановить любой объект с карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Embedded Systems Security для Windows не изолировала этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать файлы** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в Доверенную зону (см. раздел "Доверенная зона" на стр. 619).

При восстановлении объектов можно выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом устройстве, в указанной папке на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению защищаемого устройства.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Embedded Systems Security для Windows не включает его в составной объект при восстановлении. Объект, помещенный на карантин, сохраняется отдельно в выбранную папку.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты с карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.
   - Чтобы восстановить несколько объектов, выберите нужные объекты, используя клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.
4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.
5. Выполните одно из следующих действий:
   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере**, а затем выберите нужную папку или укажите путь к ней.
6. Чтобы сохранить копию объекта в папке *Карантин* после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security для Windows начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security для Windows:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Применить ко всем выбранным объектам** или **Заменить**, к остальным выбранным объектам, установите флажок **Переименовать**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

   Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

## Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows поместит указанный файл на карантин.

## Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Embedded Systems Security для Windows автоматически удаляет из папки карантина объекты, статус которых изменился на *Зараженный или обнаруживаемый* при проверке карантина с использованием обновленных баз, если программа Kaspersky Embedded Systems Security для Windows не смогла их вылечить. Kaspersky Embedded Systems Security для Windows не удаляет остальные объекты из карантина.

Можно удалять объекты с карантина.

► *Чтобы удалить объекты с карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены с карантина.

## Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Embedded Systems Security для Windows признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Embedded Systems Security для Windows признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы с карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Нельзя отправлять объекты с карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

► *Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:*

1. Если файл не находится на карантине, предварительно поместите его на **Карантин**.
2. В узле **Карантин** откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.
3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.
4. Если на защищаемом устройстве, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** содержит адрес электронной почты "Лаборатории Касперского" – newvirus@kaspersky.com. Поле Тема содержит текст "Объект карантина".

   Текст сообщения содержит следующую информацию: "Этот файл будет отправлен на анализ в "Лабораторию Касперского". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

   К сообщению будет приложен архив <имя объекта>.cab. Архив содержит файл <uuid>.klq с зашифрованным объектом, файл <uuid>.txt с информацией об объекте, полученной из Kaspersky Embedded Systems Security для Windows, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Embedded Systems Security для Windows и операционной системе защищаемого устройства:

   - название и версию операционной системы;
   - название и версию Kaspersky Embedded Systems Security для Windows;
   - дату выпуска последних установленных обновлений баз программы;
   - активный ключ.

   Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и более эффективно проанализировать файл. Однако если вы не хотите передавать эту информацию, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на защищаемом устройстве, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл можно переслать в "Лабораторию Касперского" самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **OK**.
2. Выберите папку на диске защищаемого устройства или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

## Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

► *Чтобы настроить параметры карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Карантин: свойства** настройте параметры карантина в соответствии с вашими требованиями:
   - В разделе **Параметры карантина**:
     - **Папка карантина**

       Путь к папке карантина в формате UNC (Universal Naming Convention).

       По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Quarantine\.
     - **Максимальный размер карантина (МБ)**

       Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security для Windows регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows отслеживает суммарный размер размещенных в карантине объектов.

       Если флажок снят, Kaspersky Embedded Systems Security для Windows не отслеживает суммарный размер объектов в карантине.

       По умолчанию флажок снят.
     - **Порог доступного пространства (МБ)**

       Флажок включает или выключает отслеживание минимального объема свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Embedded Systems Security для Windows регистрирует событие *Превышен порог свободного места в папке карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows отслеживает размер свободного места в папке карантина.

       Флажок **Порог доступного пространства (МБ)** активен, если установлен флажок **Максимальный размер карантина (МБ)**.

       По умолчанию флажок установлен.

Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Embedded Systems Security для Windows уведомит вас об этом, не переставая помещать объекты на карантин.

- В разделе **Параметры восстановления объектов**:
  - **Папка, в которую восстанавливаются объекты**

    Путь к папке, в которую восстанавливаются объекты, в формате UNC (Universal Naming Convention).

    Путь по умолчанию: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры карантина будут сохранены.

## Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в дереве Консоли программы в контекстном меню узла **Карантин** выберите пункт **Статистика**.

В окне **Статистика карантина** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

| Поле | Описание |
|---|---|
| **Возможно зараженных объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows признала возможно зараженными. |
| **Текущий размер карантина** | Общий объем данных в папке карантина. |
| **Ложных срабатываний** | Количество объектов, которым присвоен статус *Ложное срабатывание*, поскольку при проверке карантина с применением обновленных баз они были признаны незараженными. |
| **Вылечено объектов** | Количество объектов, которым присвоен статус *Вылечен* после проверки карантина. |
| **Всего объектов** | Общее количество объектов на карантине. |

kaspersky

# Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

## В этом разделе


О резервном копировании объектов перед лечением или удалением ..... 243

Просмотр объектов в резервном хранилище ..... 244

Восстановление файлов из резервного хранилища ..... 245

Удаление файлов из резервного хранилища ..... 247

Настройка параметров резервного хранилища ..... 248

Статистика резервного хранилища ..... 249


## О резервном копировании объектов перед лечением или удалением

Kaspersky Embedded Systems Security для Windows сохраняет зашифрованные копии объектов со статусом *Зараженный* в папке *Резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Embedded Systems Security для Windows сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Embedded Systems Security для Windows признает зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Embedded Systems Security для Windows помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Можно восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом устройстве или другом устройстве в локальной сети организации. Вы можете восстановить файл из резервного хранилища, если зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Embedded Systems Security для Windows не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

# Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только с помощью узла **Резервное хранилище** Консоли программы. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов в резервном хранилище,*

отсортируйте объекты или отфильтруйте их.

## В этом разделе

Сортировка файлов в резервном хранилище ..... 244
Фильтрация файлов в резервном хранилище ..... 244

## Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их попадания в резервное хранилище в обратном хронологическом порядке. Чтобы найти нужный файл, отсортируйте файлы по содержимому любого столбца в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В таблице файлов в узле **Резервное хранилище** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

## Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

2. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут различаться в зависимости значения, выбранного в поле **Название поля**.

   c. В поле **Значение поля** введите или выберите в списке значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
   - Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.

   После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► *Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,*

в контекстном меню узла **Снять фильтр** выберите пункт **Резервное хранилище**.

## Восстановление файлов из резервного хранилища

Kaspersky Embedded Systems Security для Windows хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный зараженный файл содержал важную информацию и при лечении файла программа Kaspersky Embedded Systems Security для Windows не смогла сохранить его целостность, в результате чего информация в файле стала недоступной;

- если вы считаете файл безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Embedded Systems Security для Windows не признавала файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите файл в качестве значения параметра **Исключать файлы** или **Не обнаруживать** соответствующих задач.

  Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходное местоположение (по умолчанию), в специальную папку для восстановленных объектов на защищаемом устройстве, в указанную папку на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 248).

По умолчанию, когда Kaspersky Embedded Systems Security для Windows восстанавливает файл, его копия сохраняется в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.
   - Чтобы восстановить несколько объектов, выберите нужные объекты, используя клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.
4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.
5. Выполните одно из следующих действий:
   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.

- Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалить объекты из хранилища после восстановления** (по умолчанию флажок снят).
7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере**, все объекты будут сохранены в одну указанную папку.
8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security для Windows начнет восстанавливать первый из выбранных вами объектов.
9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security для Windows:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Применить ко всем выбранным объектам** или **Заменить**, к остальным выбранным объектам, установите флажок **Переименовать**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

## Удаление файлов из резервного хранилища

► *Чтобы удалить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

3. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

## Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Резервное хранилище: свойства** настройте параметры резервного хранилища в соответствии с вашими требованиями:

   В разделе **Параметры резервного хранилища**:

   - **Папка резервного хранилища**

     Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

     По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Backup\.

   - **Максимальный размер резервного хранилища (МБ)**

     Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security для Windows регистрирует событие *Превышен максимальный размер резервного хранилища* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows отслеживает суммарный размер размещенных в резервном хранилище объектов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не отслеживает суммарный размер объектов в резервном хранилище.

     По умолчанию флажок снят.

   - **Порог доступного пространства (МБ)**

     Флажок включает или выключает отслеживание минимального объема свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Embedded Systems Security для Windows регистрирует событие *Превышен порог доступного пространства в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

Если флажок установлен, Kaspersky Embedded Systems Security для Windows отслеживает размер свободного места в резервном хранилище.

Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

По умолчанию флажок установлен.

Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Embedded Systems Security для Windows уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В разделе **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**

  Путь к папке, в которую восстанавливаются объекты, в формате UNC (Universal Naming Convention).

  Путь по умолчанию: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

## Статистика резервного хранилища

Можно просматривать информацию о текущем состоянии резервного хранилища – статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

*Таблица 45. Информация о текущем состоянии резервного хранилища*

| Поле | Описание |
|---|---|
| **Текущий размер резервного хранилища** | Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде |
| **Всего объектов** | Количество объектов в резервном хранилище в текущий момент |

# Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры списка заблокированных сетевых сеансов.

## В этом разделе


Список заблокированных сетевых сеансов ..... 250

Управление списком заблокированных сетевых сеансов с помощью Плагина управления ..... 251

Управление списком заблокированных сетевых сеансов с помощью Консоли программы ..... 253

Управление списком заблокированных сетевых сеансов с помощью Веб-плагина ..... 255


## Список заблокированных сетевых сеансов

По умолчанию Список заблокированных сетевых сеансов доступен, если установлен хотя бы один из следующих компонентов: Постоянная защита файлов, Защита от сетевых угроз. Эти компоненты обнаруживают удаленные попытки зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных сетевых сеансов. Информация о заблокированных сетевых сеансах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Embedded Systems Security для Windows блокирует текущий сеанс и делает недоступными общие папки или папки сетевого хранилища в рамках текущего сеанса.

Список заблокированных сетевых сеансов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать сетевые сессии, с которых ведется вредоносная деятельность**.
- Для задачи Защита от сетевых угроз: обнаружена активность, характерная для сетевых атак.

При обнаружении вредоносной активности или попыток шифрования задача отправляет информацию об атакующем сетевом сеансе в Список заблокированных сетевых сеансов, а для текущего сеанса атакующего устройства создается событие *Предупреждение*. Все попытки данного сеанса получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локальный уникальный идентификатор (LUID) узла, инициировавшего атакующий сетевой сеанс, добавлен в Список заблокированных сетевых сеансов, Kaspersky Embedded Systems Security для Windows определяет IP-адрес этого узла и добавляет его в Список заблокированных сетевых сеансов вместо идентификатора LUID атакующего узла.

По умолчанию Kaspersky Embedded Systems Security для Windows удаляет заблокированные сетевые сеансы из списка через 30 минут после добавления. Доступ к сетевым файловым ресурсам восстанавливается автоматически после удаления сетевых сеансов из Списка заблокированных сетевых сеансов. Вы можете указать период, после которого заблокированные сетевые сеансы автоматически разблокируются.

kaspersky

В случае запрета доступа к управлению хранилищами какому-либо пользователю, Список заблокированных сетевых сеансов останется доступным. Параметры заблокированных сетевых сеансов не могут быть изменены, если у пользователя отсутствует разрешение типа **Права на изменение** для управления Kaspersky Embedded Systems Security для Windows.

# Управление списком заблокированных сетевых сеансов с помощью Плагина управления

В этом разделе описано, как настроить параметры Списка заблокированных сетевых сеансов с помощью интерфейса Плагина управления.

## В этом разделе


Включение блокировки недоверенных узлов ..... 251

Настройка параметров списка заблокированных сетевых сеансов ..... 252


## Включение блокировки недоверенных узлов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в **Список заблокированных сетевых сеансов** и заблокировать доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

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

1. В 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 разделе **Интеграция с другими компонентами** установите флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных**, если требуется, чтобы программа Kaspersky Embedded Systems Security для Windows 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 была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
5. В окне **Постоянная защита компьютера** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

► *Настройте задачу Защита от сетевых угроз:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.
7. Выберите закладку **Общие**.
8. В разделе **Режим работы** выберите режим **Блокировать соединения при обнаружении атаки**.
9. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
10. В окне нажмите на кнопку **OK**.
11. Настроенные параметры задачи будут сохранены.

## Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Параметры хранилищ**.

5. В разделе **Условия блокировки сетевых сессий** на закладке **Заблокированные сетевые сессии** укажите количество дней, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.
6. Нажмите на кнопку **OK**.

# Управление списком заблокированных сетевых сеансов с помощью Консоли программы

В этом разделе описано, как настроить параметры списка заблокированных сетевых сеансов с помощью интерфейса Консоли программы.

## В этом разделе

Включение блокировки недоверенных узлов ..... 253
Настройка параметров списка заблокированных сетевых сеансов ..... 254

## Включение блокировки недоверенных узлов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в **Список заблокированных сетевых сеансов** и заблокировать доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В разделе **Глубокий** установите флажок **Блокировать сетевые сессии, с которых ведется вредоносная деятельность**, чтобы программа Kaspersky Embedded Systems Security для Windows блокировала сетевые сеансы, проявляющие вредоносную активность, во время выполнения задачи Постоянная защита файлов.
5. Если задача не была запущена, выберите закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
6. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

► *Настройте задачу Защита от сетевых угроз:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от сетевых угроз**.
4. Откроется окно **Параметры задачи**.
5. Выберите закладку **Общие**.
6. В разделе **Режим работы** выберите режим **Блокировать соединения при обнаружении атаки**.
7. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
8. Если задача не была запущена, выберите закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
9. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

## Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированных сетевых сессий**.
3. Выберите пункт меню **Свойства**.

   Откроется окно **Параметры Списка заблокированных сетевых сессий**.
4. В разделе **Условия блокировки сетевых сессий** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.
5. Нажмите на кнопку **OK**.
6. Чтобы восстановить доступ для всех заблокированных сетевых сеансов, выполните следующие действия:
   a. Откройте контекстное меню вложенного узла **Заблокированных сетевых сессий**.
   b. Выберите пункт **Разблокировать все**.

      Все сетевые сеансы будут удалены из списка и разблокированы.
7. Чтобы удалить сетевые сеансы из списка заблокированных, выполните следующие действия:
   a. В списке заблокированных сетевых сеансов в панели результатов выберите один или несколько сеансов.
   b. Откройте контекстное меню вложенного узла **Заблокированных сетевых сессий**.
   c. Выберите пункт **Разблокировать выбранное**.

      Выбранные сетевые сеансы будут разблокированы.

kaspersky

# Управление списком заблокированных сетевых сеансов с помощью Веб-плагина

В этом разделе описано, как настроить список заблокированных сетевых сеансов с помощью интерфейса Веб-плагина.

## В этом разделе


Включение блокировки сетевых сеансов ..... 255

Настройка параметров списка заблокированных сетевых сеансов ..... 256


## Включение блокировки сетевых сеансов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в **Заблокированных сетевых сессий** и заблокировать для них доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

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

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.
6. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**, чтобы программа Kaspersky Embedded Systems Security для Windows блокировала текущий сеанс и устанавливала недоступность общих сетевых ресурсов для сетевых сеансов, проявляющих вредоносную активность.
7. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
8. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

## Настройка параметров списка заблокированных сетевых сеансов

► *Чтобы настроить Список заблокированных сетевых сеансов, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Хранилища**.
6. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Хранилища**.
7. В разделе **Условия блокировки сетевых сессий** на закладке **Заблокированные сетевые сессии** укажите количество дней, часов и минут, по истечении которых с момента блокировки заблокированные сетевые сеансы получают доступ к сетевым файловым ресурсам.
8. Нажмите на кнопку **OK**.

kaspersky

# Запись событий. Журналы Kaspersky Embedded Systems Security для Windows

В этом разделе приведена информация о работе с журналами Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Способы записи событий Kaspersky Embedded Systems Security для Windows ..... 257

Журнал системного аудита ..... 258

Журналы выполнения задач ..... 260

Журнал безопасности ..... 265

Просмотр журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий" ..... 265

Настройка параметров журнала с помощью Консоли программы ..... 266

Настройка параметров журналов и уведомлений с помощью Плагина управления ..... 272


## Способы записи событий Kaspersky Embedded Systems Security для Windows

События Kaspersky Embedded Systems Security для Windows делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Embedded Systems Security для Windows;
- события, связанные с управлением Kaspersky Embedded Systems Security для Windows, например: запуск программы, создание или удаление задач, изменение параметров задач.

Kaspersky Embedded Systems Security для Windows использует следующие способы записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Embedded Systems Security для Windows.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security для Windows. Журнал событий доступен в "Просмотре событий" Microsoft Windows.
- **Журнал событий безопасности**. Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве.

Если в работе Kaspersky Embedded Systems Security для Windows возникла проблема (например, Kaspersky Embedded Systems Security для Windows или отдельная задача завершилась аварийно или не запустилась), то для ее диагностики можно создать файл трассировки и файл дампа процессов Kaspersky Embedded Systems Security для Windows и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security для Windows не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security для Windows. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Файлы, доступные для загрузки по следующим ссылкам, содержат таблицы с полными списками событий Kaspersky Embedded Systems Security для Windows следующих категорий:

- События, которые Kaspersky Embedded Systems Security для Windows записывает в журнал событий: https://support.kaspersky.com/help/KESS/3.3/ru-RU/KESS-WEL-EVENTS.ZIP
- События, которые Kaspersky Embedded Systems Security для Windows отправляет на Сервер администрирования: https://support.kaspersky.com/help/KESS/3.3/ru-RU/KESS-KSC-EVENTS.ZIP

# Журнал системного аудита

Kaspersky Embedded Systems Security для Windows ведет системный аудит событий, связанных с управлением Kaspersky Embedded Systems Security для Windows. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Embedded Systems Security для Windows, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли программы.

По умолчанию Kaspersky Embedded Systems Security для Windows хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которую Kaspersky Embedded Systems Security для Windows будет сохранять файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

kaspersky

## В этом разделе

Сортировка событий в журнале системного аудита ..... 259
Фильтрация событий в журнале системного аудита ..... 259
Удаление событий из журнала системного аудита ..... 260

# Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в списке событий.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

# Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита записи только о тех событиях, которые удовлетворяют заданным условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать события.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:
   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий журнале системного аудита.

   В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

   В списке событий журнала системного аудита отобразятся все события.

## Удаление событий из журнала системного аудита

По умолчанию Kaspersky Embedded Systems Security для Windows хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► *Чтобы удалить события из журнала системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.
3. Выполните одно из следующих действий:
   - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
   - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

# Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Embedded Systems Security для Windows и инструкции по работе с ними.

kaspersky

## В этом разделе


О журналах выполнения задач ... 261

Просмотр списка событий в журналах выполнения задач ... 261

Сортировка журналов выполнения задач ... 261

Фильтрация журналов выполнения задач ... 262

Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач ... 263

Экспорт информации из журнала выполнения задачи ... 264

Удаление журналов выполнения задач ... 264


# О журналах выполнения задач

Информация о выполнении задач Kaspersky Embedded Systems Security для Windows отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи можно просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи, а также параметры задачи.

По умолчанию Kaspersky Embedded Systems Security для Windows хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Embedded Systems Security для Windows сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Можно также выбрать события, записи о которых Kaspersky Embedded Systems Security для Windows сохраняет в журналах выполнения задач.

# Просмотр списка событий в журналах выполнения задач

► *Чтобы просмотреть журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.

   Список событий, сохраненных в журналах выполнения задач Kaspersky Embedded Systems Security для Windows, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

# Сортировка журналов выполнения задач

По умолчанию журналу выполнения задач отображаются в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать журналы выполнения задач Kaspersky Embedded Systems Security для Windows.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

## Фильтрация журналов выполнения задач

Вы можете настроить отображение в списке журналов выполнения задач только журналы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

► *Чтобы отфильтровать журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать журналы выполнения задач.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации в списке журналов выполнения задач.

В списке журналов выполнения задач отобразятся только журналы, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы выключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке журналов выполнения задач отобразятся все журналы.

## Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
4. В открывшемся окне отображается следующая информация:
   - На закладке **Статистика** отображается время запуска и завершения задачи и ее статистика.
   - На закладке **События** отображается список событий, зафиксированных во время выполнения задачи.
   - На закладке **Параметры** отображаются параметры задачи.
5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.
6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.
7. Нажмите на кнопку **Закрыть**.

Окно **Журнал выполнения** будет закрыто.

## Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.
4. В нижней части окна **Журнал выполнения** нажмите на кнопку **Экспорт**.

   Откроется окно **Сохранить как**.
5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

## Удаление журналов выполнения задач

По умолчанию Kaspersky Embedded Systems Security для Windows хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Можно вручную удалить журналы выполнения завершившихся задач.

> События из журналов задач, выполняющихся в данный момент, и задач, используемых другими пользователями, удалены не будут.

► *Чтобы удалить журналы выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Чтобы удалить журналы выполнения всех завершившихся задач, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Чтобы очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню журнала, который вы хотите очистить, и выберите пункт **Удалить**.

- Чтобы очистить журналы выполнения нескольких задач, выполните следующие действия:
  a. В панели результатов с помощью клавиш **CTRL** и **SHIFT** выберите журналы выполнения задач, которые вы хотите очистить.
  b. Откройте контекстное меню любого журнала выполнения задач и выберите пункт **Удалить**.

4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление журналов.

Выбранные журналы выполнения задач будут очищены. Удаление журналов выполнения задач будет зарегистрировано в журнале системного аудита.

# Журнал безопасности

Kaspersky Embedded Systems Security для Windows ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера и проверки по требованию, задач Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить журнал безопасности. При очистке журнала безопасности Kaspersky Embedded Systems Security для Windows регистрирует событие системного аудита.

# Просмотр журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий"

С помощью оснастки "Просмотр событий" в Microsoft Management Console можно просматривать журнал событий Kaspersky Embedded Systems Security для Windows. В журнале содержатся события, зарегистрированные Kaspersky Embedded Systems Security для Windows и необходимые для диагностики сбоев в работе программы.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий**;
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются все события. Наименее подробным является уровень Критические события, при котором регистрируются только критические события.

► *Чтобы просмотреть журнал событий Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется Microsoft Management Console.

2. Выберите **Файл** > **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите защищаемое устройство, на котором установлена программа Kaspersky Embedded Systems Security для Windows, и нажмите на кнопку **OK**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **OK**.

   В дереве Microsoft Management Console появится узел **Просмотр событий**.

6. В дереве Консоли раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб** > **Kaspersky Embedded Systems Security для Windows**.

Откроется журнал событий Kaspersky Embedded Systems Security для Windows.

# Настройка параметров журнала с помощью Консоли программы

Вы можете настраивать следующие параметры журналов Kaspersky Embedded Systems Security для Windows:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Embedded Systems Security для Windows сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*;
- события, которые Kaspersky Embedded Systems Security для Windows сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий";
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

► *Чтобы настроить параметры журналов с помощью Консоли программы:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На вкладке **Общие**, если требуется, выберите события, которые Kaspersky Embedded Systems Security для Windows сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий":

   a. В списке **Компонент** выберите компонент Kaspersky Embedded Systems Security для Windows, уровень детализации событий которого вы хотите указать.

   b. В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.

      В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

   c. Если вы хотите вручную включить запись отдельных событий для выбранного компонента или задачи:

      i. В списке **Уровень важности** выберите **Другой**.

      ii. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

3. На вкладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий для состояния защиты устройства:

   - В блоке **Хранение журналов**:

     - **Папка с журналами**;

       Путь к папке с журналами в формате UNC (Universal Naming Convention).

       По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports\.

       Если используемый по умолчанию путь изменился, создается папка с соответствующим именем. Новые файлы журналов будут сохранены в новую папку. Созданные ранее файлы журналов останутся в старой папке.

     - **Удалять события в журналах выполнения задач старше, чем (сут)**;

       Флажок включает или выключает функцию, которая удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени.

       По умолчанию флажок установлен.

- **Удалять события в журнале системного аудита старше, чем (сут)**.

  Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

  По умолчанию флажок снят.

- В блоке **Пороги формирования** укажите количество дней, по истечении которого будут регистрироваться события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.

*Таблица 46. Пороги формирования событий*

| **Параметр** | Пороги формирования событий. |
|---|---|
| **Описание** | Вы можете указать пороги формирования событий следующих типов:<br>*Базы программы устарели* и *Базы программы сильно устарели*. События возникают, если базы Kaspersky Embedded Systems Security для Windows не обновляются в течение указанного параметром количества дней с момента выпуска последних установленных обновлений баз. Вы можете настроить уведомление администратора об этих событиях.<br>*Проверка важных областей защищаемого устройства давно не выполнялась*. Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком **Считать выполнение задачи проверкой важных областей**. |
| **Возможные значения** | Количество дней от 1 до 365. |
| **Значение по умолчанию** | Базы программы устарели – 7 дней.<br>Базы программы сильно устарели – 14 дней.<br>Проверка важных областей давно не выполнялась – 30 дней. |

4. На вкладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере (см. раздел "Настройка параметров интеграции с SIEM" на стр. 270).
5. Нажмите на кнопку **OK**, чтобы сохранить изменения.

kaspersky

## В этом разделе

Об интеграции с SIEM ..... 269
Настройка параметров интеграции с SIEM ..... 270

# Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он хранит и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security для Windows может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

### Параметры надежности

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Также Kaspersky Embedded Systems Security для Windows использует события системного аудита для уведомления о неудачных попытках подключения к SIEM-серверу и об ошибках отправки событий на SIEM-сервер.

## Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

*Таблица 47. Параметры интеграции с SIEM*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Отправлять события по протоколу syslog на внешний syslog-сервер** | Не применяется | Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка. |
| **Удалять локальные копии событий при записи на внешний syslog-сервер** | Не применяется | Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок. |
| **Формат событий** | Структурированные данные | Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером. |
| **Протокол подключения** | TCP | Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UDP или TCP с помощью выпадающего списка. |
| **Параметры подключения к основному syslog-серверу** | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.<br>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<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4. |

► *Чтобы настроить параметры интеграции с SIEM:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.
3. Выберите вкладку **Интеграция с SIEM**.

4. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий на SIEM-сервер в соответствии с настроенными параметрами интеграции с SIEM.

   Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

   По умолчанию флажок снят.

5. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Флажок включает или выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

   Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

> Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

6. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В блоке **Параметры подключения**:

   - Укажите протокол подключения к SIEM.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к основному syslog-серверу.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к дополнительному syslog-серверу.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

# Настройка параметров журналов и уведомлений с помощью Плагина управления

В Консоли администрирования Kaspersky Security Center можно настроить уведомление администратора и пользователей о следующих событиях в работе Kaspersky Embedded Systems Security для Windows и с состоянием антивирусной защиты устройства:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому устройству, и пользователи терминального защищаемого устройства могут получать информацию о событиях *Обнаружен объект*.

Можно настроить уведомления о событиях Kaspersky Embedded Systems Security для Windows как для отдельного защищаемого устройства в окне **Свойства: <Имя защищаемого устройства>** выбранного защищаемого устройства, так и для группы защищаемых устройств в окне **Свойства: <Имя политики>** выбранной группы администрирования.

На закладке **Уведомления о событиях** или в окне **Настройка уведомлений** можно настроить следующие типы уведомлений:

- На закладке **Уведомления о событиях** (стандартная закладка в Kaspersky Security Center) можно настроить уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений приведена в *Справке Kaspersky Security Center*.
- В окне **Настройка уведомлений** можно настроить уведомления как администратора, так и пользователей.

Уведомления о событиях некоторых типов можно настраивать только на закладке или только в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите уведомления о событиях одного типа в одинаковом режиме на закладке **Уведомления о событиях** и в окне **Настройка уведомлений**, системный администратор будет получать уведомления об этих событиях дважды.

## В этом разделе


Настройка параметров журналов задач ..... 273

Журнал безопасности ..... 274

Настройка параметров интеграции с SIEM ..... 274

Настройка параметров уведомлений ..... 278

Настройка обмена информацией с Сервером администрирования ..... 279

## Настройка параметров журналов задач

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры журналов для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры журналов для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Журналы и уведомления** в блоке **Журналы выполнения задач** нажмите на кнопку **Настройка**.
5. Откроется окно **Параметры журналов** на вкладке **Журналы**.
6. Настройте уровень детализации событий в журналах:
   a. В списке **Компонент** выберите компонент Kaspersky Embedded Systems Security для Windows, уровень детализации событий которого вы хотите указать.
   b. В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.

      В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.
   c. Если вы хотите вручную включить запись отдельных событий для выбранного компонента или задачи:
      i. В списке **Уровень важности** выберите **Другой**.
      ii. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.
7. В блоке **Хранение журналов** настройте параметры хранения журналов:
   - **Папка с журналами**;

     Путь к папке с журналами в формате UNC (Universal Naming Convention).

     По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports\.

     Если используемый по умолчанию путь изменился, создается папка с соответствующим именем. Новые файлы журналов будут сохранены в новую папку. Созданные ранее файлы журналов останутся в старой папке.

- **Удалять события в журналах выполнения задач старше, чем (сут)**;

  Флажок включает или выключает функцию, которая удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows удаляет журналы выполнения завершенных задач и события, зарегистрированные в журналах выполняющихся задач, по истечении заданного периода времени.

  По умолчанию флажок установлен.

- **Удалять события в журнале системного аудита старше, чем (сут)**.

  Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

  По умолчанию флажок снят.

8. На вкладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере (см. раздел "Настройка параметров интеграции с SIEM" на стр. 274).
9. Нажмите на кнопку **OK**.

Настроенные параметры журналов будут сохранены.

## Журнал безопасности

Kaspersky Embedded Systems Security для Windows ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера и проверки по требованию, задач Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить журнал безопасности. При очистке журнала безопасности Kaspersky Embedded Systems Security для Windows регистрирует событие системного аудита.

## Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он хранит и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security для Windows может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

*Таблица 48. Параметры интеграции с SIEM*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Отправлять события по протоколу syslog на внешний syslog-сервер** | Не применяется | Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка. |
| **Удалять локальные копии событий при записи на внешний syslog-сервер** | Не применяется | Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок. |
| Формат событий | Структурированные данные | Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером. |
| Протокол подключения | TCP | С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам UDP или TCP, к дополнительному syslog-серверу по протоколу TCP. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Параметры подключения к основному syslog-серверу | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.<br>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<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4. |

► *Чтобы настроить параметры интеграции с SIEM:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры журналов для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры журналов для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Журналы и уведомления** в блоке **Настройка** нажмите на кнопку **Журналы выполнения задач**.

   Откроется окно **Параметры журналов и уведомлений**.
5. Выберите вкладку **Интеграция с SIEM**.
6. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий на SIEM-сервер в соответствии с настроенными параметрами интеграции с SIEM.

Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

По умолчанию флажок снят.

7. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Флажок включает или выключает удаление локальных копий журналов при их отправке на SIEM-сервер.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах.

   Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

8. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

9. В блоке **Параметры подключения**:

   - Укажите протокол подключения к SIEM.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к основному syslog-серверу.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.
   - В одноименных полях укажите адрес в формате IPv4 и порт для подключения к дополнительному syslog-серверу.

10. Нажмите на кнопку **OK**.

Настроенные параметры интеграции с SIEM будут применены.

## Настройка параметров уведомлений

► *Чтобы настроить уведомления Kaspersky Embedded Systems Security для Windows:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Журналы и уведомления** в подразделе **Настройка** нажмите на кнопку **Уведомления о событиях**.
5. В окне **Настройка уведомлений** настройте следующие параметры Kaspersky Embedded Systems Security для Windows согласно вашим требованиям:
   - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.
   - В разделе **Уведомление пользователей** настройте способ уведомления пользователей. Если требуется, задайте текст уведомления.
   - В разделе **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
   - В разделе **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Embedded Systems Security для Windows регистрирует события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.
     - **Базы программы устарели (сут);**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 7 дней.
     - **Базы программы сильно устарели (сут);**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 14 дней.
     - **Проверка важных областей защищаемого устройства давно не выполнялась (сут).**

       Количество дней с момента последнего успешного завершения задачи Проверка важных областей.

       По умолчанию установлено 30 дней.
6. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

## Настройка обмена информацией с Сервером администрирования

► *Чтобы выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security для Windows будет передавать на Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Журналы и уведомления** в подразделе **Настройка** нажмите на кнопку **Взаимодействие с Сервером администрирования**.

   Откроется окно **Взаимодействие с Сервером администрирования**.
5. В окне **Взаимодействие с Сервером администрирования** выберите типы объектов, информацию о которых Kaspersky Embedded Systems Security для Windows будет передавать на Сервер администрирования Kaspersky Security Center:
   - Объекты на карантине.
   - Резервные копии объектов.
6. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security для Windows будет передавать информацию о выбранных типах объектов на Сервер администрирования.

# Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Embedded Systems Security для Windows о событиях программы и о состоянии защиты устройства, а также инструкцию по настройке уведомлений.

## В этом разделе


Способы уведомления администратора и пользователей ..... 280

Настройка уведомлений администратора и пользователей ..... 281


## Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к устройству, о событиях, связанных с работой Kaspersky Embedded Systems Security для Windows, и о состоянии антивирусной защиты устройства.

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к устройству, и пользователи терминального устройства могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли программы можно активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения пользователей терминального защищаемого устройства, если защищаемое устройство является терминальным.

  b. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.
- Способы уведомления администраторов:
  a. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

  b. Запуск исполняемого файла.

     При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого устройства.

  c. Отправка по электронной почте.

     Этот способ использует для передачи сообщений электронную почту.

Вы можете составить текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

# Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► *Чтобы настроить уведомления о событиях, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** выберите способ уведомления:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Уведомление пользователя можно настроить только для следующих событий: **Обнаружен объект**, **Обнаружено и запрещено недоверенное устройство** и **Сетевая сессия добавлена в список недоверенных**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**.

   b. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после выбора способа уведомлений для одного типа событий, выберите остальные типы событий, для которых вы хотите использовать этот же текст сообщения, с помощью клавиш **CTRL** и **SHIFT**, а затем нажмите на кнопку **Текст сообщения**.

   c. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   d. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Чтобы настроить способы уведомления администраторов о выбранном событии, выберите закладку **Уведомления** и в разделе **Настройка** нажмите на кнопку **Уведомление администраторов**. Затем в окне **Дополнительные параметры** выполните настройку выбранных способов уведомления. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте выберите закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса точкой с запятой), имя или сетевой адрес SMTP-сервера и номер порта. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** можно также добавлять переменные с информацией о событии (см. таблицу ниже).

Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Использовать SMTP-аутентификацию** установите флажок **Параметры аутентификации** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

b. Для уведомлений средствами службы сообщений Windows составьте список защищаемых устройств, получающих уведомления, на закладке **Служба сообщений**: для каждого защищаемого устройства, которое вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите файл на локальном диске защищаемого устройства или введите полный путь к нему. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

   Если вы хотите ограничить количество уведомлений о событиях одного типа за период времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите количество экземпляров и период времени.

5. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

*Таблица 49. Поля с информацией о событии*

| Переменная | Описание |
|---|---|
| %EVENT_TYPE% | Тип события. |
| %EVENT_TIME% | Время возникновения события. |
| %EVENT_SEVERITY% | Уровень важности события. |
| %OBJECT% | Имя объекта (в задачах постоянной защиты компьютера и проверки по требованию).<br>В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении. |
| %VIRUS_NAME% | Имя объекта согласно классификации Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security для Windows возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач" на стр. 263). |
| %VIRUS_TYPE% | Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security для Windows возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи. |

| Переменная | Описание |
| --- | --- |
| %USER_COMPUTER% | В задачах Постоянная защита файлов имя защищаемого устройства пользователя, который обратился к объекту на устройстве. |
| %USER_NAME% | В задачах Постоянная защита файлов имя пользователя, который обратился к объекту на устройстве. |
| %FROM_COMPUTER% | Имя защищаемого устройства, с которого поступило уведомление. |
| %EVENT_REASON% | Причина возникновения события (некоторые события не имеют этого поля). |
| %ERROR_CODE% | Код ошибки (только для события "внутренняя ошибка задачи"). |
| %TASK_NAME% | Название задачи (имеется только у событий, связанных с выполнением задач). |

# Запуск и остановка Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security.

## В этом разделе


Запуск Плагина управления Kaspersky Embedded Systems Security для Windows ..... 284

Запуск Консоли Kaspersky Embedded Systems Security для Windows из меню Пуск..... 284

Запуск и остановка службы Kaspersky Security..... 285

Запуск компонентов Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы ..... 286


## Запуск Плагина управления Kaspersky Embedded Systems Security для Windows

Для запуска Плагина управления Kaspersky Embedded Systems Security для Windows в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на защищаемое устройство администратора, он запускается вместе с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

## Запуск Консоли Kaspersky Embedded Systems Security для Windows из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль программы из меню **Пуск**, выполните следующие действия:*

1. в меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security для Windows** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security для Windows**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► *Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security для Windows** > **Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.

Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом устройстве откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом устройстве, подключитесь к защищаемому устройству.

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

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите команду **Подключиться к другому компьютеру**.

   Откроется окно **Выбор защищаемого устройства**.
3. В открывшемся окне выберите **Другое устройство**.
4. В поле ввода справа укажите сетевое имя защищаемого устройства.
5. Нажмите на кнопку **OK**.

Консоль программы подключится к защищаемому устройству.

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

# Запуск и остановка службы Kaspersky Security

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

По умолчанию при запуске Kaspersky Embedded Systems Security для Windows запускаются задачи Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security, программа автоматически запустит только задачи, в расписании которых указано **При запуске программы**. Остальные задачи нужно запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security с помощью контекстного меню узла **Kaspersky Embedded Systems Security для Windows** или с помощью оснастки Службы Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Embedded Systems Security для Windows, если вы входите в группу "Администраторы" на защищаемом устройстве.

► *Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите одну из следующих команд:
   - **Остановить программу**
   - **Запустить программу**

Служба Kaspersky Security будет запущена или остановлена.

# Запуск компонентов Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы

В этом разделе приведена информация о работе Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы.

## В этом разделе


О работе Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы ..... 286

Запуск Kaspersky Embedded Systems Security для Windows в безопасном режиме ..... 287


## О работе Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы

Компоненты Kaspersky Embedded Systems Security для Windows можно запустить при загрузке операционной системы в безопасном режиме. Наряду со службой Kaspersky Security (kavfs.exe) загружается драйвер klam.sys. Драйвер используется для регистрации службы Kaspersky Security как защищенной службы при загрузке операционной системы. Дополнительные сведения приведены в разделе Регистрация службы Kaspersky Security как защищенной службы.

Kaspersky Embedded Systems Security для Windows можно запустить при загрузке операционной системы в следующих безопасных режимах:

- Безопасный режим с типом загрузки "Минимальная" – стандартный вариант безопасного режима загрузки операционной системы. При этом Kaspersky Embedded Systems Security для Windows может запускать следующие компоненты:
  - Постоянная защита файлов.
  - Проверка по требованию.
  - Контроль запуска программ и Формирование правил контроля запуска программ.
  - Анализ журналов.
  - Мониторинг файловых операций.
  - Мониторинг целостности файлов на основе эталона.
  - Проверка целостности программы.

Безопасный режим с типом загрузки «Сеть» – загрузка операционной системы в безопасном режиме с поддержкой сетевых драйверов. В этом режиме помимо компонентов, запускаемых в безопасном режиме с типом загрузки «Минимальная», Kaspersky Embedded Systems Security для Windows может запускать следующие компоненты:

  - Обновление баз программы.
  - Обновление модулей программы.

## Запуск Kaspersky Embedded Systems Security для Windows в безопасном режиме

По умолчанию, Kaspersky Embedded Systems Security для Windows не запускается при загрузке операционной системы в безопасном режиме.

► *Чтобы запустить Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `1`.
5. Нажмите на кнопку **OK**.

► *Чтобы отменить запуск Kaspersky Embedded Systems Security для Windows при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `0`.
5. Нажмите на кнопку **OK**.

kaspersky

# Механизмы самозащиты Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Embedded Systems Security для Windows.

## В этом разделе


О механизмах самозащиты Kaspersky Embedded Systems Security для Windows ..... 289

Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security для Windows ..... 289

Защита от изменений ключей реестра Kaspersky Embedded Systems Security для Windows ..... 290

Регистрация службы Kaspersky Security как защищенной службы ..... 291

Управление правами доступа к функциям Kaspersky Embedded Systems Security для Windows .... 291


## О механизмах самозащиты Kaspersky Embedded Systems Security для Windows

В Kaspersky Embedded Systems Security для Windows реализованы механизмы самозащиты, обеспечивающие защиту от изменения или удаления папок программы, процессов памяти и записей системного реестра.

## Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows запрещает всем пользователям переименовывать и удалять папки с установленными компонентами программы. По умолчанию используются следующие пути к папкам установки программы:

- В Microsoft Windows 32-разрядной версии: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

# Защита от изменений ключей реестра Kaspersky Embedded Systems Security для Windows

Kaspersky Embedded Systems Security для Windows ограничивает доступ к следующим ключам и ветвям реестра, обеспечивающим загрузку драйверов и служб программы:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3] (в Microsoft Windows 64-разрядной версии)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\Trace]

Права на изменение этих ветвей и ключей реестра имеют только пользователи с учетной записью Локальная система (SYSTEM). Пользователи с учетными записями Пользователь и Администратор имеют права только на чтение.

### Защита от изменений в памяти служебных компонентов программы

Для защиты служебных компонентов программы от сторонних процессов драйверы Kaspersky Embedded Systems Security для Windows ограничивают доступ к следующим исполняемым файлам:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

По умолчанию доступ к памяти служебных компонентов Kaspersky Embedded Systems Security для Windows ограничен для сторонних процессов.

Функции самозащиты можно включить в свойствах политики Консоли Kaspersky Embedded Systems Security для Windows (см. раздел "Настройка общих параметров программы в Консоли программы" на стр. 157) и Плагина управления Kaspersky Embedded Systems Security для Windows (см. раздел "Настройка параметров безопасности в Kaspersky Security Center" на стр. 113).

# Регистрация службы Kaspersky Security как защищенной службы

Технология *Protected Process Light* (PPL) гарантирует, что операционная система выполняет загрузку только доверенных служб и процессов. Для того чтобы запустить службу как защищенную, на защищаемом устройстве должен быть установлен драйвер *Early Launch Antimalware*.

Драйвер *Early Launch Antimalware* (ELAM) обеспечивает защиту устройств в сети при их включении и при инициализации драйверов сторонних производителей.

Драйвер ELAM устанавливается автоматически во время установки Kaspersky Embedded Systems Security для Windows и используется для регистрации службы Kaspersky Security как защищенной во время запуска операционной системы. Когда служба Kaspersky Security (KAVFS) запускается как системный защищенный процесс, другие незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищенного процесса и останавливать службу.

При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздними версиями. Если программа Kaspersky Embedded Systems Security для Windows установлена на сервер под управлением операционной системы, поддерживающей PPL, управление правами пользователей для службы Kaspersky Security (KAVFS) будет недоступно.

► *Чтобы установить Kaspersky Embedded Systems Security для Windows как защищенный процесс, выполните следующую команду:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

# Управление правами доступа к функциям Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security для Windows и службами операционной системы, которые регистрирует программа, а также инструкции по настройке этих прав.

kaspersky

## В этом разделе


О правах на управление Kaspersky Embedded Systems Security для Windows ..... 292

О правах на управление регистрируемыми службами ..... 294

О правах доступа к службе Kaspersky Security Management ..... 295

О правах на управление службой Kaspersky Security ..... 295

Управление правами доступа с помощью Плагина управления ..... 297

Управление правами доступа с помощью Консоли программы ..... 302

Управление правами доступа с помощью Веб-плагина ..... 306


# О правах на управление Kaspersky Embedded Systems Security для Windows

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security для Windows имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, пользователи ESS Administrators группы KICS Administrators, созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security для Windows, а также системная группа SYSTEM.

Пользователи, которые имеют доступ уровня Изменение прав в Kaspersky Embedded Systems Security для Windows, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security для Windows другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Embedded Systems Security для Windows, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security для Windows, параметры компонентов и права пользователей Kaspersky Embedded Systems Security для Windows, а также возможность просматривать статистику Kaspersky Embedded Systems Security для Windows.
- **Изменение** – доступ ко всем функциям программы, за исключением изменения прав пользователей: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security для Windows и параметры компонентов Kaspersky Embedded Systems Security для Windows.
- **Чтение** – возможность просматривать общие параметры Kaspersky Embedded Systems Security для Windows, параметры компонентов Kaspersky Embedded Systems Security для Windows, статистику Kaspersky Embedded Systems Security для Windows и права пользователей Kaspersky Embedded Systems Security для Windows.

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Embedded Systems Security для Windows.

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

*Таблица 50. Права доступа к функциям Kaspersky Embedded Systems Security для Windows*

| Права доступа | Описание |
|---|---|
| Управление задачами | Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security для Windows. |
| Создание и удаление задач проверки по требованию | Возможность создавать и удалять задачи проверки по требованию. |
| Изменение параметров | Возможности:<br>• Импортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security для Windows.<br>• Редактировать настройки программы. |
| Чтение параметров | Возможности:<br>• просматривать общие параметры Kaspersky Embedded Systems Security для Windows и параметры задач;<br>• экспортировать в конфигурационный файл параметры Kaspersky Embedded Systems Security для Windows;<br>• Просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений. |
| Управление хранилищами | Возможности:<br>• Помещать объекты на карантин.<br>• Удалять объекты из карантина и резервного хранилища.<br>• Восстанавливать объекты из карантина и резервного хранилища. |
| Управление журналами | Возможность удалять журналы выполнения задач и очищать журнал системного аудита. |
| Чтение журналов | Возможность просматривать события в журналах выполнения задач и журнале системного аудита. |
| Чтение статистики | Возможность просматривать статистику работы каждой задачи Kaspersky Embedded Systems Security для Windows. |
| Лицензирование программы | Возможность активировать Kaspersky Embedded Systems Security для Windows. |
| Удаление программы | Возможность удалить Kaspersky Embedded Systems Security для Windows. |
| Чтение прав | Возможность просматривать список и права доступа пользователей Kaspersky Embedded Systems Security для Windows. |
| Изменение прав | Возможности:<br>• Изменять список пользователей, имеющих доступ к управлению программой.<br>• изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security для Windows. |

# О правах на управление регистрируемыми службами

При установке Kaspersky Embedded Systems Security для Windows регистрирует в Windows службу Kaspersky Security (KAVFS), службу Kaspersky Security Management (KAVFSGT) и службу Kaspersky Security Exploit Prevention (KAVFSSLP).

Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Если программа Kaspersky Embedded Systems Security для Windows установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

### Служба Kaspersky Security

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

Пользователи, имеющие доступ уровня Изменение прав (см. раздел "Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля" на стр. 304), могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

### Служба Kaspersky Security Management

Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security для Windows, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, и пользователи группы ESS Administrators, созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security для Windows.

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

### Служба Kaspersky Security Exploit Prevention

По умолчанию доступ к управлению службой Kaspersky Security Exploit Prevention имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также в группу SYSTEM с правами на чтение и исполнение.

## О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Embedded Systems Security для Windows.

При установке Kaspersky Embedded Systems Security для Windows регистрирует службу Kaspersky Security Management (KAVFSGT). Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, используемая для подключения к Kaspersky Embedded Systems Security для Windows, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, и пользователи группы KICS Administrators, ESS Administrators созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security для Windows.

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 Embedded Systems Security для Windows.

Вы можете подключиться к Kaspersky Embedded Systems Security для Windows с локальной учетной записью, если на защищаемом устройстве зарегистрирована учетная запись с такими же именем пользователя и паролем.

## О правах на управление службой Kaspersky Security

При установке Kaspersky Embedded Systems Security для Windows регистрирует в Windows службу Kaspersky Security (KAVFS), а также включает функциональные компоненты, запускаемые при запуске операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности защищаемого устройства с помощью службы Kaspersky Security, можно ограничить права на управление службой Kaspersky Security с помощью Консоли программы или Плагина управления.

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу Администраторы на защищаемом устройстве. Права на чтение имеют группы SERVICE и INTERACTIVE, а права на чтение и исполнение имеет группа SYSTEM.

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

Пользователи, имеющие доступ к функциям (см. раздел "О правах на управление Kaspersky Embedded Systems Security для Windows" на стр. 292) уровня Изменение прав, могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security для Windows один из следующих стандартных уровней доступа для управления службой Kaspersky Security:

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

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Embedded Systems Security для Windows (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 51. Права доступа к функциям службы Kaspersky Security*

| Функция | Описание |
|---|---|
| Просмотр параметров службы | Возможность просматривать общие параметры и права пользователей для службы Kaspersky Security. |
| Запрос статуса службы у Диспетчера управления службами | Возможность запрашивать статус выполнения службы Kaspersky Security у Диспетчера управления службами Microsoft Windows. |
| Запрос статуса у службы | Возможность запрашивать статус 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. |

| Функция | Описание |
| --- | --- |
| Изменение прав | Возможности:<br>• добавлять и удалять пользователей службы Kaspersky Security;<br>• изменять права доступа пользователей к службе Kaspersky Security. |
| Удаление службы | Возможность отмены регистрации службы Kaspersky Security в диспетчере управления службами Microsoft Windows. |
| Пользовательские запросы к службе | Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security. |

# Управление правами доступа с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка прав доступа для одного или всех защищаемых устройств сети.

## В этом разделе

Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security ..... 297

Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ..... 300

### Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security для Windows и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).

- Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).

4. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security для Windows.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security 3.3 для Windows**.
5. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.
6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security для Windows.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security для Windows**.

5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
6. В разделе **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Embedded Systems Security для Windows: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Права на чтение**.
     - Следующие права на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Права на чтение**.
   - **Изменение**:
     - Все права на управление Kaspersky Embedded Systems Security для Windows, кроме **Права на изменение**.
     - Следующие права на управление службой Kaspersky Security: **Настройка параметров службы**, **Права на чтение**.
   - **Особые разрешения**: следующие права на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Права на чтение**, **Пользовательские запросы к KAVFS**.
7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security для Windows** выберите нужного пользователя или группу.
   b. Нажмите на кнопку **Изменить**.
   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.
   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.
   e. Нажмите на кнопку **OK**.
   f. В окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security для Windows** нажмите на кнопку **OK**.
8. В окне **Разрешения для службы Kaspersky Embedded Systems Security для Windows** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security будут сохранены.

## Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security для Windows.

Kaspersky Embedded Systems Security для Windows запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security для Windows;
- изменение компонентов Kaspersky Embedded Systems Security для Windows;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security для Windows скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security для Windows хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Embedded Systems Security для Windows не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Выберите группу администрирования, содержащую защищаемые устройства, для которых вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры политики для группы защищаемых устройств, выберите закладку **Политики** и с помощью контекстного меню перейдите к свойствам **<Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, откройте окно **Параметры программы** (см. раздел "**Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера**" на стр. 131) в Kaspersky Security Center.
3. На закладке **Безопасность и надежность** в разделе **Параметры программы** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Embedded Systems Security для Windows будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

kaspersky

# Управление правами доступа с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка прав доступа для защищаемого устройства.

## В этом разделе


Настройка прав доступа на управление Kaspersky Embedded Systems Security для Windows и службой Kaspersky Security ..... 302

Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ..... 304


## Настройка прав доступа на управление Kaspersky Embedded Systems Security для Windows и службой Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security для Windows и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security для Windows.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security 3.3 для Windows**.

5. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.
6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security для Windows.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security для Windows**.
5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
6. В разделе **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security.

- **Чтение**:
  - Следующие разрешения на управление Kaspersky Embedded Systems Security для Windows: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Права на чтение**.
  - Следующие права на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Права на чтение**.
- **Изменение**:
  - Все права на управление Kaspersky Embedded Systems Security для Windows, кроме **Права на изменение**.
  - Следующие права на управление службой Kaspersky Security: **Настройка параметров службы**, **Права на чтение**.
- **Особые разрешения**: следующие права на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Права на чтение**, **Пользовательские запросы к KAVFS**.

7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security для Windows** выберите нужного пользователя или группу.
   b. Нажмите на кнопку **Изменить**.
   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.
   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.
   e. Нажмите на кнопку **OK**.
   f. В окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security для Windows** нажмите на кнопку **OK**.
8. В окне **Разрешения для службы Kaspersky Embedded Systems Security для Windows** нажмите на кнопку **Применить**.
9. Настроенные права на управление Kaspersky Embedded Systems Security для Windows или службой Kaspersky Security будут сохранены.

## Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security для Windows.

Kaspersky Embedded Systems Security для Windows запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security для Windows;

- изменение компонентов Kaspersky Embedded Systems Security для Windows;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security для Windows скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security для Windows хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Embedded Systems Security для Windows не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security для Windows** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

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

   Поля **Пароль** и **Подтверждение пароля** станут активными.
3. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows.

4. В поле **Подтверждение пароля** введите пароль повторно.
5. Нажмите на кнопку **OK**.

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

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

# Управление правами доступа с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка прав доступа для защищаемых устройств сети.

## В этом разделе

Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security ..... 306

Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля ..... 307

### Настройка прав доступа к Kaspersky Embedded Systems Security для Windows и службе Kaspersky Security

Чтобы настроить права доступа для пользователя или группы, необходимо указать строку дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL). Дополнительная информация о строке дескриптора безопасности приведена на веб-сайте Microsoft.

► *Чтобы настроить права доступа для пользователя или группы, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security для Windows.

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

6. Добавьте пользователя или группу, указав строку дескриптора безопасности в окне **Права пользователей на управление программой** или **Права пользователей на управление службой Kaspersky Security Service**.
7. Нажмите на кнопку **OK**.

## Защита доступа к функциям Kaspersky Embedded Systems Security для Windows с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security для Windows.

Kaspersky Embedded Systems Security для Windows запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security для Windows;
- изменение компонентов Kaspersky Embedded Systems Security для Windows;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security для Windows скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security для Windows хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Embedded Systems Security для Windows не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры программы**.
5. В разделе **Безопасность и надежность** нажмите на кнопку **Настройка**.
6. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.
7. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security для Windows.
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Embedded Systems Security для Windows будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

# 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 ..... 309

Об области защиты и параметрах безопасности задачи ..... 310

О виртуальной области защиты ..... 311

Стандартные области защиты ..... 311

Стандартные уровни безопасности ..... 312

Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов ..... 315

Параметры задачи Постоянная защита файлов по умолчанию ..... 317

Управление задачей Постоянная защита файлов с помощью Плагина управления ..... 319

Управление задачей Постоянная защита файлов с помощью Консоли программы ..... 335

Управление задачей Постоянная защита файлов с помощью Веб-плагина ..... 356


## О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Embedded Systems Security для Windows проверяет следующие объекты защищаемого устройства при доступе к ним:

- объекты операционной системы;
- альтернативные потоки данных NTFS;
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств.

При записи или считывании файла любой программой на защищаемом устройстве, Kaspersky Embedded Systems Security для Windows перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Перед лечением или удалением Kaspersky Embedded Systems Security для Windows сохраняет зашифрованную копию исходного файла в папку резервного хранилища.

Kaspersky Embedded Systems Security для Windows также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих параметрах.

# Об области защиты и параметрах безопасности задачи

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы устройства. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов устройства, контролируемых Kaspersky Embedded Systems Security для Windows. По умолчанию сетевые файловые ресурсы устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы перейти к отображению сетевых файловых ресурсов в виде дерева в Консоли программы,*

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

Независимо от того, отображаются ли файловые ресурсы защищаемого устройства в виде списка или в виде дерева, значки узлов имеют следующие значения:

☑ Узел включен в область защиты.

☐ Узел исключен из области защиты.

☑ По крайней мере, один из узлов, вложенных в этот узел, исключен из области защиты, или параметры безопасности вложенных узлов отличаются от параметров безопасности родительского узла (только при отображении в виде дерева).

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

С помощью Консоли программы можно также добавлять в область защиты виртуальные диски (см. раздел "Формирование виртуальной области защиты" на стр. 345). Имена виртуальных узлов отображаются синим цветом.

### Параметры безопасности

Параметры безопасности задачи можно настроить как едиными для всех узлов или элементов, входящих в область защиты, так и индивидуальными для каждого узла или элемента в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- Выбрать один из трех стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 312).
- Настроить параметры безопасности вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 327) для выбранных узлов или элементов в дереве или списке файловых ресурсов (уровень безопасности изменится на **Другой**).

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

# О виртуальной области защиты

Kaspersky Embedded Systems Security для Windows может проверять не только существующие папки и файлы на жестких и съемных дисках, но и диски, которые динамически создаются на защищаемом устройстве различными программами и службами.

Если все объекты устройства включены в область защиты, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для динамических узлов или если вы выбрали для защиты отдельные области устройства, то, для того чтобы включить в область защиты виртуальные диски, файлы или папки, вам нужно предварительно создать их в Консоли программы, то есть задать виртуальную область защиты. Созданные диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого устройства.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, все появившиеся в ней виртуальные папки или файлы не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

# Стандартные области защиты

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security для Windows предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Embedded Systems Security для Windows защищает файлы на жестких дисках устройства.
- **Съемные диски**. Kaspersky Embedded Systems Security для Windows защищает файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.

- **Сетевое окружение**. Kaspersky Embedded Systems Security для Windows защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на устройстве. Kaspersky Embedded Systems Security для Windows не защищает файлы, когда к ним обращаются программы с других защищаемых устройств.
- **Виртуальные диски**. Можно включать в область защиты виртуальные папки и файлы, а также диски, временно подключенные к устройству, например, общие диски кластера.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

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

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы включить в область защиты объекты на виртуальном диске, включите в область защиты папку на устройстве, связанную с этим виртуальным диском.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов защищаемого устройства. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

# Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Embedded Systems Security для Windows на защищаемых устройствах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

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

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Только сообщать

Уровень безопасности **Только уведомлять** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

*Таблица 52. Стандартные уровни безопасности и соответствующие им значения параметров*

| Параметры | Уровень безопасности | | | |
|---|---|---|---|---|
| | Максимальное быстродействие | Рекомендуемый | Максимальная защита | Только сообщать |
| **Защита объектов** | По расширению | По формату | По формату | По формату |
| **Проверка только новых и измененных файлов** | Включено | Включено | Выключено | Включено |
| **Действия над зараженными и другими обнаруженным и объектами** | Блокировать доступ и лечить. Удалить, если не удалось вылечить | Блокировать доступ и выполнять рекомендованное специалистами "Лаборатории Касперского" действие | Блокировать доступ и лечить. Удалить, если не удалось вылечить | Только сообщать |
| **Действия над возможно зараженными объектами** | Блокировать доступ и поместить на карантин | Блокировать доступ и выполнять рекомендованное специалистами "Лаборатории Касперского" действие | Блокировать доступ и поместить на карантин | Только сообщать |
| Системно-критические объекты – это файлы, необходимые для работы операционной системы и Kaspersky Embedded Systems Security для Windows. Такие объекты нельзя удалить. Процессы, относящиеся к таким объектам, не могут быть прекращены. | | | | |
| **Исключать файлы** | Нет | Нет | Нет | Нет |
| **Не обнаруживать** | Нет | Нет | Нет | Нет |
| **Останавливать проверку, если она длится более (сек.)** | 60 сек. | 60 сек. | 60 сек. | 60 сек. |

| Параметры | Уровень безопасности | | | |
|---|---|---|---|---|
| **Не проверять составные объекты размером более (МБ)** | 8 МБ | 8 МБ | Не установлен | 8 МБ |
| **Альтернативные потоки NTFS** | Да | Да | Да | Да |
| **Загрузочные секторы дисков и MBR** | Да | Да | Да | Да |
| **Защита составных объектов** | • Упакованные объекты*<br>* Только новые и измененные | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Только новые и измененные | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Все объекты | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Только новые и измененные |
| **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой** | Нет | Нет | Да | Нет |

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** и **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените параметры безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** или **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

# Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Embedded Systems Security для Windows проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*

- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*

- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

# Параметры задачи Постоянная защита файлов по умолчанию

По умолчанию в задаче Постоянная защита файлов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 53. Параметры задачи Постоянная защита файлов по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Область защиты | Защищаемое устройство целиком, исключая виртуальные диски. | Используйте этот параметр, чтобы изменить область защиты. |
| Параметры безопасности | Единые для всей области защиты; соответствует уровню безопасности **Рекомендуемый**. | Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия:<br>• выбрать другой стандартный уровень безопасности;<br>• вручную изменить параметры безопасности.<br>Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла. |
| **Режим защиты объектов** | **Интеллектуальный режим** | Этот параметр используется, чтобы указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security для Windows проверяет их. |
| **Эвристический анализатор** | Применяется уровень безопасности **Средний**. | Вы можете включать и выключать эвристический анализатор, а также регулировать уровень анализа. |
| **Применять доверенную зону** | Применяется. | Единый список исключений, который можно применять в выбранных задачах. |
| **Использовать KSN для защиты** | Применяется. | Используйте этот параметр, чтобы повысить эффективность защиты устройства с помощью облачных служб Kaspersky Security Network (доступных, если принято Положение о KSN). |
| Расписание запуска задачи | При запуске программы. | Этот параметр используется, чтобы настроить запуск задачи по расписанию. |
| **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность** | Не применяется. | Этот параметр используется, чтобы заблокировать текущий сеанс и добавить IP-адрес или локально уникальный идентификатор (LUID) узла, для которого была обнаружена вредоносная активность, в раздел Хранилище заблокированных хостов. |
| **Запустить сканирование важных областей при обнаружении активного заражения** | Применяется. | При обнаружении активного заражения Kaspersky Embedded Systems Security для Windows создает и запускает временную задачу Проверка важных областей. |

kaspersky

# Управление задачей Постоянная защита файлов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

## В этом разделе


Навигация ..... 319

Настройка задачи Постоянная защита файлов ..... 320

Создание и настройка области защиты задачи ..... 326

Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ..... 327

Настройка параметров безопасности вручную ..... 327


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам политики для задачи Постоянная защита файлов ..... 319

Переход к параметрам задачи Постоянная защита файлов ..... 320


### Переход к параметрам политики для задачи Постоянная защита файлов

► *Чтобы перейти к параметрам задачи Постоянная защита файлов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

### Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров задачи Постоянная защита файлов для отдельного устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В блоке **Задачи** выберите задачу **Постоянная защита файлов**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

## Настройка задачи Постоянная защита файлов

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Параметры перехвата** (см. раздел "**Выбор режима защиты**" на стр. 321)
     - **Эвристический анализатор** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 322)
     - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 322)
   - На закладке **Управление задачей**:
     - Запуск задачи по расписанию (см. раздел "Настройка расписания задач" на стр. 145).

3. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Формирование области защиты" на стр. 342).
     - В открывшемся окне выберите, что требуется включить в область защиты задачи:
       - **Предопределенная область**
       - **Диск, папка или сетевой объект**
       - **Файл**
     - Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 312) или настройте параметры защиты вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 327).
4. Нажмите на кнопку **OK** в окне **Постоянная защита файлов**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

Выбор режима защиты ..... 321
Настройка эвристического анализатора и интеграции с другими компонентами программы ..... 322
Настройка расписания задач ..... 324

## Выбор режима защиты

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security для Windows проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**

     Kaspersky Embedded Systems Security для Windows выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security для Windows повторно проверяет объект только после его последнего сохранения этим процессом.

- **При открытии и изменении**

  Kaspersky Embedded Systems Security для Windows проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

  Этот вариант выбран по умолчанию.

- **При открытии**

  Kaspersky Embedded Systems Security для Windows проверяет все объекты при их открытии на чтение, выполнение и изменение.

- **При выполнении**

  Kaspersky Embedded Systems Security для Windows проверяет файл только при открытии на выполнение.

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

  Kaspersky Embedded Systems Security для Windows выполняет более длительный анализ запускаемых процессов с большей вероятностью обнаружения угрозы. Запуск процесса блокируется до завершения анализа.

3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

## Настройка эвристического анализатора и интеграции с другими компонентами программы

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

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни чувствительности проверки:

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

  Этот уровень выбран по умолчанию.
- **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

- Установите или снимите флажок **Применить Доверенную зону**.

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

  По умолчанию флажок установлен.

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

  Этот флажок включает или выключает использование служб KSN.

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

  Если флажок снят, задача не использует службы KSN.

  По умолчанию флажок установлен.

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

- Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

- Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.

  Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Embedded Systems Security для Windows удаляет эту временную задачу.

  Если флажок не установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows не создает и не запускает задачу Проверка важных областей.

По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

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

## Настройка расписания задач

В Консоли программы вы можете настроить расписание локальных системных и пользовательских задач. Настраивать расписание групповых задачам с помощью Консоли программы невозможно.

► *Чтобы настроить расписание групповых задач с помощью Плагина управления, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
      - **Ежесуточно**, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.

- **Еженедельно**, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
- **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security для Windows.
- **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату начала действия расписания.

> После того как вы укажете частоту, дату и время запуска задачи, отобразится расчетное время очередного запуска задачи.
> Перейдите на закладку **Расписание** и откройте окно **Параметры задачи**. В поле **Следующий запуск** в верхней части окна отображается расчетное время запуска. Расчетное время следующего запуска задачи обновляется каждый раз, когда вы открываете окно.
> В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 116) запрещен действующей политикой Kaspersky Security Center.

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

> Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131)".

## Создание и настройка области защиты задачи

► *Чтобы создать и настроить область защиты задачи в Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. Выберите закладку **Область защиты**.

   Все элементы, на которые распространяется область защиты задачи, перечислены в таблице **Область защиты**.
3. Нажмите на кнопку **Добавить**, чтобы добавить в список новый элемент.

   Откроется окно **Добавление в область защиты**.
4. Выберите тип объектов для добавления в область защиты:
   - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
   - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
   - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

   Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.
5. Чтобы исключить отдельные элементы из области защиты, снимите флажки рядом с именами этих элементов или выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
6. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
7. Чтобы скрыть добавленную ранее область защиты или исключение в списке сетевых файловых ресурсов, в контекстном меню требуемой области защиты выберите пункт **Удалить область**.

   Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.
8. Нажмите на кнопку **OK**.

Окно Параметры области защиты закроется. Настроенные параметры будут сохранены.

Задачу **Постоянная защита файлов** можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

## Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранного в дереве файловых ресурсов узла можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. 320) **Свойства: Постоянная защита файлов**.
2. Выберите закладку **Область защиты**.
3. В списке защищаемых устройств выберите элемент, включенный в область защиты, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **OK** в окне **Свойства: Постоянная защита файлов**.

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

## Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 312) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

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

1. Откройте окно **Постоянная защита файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. На закладке **Область защиты** выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
3. На закладке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями:
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 328)
   - Действия (см. раздел "Настройка действий" на стр. 331)
   - Производительность (см. раздел "Настройка производительности" на стр. 333)
5. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Новые параметры области защиты будут сохранены.

## В этом разделе

Настройка общих параметров задачи ..... 328
Настройка действий ..... 331
Настройка производительности ..... 333

## Настройка общих параметров задачи

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

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите типы объектов, которые вы хотите включить в область защиты:
   - **Все объекты**

     Kaspersky Embedded Systems Security для Windows проверяет все объекты.
   - **Объекты, проверяемые по формату**

     Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

  Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

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

- **Все** / **Только новые архивы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

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

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**.

     Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**.

  Выберите действие из раскрывающегося списка:

  - **Лечить**.
  - **Лечить. Удалять, если не удалось вылечить**. **Лечить. Удалять, если не удалось вылечить**.
  - **Удалять**.

  Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

  - **Рекомендуемое**.

Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Выберите действие над возможно зараженными объектами:

- **Только сообщать**.

  Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

  Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

  Выберите действие из раскрывающегося списка:

  - **Помещать на карантин**.
  - **Удалять**.

    Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

  - **Рекомендуемое**.

    Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

2. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Embedded Systems Security для Windows не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.
   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.
3. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

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

   Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.
4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

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

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 319).
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 Embedded Systems Security для Windows пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

  По умолчанию флажок снят.

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

  Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

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

4. В блоке **Дополнительные параметры**:

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

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

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

  Если флажок снят, продолжительность проверки не ограничена.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

  Исключение из проверки объектов больше указанного размера.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

# Управление задачей Постоянная защита файлов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе

Навигация ..... 336
Настройка задачи Постоянная защита файлов ..... 336
Формирование области защиты ..... 342
Настройка параметров безопасности вручную ..... 346
Статистика задачи Постоянная защита файлов ..... 354

kaspersky

# Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе

Переход к параметрам задачи Постоянная защита файлов ..... 336

Переход к параметрам области действия задачи Постоянная защита файлов ..... 336

### Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну общих параметров задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

### Переход к параметрам области действия задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров области защиты для задачи Постоянная защита файлов, выполните следующие действия.*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

# Настройка задачи Постоянная защита файлов

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 336).
2. На закладке **Общие** настройте следующие параметры задачи:
   - **Режим защиты объектов** (см. раздел "**Выбор режима защиты объектов**" на стр. 337)
   - **Эвристический анализатор** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 338)
   - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 338)

3. На закладках **Расписание** и **Дополнительно** настройте расписание задачи (см. раздел "Настройка параметров расписания задач" на стр. 165).
4. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.
5. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
6. Выполните следующие действия:
   - В дереве или списке файловых ресурсов устройства выберите узлы или элементы, которые вы хотите включить в область защиты задачи.
   - Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 312) или настройте параметры защиты объекта вручную (см. раздел "Настройка параметров безопасности" на стр. 596).
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

Выбор режима защиты объектов ..... 337
Настройка эвристического анализатора и интеграции с другими компонентами программы ..... 338
Настройка параметров расписания задач ..... 340

## Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security для Windows проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 336).
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**

     Kaspersky Embedded Systems Security для Windows выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security для Windows повторно проверяет объект только после его последнего сохранения этим процессом.

- **При открытии и изменении**

  Kaspersky Embedded Systems Security для Windows проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.

  Этот вариант выбран по умолчанию.

- **При открытии**

  Kaspersky Embedded Systems Security для Windows проверяет все объекты при их открытии на чтение, выполнение и изменение.

- **При выполнении**

  Kaspersky Embedded Systems Security для Windows проверяет файл только при открытии на выполнение.

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

  Kaspersky Embedded Systems Security для Windows выполняет более длительный анализ запускаемых процессов с большей вероятностью обнаружения угрозы. Запуск процесса блокируется до завершения анализа.

3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

## Настройка эвристического анализатора и интеграции с другими компонентами программы

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

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 336).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

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

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

     По умолчанию флажок установлен.

     По ссылке **Доверенная зона** перейдите к параметрам доверенной зоны.

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

     Этот флажок включает или выключает использование служб KSN.

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

     Если флажок снят, задача не использует службы KSN.

     По умолчанию флажок установлен.

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

- Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

  Флажок включает или выключает блокировку текущего сеанса и контролирует доступность общих сетевых ресурсов в рамках текущего сеанса.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows блокирует текущий сеанс и в рамках текущего сеанса делает недоступными общие сетевые ресурсы для узлов, для которых обнаружена вредоносная активность в разделе Хранилище заблокированных узлов.

  Если флажок снят, условия не применяются и Kaspersky Embedded Systems Security для Windows работает в обычном режиме.

  По умолчанию флажок снят.

  Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

  Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

- Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.

  Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Embedded Systems Security для Windows удаляет эту временную задачу.

  Если флажок не установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows не создает и не запускает задачу Проверка важных областей.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

## Настройка параметров расписания задач

В Консоли программы можно настроить расписание запуска локальных системных и пользовательских задач. Однако настроить расписание запуска групповых задач нельзя.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню задачи, для которой требуется настроить расписание.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.

4. Выполните следующие действия, чтобы настроить расписание:
   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, чтобы задача запускалась с периодичностью в заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, чтобы задача запускалась с периодичностью в заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, чтобы задача запускалась с периодичностью в заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
      - **При запуске программы**, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security для Windows.
      - **После обновления баз программы**, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.
   c. В поле **Начать с** укажите дату первого запуска задачи.

   После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
   В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск локальных системных задач по расписанию запрещен действующей политикой Kaspersky Security Center.

5. На закладке **Дополнительно** настройте следующие параметры расписания:
   - В разделе **Параметры остановки задачи**:
     a. Установите флажок **Длительность**. В полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с**. В полях справа укажите, когда требуется приостановить и возобновить выполнение задачи (в рамках 24 часов).
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить с** и укажите дату прекращения действия расписания.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы запускать пропущенные задачи.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **OK**.

Параметры расписания задачи будут сохранены.

kaspersky

# Формирование области защиты

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

## В этом разделе


Настройка отображения сетевых файловых ресурсов ..... 342

Формирование области защиты ..... 342

Включение сетевых объектов в область защиты ..... 344

Формирование виртуальной области защиты ..... 345


## Настройка отображения сетевых файловых ресурсов

► *Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области защиты, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

   По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.
3. Нажмите на кнопку **Сохранить**.

## Формирование области защиты

Процедура формирования области действия задачи Постоянная защита файлов зависит от выбранного отображения сетевых файловых ресурсов (см. раздел "Об области защиты и параметрах безопасности задачи" на стр. 310). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

Чтобы применить к задаче новые параметры области защиты, нужно перезапустить задачу Постоянная защита файлов.

► *Чтобы сформировать область защиты с помощью дерева сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с названием нужного типа дисков. Например, чтобы включить все съемные диски устройства, установите флажок **Съемные диски**.
     - Если вы хотите включить в область защиты отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного диска. Например, чтобы выбрать съемный диск F:, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

► *Чтобы сформировать область защиты с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В окне **Добавление области защиты** выберите тип объектов, который вы хотите включить в область защиты:
      - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
      - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.

- **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

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

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

6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

Задачу Постоянная защита файлов можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Если указана сложная область защиты, например, заданы разные значения параметров безопасности для отдельных узлов в дереве файловых ресурсов устройства, это может привести к замедлению проверки объектов при доступе к ним.

## Включение сетевых объектов в область защиты

Вы можете включать в область защиты сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► *Чтобы включить в область защиты сетевой объект, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, чтобы добавить сетевую папку в область защиты.
   - Выберите пункт **Добавить сетевой файл**, чтобы добавить сетевой файл в область защиты.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention).
5. Нажмите на клавишу **ENTER**.
6. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область защиты.
7. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Формирование виртуальной области защиты

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 592).

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню узла **Виртуальные диски**.
4. Выберите пункт **Добавить виртуальный диск**.
5. В списке доступных имен выберите имя создаваемого виртуального диска.
6. Установите флажок рядом с диском, чтобы включить его в область защиты.
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

3. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, чтобы добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, чтобы добавить виртуальный файл в область защиты.
4. В поле ввода задайте имя папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
6. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 312) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

При работе с деревом файловых ресурсов защищаемого устройства параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 172).

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 342), создать область защиты (см. раздел "Формирование области защиты" на стр. 342) и создать виртуальную область защиты (см. раздел "Формирование виртуальной области защиты" на стр. 345).
3. В правой части окна выполните одно из следующих действий:
   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. 347).
   - На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
     - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 347)
     - **Действия** (см. раздел "**Настройка действий**" на стр. 350)
     - **Производительность** (см. раздел "**Настройка производительности**" на стр. 353)

4. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Новые параметры области защиты будут сохранены.

## В этом разделе

Выбор стандартных уровней безопасности в задаче Постоянная защита файлов ..... 347
Настройка общих параметров задачи..... 347
Настройка действий..... 350
Настройка производительности ..... 353

## Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область защиты.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

## Настройка общих параметров задачи

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. Выберите закладку **Общие**.

3. В блоке **Защита объектов** укажите объекты, которые требуется включить в область защиты:
   - **Все объекты**

     Kaspersky Embedded Systems Security для Windows проверяет все объекты.
   - **Объекты, проверяемые по формату**

     Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

     Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
   - **Объекты, проверяемые по указанному списку расширений**

     Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

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

     Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

     Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

     Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

     По умолчанию флажок установлен.
4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

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

- **Все** / **Только новые архивы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**.

  Выберите действие из раскрывающегося списка:

  - **Лечить**.
  - **Лечить. Удалять, если не удалось вылечить**. **Лечить. Удалять, если не удалось вылечить**.
  - **Удалять**.

  Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

  - **Рекомендуемое**.

Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

1. Выберите действие над возможно зараженными объектами:

- **Только сообщать**.

  Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

  Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

  Выберите действие из раскрывающегося списка:

  - **Помещать на карантин**.
  - **Удалять**.

    Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**.

  Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

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

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

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Embedded Systems Security для Windows не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

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

   d. Нажмите на кнопку **OK**.

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

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

   Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.

4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

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

1. Откройте окно **Настройка области защиты** (см. раздел "**Переход к параметрам области действия задачи Постоянная защита файлов**" на стр. 336).
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 Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
4. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**

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

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

     Если флажок снят, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки объектов больше указанного размера.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

## Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Embedded Systems Security для Windows с момента запуска задачи.

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

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

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

Вы можете просмотреть информацию об объектах, обработанных Kaspersky Embedded Systems Security для Windows с момента запуска задачи (см. таблицу ниже).

*Таблица 54. Статистика задачи Постоянная защита файлов*

| Поле | Описание |
|---|---|
| **Обнаружено** | Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security для Windows. Например, если программа Kaspersky Embedded Systems Security для Windows обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу. |
| **Зараженных и других обнаруживаемых объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows признала зараженными, или количество обнаруженных легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным. |
| **Возможно зараженных объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows признала возможно зараженными. |
| **Объектов не вылечено** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows не вылечила по следующим причинам:<br>• Тип обнаруженного объекта не предполагает лечения.<br>• При лечении возникла ошибка. |
| **Объектов не помещено на карантин** | Количество объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось поместить на карантин, например, из-за отсутствия свободного места на диске. |
| **Объектов не удалено** | Количество объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось удалить, например, если доступ к объекту был заблокирован другой программой. |
| **Объектов не проверено** | Количество объектов в области защиты, которые программе Kaspersky Embedded Systems Security для Windows не удалось проверить, например, если доступ к объекту был заблокирован другой программой. |
| **Объектов, не помещенных в резервное хранилище** | Количество объектов, копии которых программе Kaspersky Embedded Systems Security для Windows не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске. |
| **Ошибок обработки** | Количество объектов, во время обработки которых возникла ошибка задачи. |
| **Вылечено объектов** | Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security для Windows. |
| **Помещено на карантин** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows поместила на карантин. |
| **Помещено в резервное хранилище** | Количество объектов, копии которых программа Kaspersky Embedded Systems Security для Windows сохранила в резервном хранилище. |
| **Удалено объектов** | Количество объектов, которые удалила программа Kaspersky Embedded Systems Security для Windows. |
| **Защищенных паролем объектов** | Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security для Windows пропустила, так как эти объекты защищены паролем. |

| Поле | Описание |
|---|---|
| **Поврежденных объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows пропустила, так как их формат искажен. |
| **Обработано объектов** | Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security для Windows. |

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

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

# Управление задачей Постоянная защита файлов с помощью Веб-плагина

В этом разделе описано управление задачей Постоянная защита файлов с помощью интерфейса Веб-плагина.

## В этом разделе

Настройка задачи Постоянная защита файлов ..... 356
Настройка области защиты для задачи ..... 360

## Настройка задачи Постоянная защита файлов

С помощью Веб-плагина нельзя изменить стандартный уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задаче Постоянная защита файлов" на стр. 327) для задачи Постоянная защита файлов.

► *Чтобы настроить задачу Постоянная защита файлов с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.

5. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 55. Параметры задачи Постоянная защита файлов*

| Параметр | Описание |
|---|---|
| **Интеллектуальный режим** | Kaspersky Embedded Systems Security для Windows выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security для Windows повторно проверяет объект только после его последнего сохранения этим процессом. |
| **При открытии** | Kaspersky Embedded Systems Security для Windows проверяет все объекты при их открытии на чтение, выполнение и изменение. |
| **При открытии и изменении** | Kaspersky Embedded Systems Security для Windows проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен.<br>Этот вариант выбран по умолчанию. |
| **При выполнении** | Kaspersky Embedded Systems Security для Windows проверяет файл только при открытии на выполнение. |
| **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)** | Kaspersky Embedded Systems Security для Windows выполняет более длительный анализ запускаемых процессов с большей вероятностью обнаружения угрозы. Запуск процесса блокируется до завершения анализа.<br>Kaspersky Embedded Systems Security для Windows выполняет более длительный анализ запускаемых процессов с большей вероятностью обнаружения угрозы. Запуск процесса блокируется до завершения анализа. |
| **Использовать эвристический анализатор** | Флажок включает или выключает использование эвристического анализатора при проверке объектов.<br>Если флажок установлен, эвристический анализатор включен.<br>Если флажок снят, эвристический анализатор выключен.<br>По умолчанию флажок установлен. |

| Параметр | Описание |
| --- | --- |
| **Уровень эвристического анализа** | Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.<br>Существуют следующие уровни чувствительности проверки:<br>• **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.<br>• **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".<br>Этот уровень выбран по умолчанию.<br>• **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.<br>Параметр доступен, если установлен флажок **Использовать эвристический анализатор**. |
| **Применять доверенную зону** | Флажок включает или выключает применение доверенной зоны в работе задачи.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.<br>По умолчанию флажок установлен. |

| Параметр | Описание |
| --- | --- |
| **Использовать KSN для защиты** | Этот флажок включает или выключает использование служб KSN.<br>Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.<br>Если флажок снят, задача не использует службы KSN.<br>По умолчанию флажок установлен. |
| **Блокировать доступ к сетевым файловым ресурсам для сетевых сессий, с которых ведется вредоносная активность** | Флажок включает или выключает блокировку текущего сеанса и контролирует доступность общих сетевых ресурсов в рамках текущего сеанса.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows блокирует текущий сеанс и в рамках текущего сеанса делает недоступными общие сетевые ресурсы для узлов, для которых обнаружена вредоносная активность в разделе Хранилище заблокированных узлов.<br>Если флажок снят, условия не применяются и Kaspersky Embedded Systems Security для Windows работает в обычном режиме.<br>По умолчанию флажок снят.<br>Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.<br>Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов. |
| **Запустить сканирование важных областей при обнаружении активного заражения** | Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Embedded Systems Security для Windows удаляет эту временную задачу.<br>Если флажок не установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security для Windows не создает и не запускает задачу Проверка важных областей.<br>По умолчанию флажок установлен. |

| Параметр | Описание |
|---|---|
| **Область защиты** | Можно настроить параметры безопасности для области защиты (см. раздел "Настройка параметров безопасности вручную" на стр. 327). |

## Настройка области защиты для задачи

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

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.
6. Выберите раздел **Область защиты**.
7. Выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
   - Выберите существующее правило и нажмите на кнопку **Изменить**.

   Откроется окно **Изменить область**.
8. Установите переключатель в положение **Активный** и выберите тип объекта.
9. В разделе **Защита объектов** настройте следующие параметры:
   - **Режим защиты объектов**:
     - **Все объекты**

       Kaspersky Embedded Systems Security для Windows проверяет все объекты.
     - **Объекты, проверяемые по формату**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

10. В разделе **Защита объектов** установите или снимите флажок **Проверка только новых и измененных файлов**.

    Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

    Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

    Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

11. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

    - **Архивы**

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

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

      Значение по умолчанию зависит от выбранного уровня защиты.

- **SFX-архивы**

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

- **Упакованные объекты**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Почтовые базы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых баз при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Файлы почтовых форматов**

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Вложенные OLE-объекты**

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**

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

  Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

  Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.

12. Выберите действие над зараженными и другими обнаруживаемыми объектами:

- **Только сообщать**.

  Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

  Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**.

  Выберите действие из раскрывающегося списка:

  - **Лечить**.
  - **Лечить. Удалять, если не удалось вылечить**.**Лечить. Удалять, если не удалось вылечить**.
  - **Удалять**.

    Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

  - **Рекомендуемое**.

    Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

13. Выберите действие над возможно зараженными объектами:
    - **Только сообщать**.

      Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

      Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.
    - **Блокировать доступ**.

      Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows блокирует доступ к обнаруженным или возможно зараженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.
    - **Выполнять дополнительное действие**.

      Выберите действие из раскрывающегося списка:
      - **Помещать на карантин**.
      - **Удалять**.

        Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.
      - **Рекомендуемое**.

        Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".
14. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
    a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

       Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Embedded Systems Security для Windows не позволит открыть или запустить зараженный объект независимо от вашего выбора.

       Если флажок снят, Kaspersky Embedded Systems Security для Windows выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

       По умолчанию флажок снят.
    b. Нажмите на кнопку **Настройка**.
    c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
    d. Нажмите на кнопку **OK**.

15. В разделе **Исключения** настройте следующие параметры:
    - Снимите или установите флажок **Исключать файлы**.

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

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

      По умолчанию флажок снят.
    - Снимите или установите флажок **Не обнаруживать**.

      Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

      По умолчанию флажок снят.
16. В разделе **Оптимизация** настройте следующие параметры:
    - **Останавливать проверку, если она длится более (сек.).**

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

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

      Если флажок снят, продолжительность проверки не ограничена.

      По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
    - **Не проверять составные объекты размером более (МБ).**

      Исключение из проверки объектов больше указанного размера.

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

      По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift.**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker.**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

17. Нажмите на кнопку **OK**.

# Использование KSN

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

В сертифицированной версии программы использование Глобального KSN не допускается, так как приводит к выводу программы из сертифицированного состояния.

## В этом разделе


О задаче Использование KSN ..... 367

Параметры по умолчанию для задачи Использование KSN ..... 369

Управление использованием KSN с помощью Плагина управления ..... 370

Управление использованием KSN с помощью Консоли программы ..... 373

Управление использованием KSN с помощью Веб-плагина ..... 376

Настройка передачи дополнительных данных ..... 379

Статистика задачи Использование KSN ..... 380


## О задаче Использование KSN

*Kaspersky Security Network* (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows получает от Kaspersky Security Network только информацию о репутации программ.

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

Более подробная информация о передаче, обработке, хранении и уничтожении информации об использовании программы приведена в окне **Положение о Kaspersky Security Network** задачи Использование KSN и в Политике конфиденциальности на веб-сайте "Лаборатории Касперского".

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Embedded Systems Security для Windows. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network можно использовать в следующих задачах Kaspersky Embedded Systems Security для Windows:

- Постоянная защита файлов.
- Проверка по требованию.
- Правила контроля запуска программ.

**Kaspersky Private Security Network**

Подробная информация о настройке Kaspersky Private Security Network (далее также "Локальный KSN") приведена в *Справке Kaspersky Security Center*.

Если вы используете Локальный KSN на устройстве, в окне **Положение о Kaspersky Security Network** (см. раздел "**Настройка обработки данных с помощью Плагина управления**" на стр. 372) задачи Использование KSN можно ознакомиться с Положением о KSN и включить использование компонента, установив флажок **Я принимаю условия использования Kaspersky Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KSN (запросы безопасности, статистические данные), в службы KSN.

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

Если вы отключаете Локальный KSN во время выполнения задачи Использование KSN, происходит ошибка *Нарушение лицензии* и выполнение задачи прекращается. Чтобы продолжить защищать устройство, вам нужно принять Положение о KSN в окне **Положение о Kaspersky Security Network** и перезапустить задачу.

**Отзыв согласия с Положением о KSN**

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

- Вы сняли флажок **Разрешить отправку данных о проверяемых файлах**: программа перестает отправлять контрольные суммы проверенных файлов в службу KSN для анализа.
- Вы сняли флажок **Разрешить отправку статистики Kaspersky Security Network**: программа прекращает обрабатывать данные с дополнительной статистикой KSN.
- Вы сняли флажок **Я принимаю условия использования Kaspersky Security Network**: программа прекращает обрабатывать все связанные с KSN данные, задача Использование KSN останавливается.

- Вы удалили компонент Использование KSN: обработка всех связанных с KSN данных останавливается.
- Вы удалили Kaspersky Embedded Systems Security для Windows: обработка всех связанных с KSN данных останавливается.
- Вы удалили лицензионный ключ Kaspersky Embedded Systems Security для Windows или приостановили использование лицензии: обработка всех связанных с KSN данных останавливается.

# Параметры по умолчанию для задачи Использование KSN

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

*Таблица 56. Параметры по умолчанию для задачи Использование KSN*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Действия над объектами, недоверенными в KSN** | Удалить | Вы можете указывать действия, которые Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows рассчитывает MD5-хеш для файлов любого размера. |
| **Расписание запуска задачи** | Время первого запуска не задано. | Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |
| **Использовать Kaspersky Security Center в качестве прокси-сервера KSN** | Выбрано. | По умолчанию все данные отправляются в KSN через Kaspersky Security Center.<br>Этот параметр можно изменять только с помощью Плагина управления. |
| **Я принимаю условия использования Kaspersky Security Network** | Флажок снят | Если флажок установлен, от вас получено согласие на участие в KSN после установки программы. Вы можете изменить свое решение в любой момент. |
| **Разрешить отправку статистики Kaspersky Security Network** | Установлен (применяется, только если принято Положение о KSN). | Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Разрешить отправку данных о проверяемых файлах** | Установлен (применяется, только если принято Положение о KSN). | Если Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент. |

# Управление использованием KSN с помощью Плагина управления

В этом разделе описана настройка использования KSN и обработки данных с помощью Плагина управления.

## В этом разделе


Настройка задачи Использование KSN с помощью Плагина управления ..... 370

Настройка обработки данных с помощью Плагина управления ..... 372


## Настройка задачи Использование KSN с помощью Плагина управления

► *Чтобы настроить задачу Использование KSN, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Использование KSN**.

   Откроется окно **Использование KSN**.
5. На закладке **Общие** настройте следующие параметры задачи:
   - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Embedded Systems Security для Windows при обнаружении объекта, имеющего репутацию недоверенного в KSN:

- **Удалять**

  Kaspersky Embedded Systems Security для Windows удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

  Этот вариант выбран по умолчанию.

- **Фиксировать информацию в отчете**

  Kaspersky Embedded Systems Security для Windows фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security для Windows не удаляет недоверенный объект.

- В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
  - 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 Embedded Systems Security для Windows не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

    Если флажок снят, Kaspersky Embedded Systems Security для Windows рассчитывает контрольную сумму для файлов любого размера. По умолчанию флажок установлен.

  - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security для Windows будет рассчитывать контрольную сумму.

- В разделе **Прокси-сервер KSN** снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

  Флажок позволяет управлять передачей данных от защищаемых устройств в KSN.

  Если флажок снят, данные с Сервера администрирования и защищаемых устройств отправляются в KSN напрямую (минуя Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую.

  Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center. По умолчанию флажок установлен.

Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Справке Kaspersky Security Center*.

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

   Программа будет запускать задачу Использование KSN по расписанию.

7. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Плагина управления" на стр. 372).

8. Нажмите на кнопку **OK**.

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

## Настройка обработки данных с помощью Плагина управления

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Положение о KSN** в подразделе **Использование KSN**.

   Откроется окно **Положение о Kaspersky Security Network**.
5. На закладке **Службы и статистика KSN** прочитайте текст Положения и установите флажок **Я принимаю условия использования Kaspersky Security Network**.
6. Для повышения уровня защиты, следующие флажки установлены по умолчанию:
   - **Разрешить отправку данных о проверяемых файлах**

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не отправляет контрольные суммы файлов в KSN.

     Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено «Лабораторией Касперского» с целью защиты репутационных серверов от DDoS*.

     По умолчанию флажок установлен.

- **Разрешить отправку статистики Kaspersky Security Network**

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не отправляет дополнительную статистику.

  По умолчанию флажок установлен.

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

7. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы программа Kaspersky Embedded Systems Security для Windows отправляла дополнительную статистику в "Лабораторию Касперского".

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не отправляет дополнительную статистику.

   По умолчанию флажок установлен.

8. Нажмите на кнопку **OK**.

   Конфигурация обработки данных будет сохранена.

# Управление использованием KSN с помощью Консоли программы

В этом разделе описана настройка использования KSN и обработки данных с помощью Консоли программы.

## В этом разделе

Настройка задачи Использование KSN с помощью Консоли программы ..... 374

Настройка обработки данных с помощью Консоли программы ..... 375

## Настройка задачи Использование KSN с помощью Консоли программы

► *Чтобы настроить задачу Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
   - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Embedded Systems Security для Windows при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалять**

       Kaspersky Embedded Systems Security для Windows удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

       Этот вариант выбран по умолчанию.
     - **Фиксировать информацию в отчете**

       Kaspersky Embedded Systems Security для Windows фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security для Windows не удаляет недоверенный объект.
   - В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
     - 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 Embedded Systems Security для Windows не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

       Если флажок снят, Kaspersky Embedded Systems Security для Windows рассчитывает контрольную сумму для файлов любого размера.

       По умолчанию флажок установлен.
     - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security для Windows будет рассчитывать контрольную сумму.

5. Если требуется, настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

   Программа будет запускать задачу Использование KSN по расписанию.

6. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. 375).

7. Нажмите на кнопку **OK**.

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

## Настройка обработки данных с помощью Консоли программы

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.

2. Выберите вложенный узел **Использование KSN**.

3. В панели результатов перейдите по ссылке **Положение о KSN**.

   Откроется окно **Положение о Kaspersky Security Network**.

4. На закладке **Службы и статистика KSN** прочитайте текст Положения и установите флажок **Я принимаю условия использования Kaspersky Security Network**.

5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не отправляет контрольные суммы файлов в KSN.

     Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено «Лабораторией Касперского» с целью защиты репутационных серверов от DDoS*.

     По умолчанию флажок установлен.

- **Разрешить отправку статистики Kaspersky Security Network**

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не отправляет дополнительную статистику.

  По умолчанию флажок установлен.

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

6. Флажок **Разрешить отправку статистики Kaspersky Security Network** установлен по умолчанию. Вы можете снять флажок в любое время, если не хотите, чтобы программа Kaspersky Embedded Systems Security для Windows отправляла дополнительную статистику в "Лабораторию Касперского".

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не отправляет дополнительную статистику.

   По умолчанию флажок установлен.

7. Нажмите на кнопку **OK**.

Конфигурация обработки данных будет сохранена.

# Управление использованием KSN с помощью Веб-плагина

► *Чтобы настроить использование KSN и обработку данных с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Использование KSN**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 57. Настройка параметров задачи Использования KSN и обработки данных с помощью Плагина управления*

| Параметр | Описание |
|---|---|
| **Удалять** | Kaspersky Embedded Systems Security для Windows удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.<br>Этот вариант выбран по умолчанию. |
| **Фиксировать информацию в отчете** | Kaspersky Embedded Systems Security для Windows фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security для Windows не удаляет недоверенный объект. |
| **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает** | Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.<br>Продолжительность расчета контрольной суммы зависит от размера файла.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows рассчитывает контрольную сумму для файлов любого размера.<br>По умолчанию флажок установлен. |
| **Принять условия Положения о Kaspersky Security Network** | Устанавливая этот флажок, вы подтверждаете, что прочитали и принимаете условия Положения о Kaspersky Security Network. |

| Параметр | Описание |
| --- | --- |
| **Разрешить отправку данных о проверяемых файлах** | Если флажок установлен, Kaspersky Embedded Systems Security для Windows отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.<br><br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не отправляет контрольные суммы файлов в KSN.<br><br>Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено «Лабораторией Касперского» с целью защиты репутационных серверов от DDoS*.<br><br>По умолчанию флажок установлен. |
| **Разрешить отправку статистики Kaspersky Security Network** | Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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.<br><br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не отправляет дополнительную статистику.<br><br>По умолчанию флажок установлен. |
| Управление задачами | Вы можете настроить расписание запуска задачи. |

# Настройка передачи дополнительных данных

В Kaspersky Embedded Systems Security для Windows можно настроить отправку в "Лабораторию Касперского" следующих данных:

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

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

Соответствующие флажки можно установить или снять (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. 375), только если установлен флажок **Я принимаю условия использования Kaspersky Security Network**.

По умолчанию Kaspersky Embedded Systems Security для Windows отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

Состояние флажка **Я принимаю условия использования Kaspersky Security Network** невозможно изменить, если политика Kaspersky Security Center запрещает изменение параметров, связанных с обработкой данных.

*Таблица 58. Возможные состояния флажков и соответствующие условия*

| **Состояние флажка** | **Условия для состояния флажка** Разрешить отправку данных о проверяемых файлах | **Условия для состояния флажка** Разрешить отправку статистики Kaspersky Security Network | **Условия для состояния флажка** Я принимаю условия использования Kaspersky Security Network |
|---|---|---|---|
| ☑ | • отправляются запросы репутации<br>• действия с флажком доступны | • отправляется дополнительная статистика<br>• действия с флажком доступны | • принимаются условия Положения о Kaspersky Security Network<br>• действия с флажком доступны |
| ☑ | • отправляются запросы репутации<br>• действия с флажком недоступны | • отправляется дополнительная статистика<br>• действия с флажком недоступны | • принимаются условия Положения о Kaspersky Security Network<br>• действия с флажком недоступны |

| Состояние флажка | Условия для состояния флажка Разрешить отправку данных о проверяемых файлах | Условия для состояния флажка Разрешить отправку статистики Kaspersky Security Network | Условия для состояния флажка Я принимаю условия использования Kaspersky Security Network |
|---|---|---|---|
| ☐ | • не отправляются запросы репутации<br>• действия с флажком доступны | • не отправляется дополнительная статистика<br>• действия с флажком доступны | • не принимаются условия Положения о Kaspersky Security Network<br>• действия с флажком доступны |
| ☐ | • не отправляются запросы репутации<br>• действия с флажком недоступны | • не отправляется дополнительная статистика<br>• действия с флажком недоступны | • не принимаются условия Положения о Kaspersky Security Network<br>• действия с флажком недоступны |

# Статистика задачи Использование KSN

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

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

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.

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

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Embedded Systems Security для Windows обработала за время выполнения задачи (см. таблицу ниже).

*Таблица 59. Статистика задачи Использование KSN*

| Поле | Описание |
|---|---|
| **Ошибки отправки запросов** | Количество запросов в KSN, во время обработки которых возникла ошибка задачи. |
| **Пакетов статистик сформировано** | Количество пакетов с данными, которые были отправлены на обработку в KSN. |
| **Удалено объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows удалила в результате выполнения задачи Использование KSN. |
| **Помещено в резервное хранилище** | Количество объектов, копии которых программа Kaspersky Embedded Systems Security для Windows сохранила в резервном хранилище. |
| **Объектов не удалено** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи. |
| **Объектов, не помещенных в резервное хранилище** | Количество объектов, копии которых программа Kaspersky Embedded Systems Security для Windows попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи. |
| **Ограниченный режим** | Статус отправки запросов файловой репутации в ограниченном режиме. В ограниченном режиме Kaspersky Embedded Systems Security для Windows отправляет только часть запросов о репутации файлов, в соответствии с рекомендациями специалистов "Лаборатории Касперского". |

kaspersky

# Защита от сетевых угроз

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

## В этом разделе


О задаче Защита от сетевых угроз ..... 382

Параметры по умолчанию для задачи Защита от сетевых угроз ..... 383

Настройка задачи Защита от сетевых угроз с помощью Консоли программы ..... 383

Настройка задачи Защита от сетевых угроз с помощью Плагина управления..... 384

Настройка задачи Защита от сетевых угроз с помощью Веб-плагина ..... 386


## О задаче Защита от сетевых угроз

Защиту от сетевых угроз можно установить только на устройства с операционной системой Microsoft Windows 7 и более поздних версий или Windows Server 2008 R2 и более поздних версий.

Задача Защита от сетевых угроз выполняет проверку входящего сетевого трафика на наличие действий, характерных для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Embedded Systems Security для Windows блокирует сетевую активность со стороны атакующего компьютера. На экране отображается предупреждение, сообщающее о попытке сетевой атаки и содержащее информацию об атакующем компьютере.

По умолчанию задача Защита от сетевых угроз выполняется в режиме **Блокировать соединения при обнаружении атаки**. В этом режиме Kaspersky Embedded Systems Security для Windows добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

IP-адреса узлов, проявляющих активность, характерную для сетевых атак, удаляются из списка заблокированных узлов в следующих случаях:

- Программа Kaspersky Embedded Systems Security для Windows удалена.
- IP-адрес удален из списка заблокированных узлов вручную.
- Истек срок блокировки узла.
- Завершилось выполнение задачи Защита от сетевых угроз и не установлен флажок **Не останавливать анализ трафика, если задача не исполняется**.
- Выключен режим **Блокировать соединения при обнаружении атаки**.

# Параметры по умолчанию для задачи Защита от сетевых угроз

По умолчанию в задаче Защита от сетевых угроз используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 60. Параметры по умолчанию для задачи Защита от сетевых угроз*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Режим работы** | **Только уведомлять об обнаруженных атаках** | Задачу Защита от сетевых угроз можно запустить в одном из следующих режимов: **Не осуществлять мониторинг**, **Только уведомлять об обнаруженных атаках** или **Блокировать соединения при обнаружении атаки**. |
| **Исключения** | Список исключений не используется. | Укажите области, которые вы хотите исключить из области защиты. |
| **Параметры расписания** | По умолчанию, задача Защита от сетевых угроз запускается автоматически при запуске Kaspersky Embedded Systems Security для Windows. | Можно настроить расписание. |

# Настройка задачи Защита от сетевых угроз с помощью Консоли программы

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Консоли программы.

## В этом разделе

Общие параметры задачи ..... 383
Добавление исключений ..... 384

## Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.

3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от сетевых угроз**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Общие**.
5. В разделе **Режим работы** выберите режим работы задачи:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
6. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
7. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
8. Нажмите на кнопку **OK**.

## Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Защита от сетевых угроз**.

   Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
5. Укажите IP-адрес и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **OK**.

# Настройка задачи Защита от сетевых угроз с помощью Плагина управления

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Плагина управления.

### В этом разделе

Общие параметры задачи ..... 385
Добавление исключений ..... 385

## Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Постоянная защита компьютера** в блоке **Защита от сетевых угроз** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от сетевых угроз**.
5. Выберите закладку **Общие**.
6. В разделе **Режим работы** выберите режим работы задачи:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
7. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
8. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
9. Нажмите на кнопку **OK**.

## Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

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

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.
5. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
6. Укажите IP-адрес и нажмите на кнопку **Добавить**.
7. Нажмите на кнопку **OK**.

# Настройка задачи Защита от сетевых угроз с помощью Веб-плагина

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Веб-плагина.

## В этом разделе

Общие параметры задачи ..... 386
Добавление исключений ..... 387

## Общие параметры задачи

► *Чтобы настроить общие параметры задачи Защита от сетевых угроз с помощью Веб-консоли:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. В блоке **Защита от сетевых угроз** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от сетевых угроз**.
6. Выберите вкладку **Общие**.

7. В разделе **Режим работы** выберите режим обработки:
   - **Не осуществлять мониторинг**.
   - **Только уведомлять об обнаруженных атаках**.
   - **Блокировать соединения при обнаружении атаки**.
8. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
9. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.
10. Нажмите на кнопку **OK**.

## Добавление исключений

► *Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.
6. На закладке **Исключения** установите флажок **Не контролировать IP-адреса, указанные в исключениях**.
7. Укажите IP-адрес и нажмите на кнопку **Добавить**.
8. Нажмите на кнопку **OK**.

kaspersky

# Контроль запуска программ

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

## В этом разделе


О задаче Контроль запуска программ ..... 388

О правилах контроля запуска программ ..... 390

О Контроле пакетов установки ..... 392

Об использовании KSN в задаче Контроль запуска программ ..... 394

О формировании правил контроля запуска программ ..... 395

Параметры по умолчанию для задачи Контроль запуска программ ..... 397

Управление контролем запуска программ с помощью Плагина управления ..... 401

Управление контролем запуска программ с помощью Консоли программы ..... 425

Управление контролем запуска программ с помощью Веб-плагина ..... 446


## О задаче Контроль запуска программ

Во время выполнения задачи Контроль запуска программ Kaspersky Embedded Systems Security для Windows проверяет попытки пользователей запускать различные программы и разрешает или запрещает запуск этих программ. Задача Контроль запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются.

Вы можете разрешить запуск программ одним из следующих способов:

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

Запрет запуска программы имеет в задаче более высокий приоритет. Например, если запуск программы запрещен одним из правил, программа не будет запущена, независимо от заключения KSN о доверенности программы. При этом если программа признана недоверенной службами KSN, но подпадает под действие разрешающего правила, запуск такой программы будет запрещен.

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

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

- **Активный**. Kaspersky Embedded Systems Security для Windows с помощью набора правил контролирует запуск программ, которые попадают под действия правил контроля запуска программ. Область применения правил контроля запуска программ указывается в параметрах этой задачи. Если программа удовлетворяет правилам контроля запуска программ, а параметры задачи не удовлетворяют ни одному из указанных правил, то запуск такой программы будет запрещен.

  Запуск программ, которые не подпадают под действие правил, указанных в параметрах задачи Контроль запуска программ, не разрешается, независимо от параметров задачи Контроль запуска программ.

  Задачу **Контроль запуска программ** нельзя запустить в активном режиме, если не создано ни одного правила или если для одного защищаемого устройства создано более 65535 правил.

- **Только статистика**. В Kaspersky Embedded Systems Security для Windows не используются правила контроля запуска программ для запрета или разрешения запуска программ. Выполняется только запись информации обо всех запусках программ, правилах, выполненных при запуске программ, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Активный**. Разрешен запуск всех программ. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования правил контроля запуска программ (см. раздел "Формирование разрешающих правил по событиям задачи Контроль запуска программ" на стр. 439) на основе информации, зафиксированной в журнале выполнения задачи.

Вы можете настроить задачу Контроль запуска программ по одному из следующих сценариев:

- Дополнительная настройка (см. раздел "О правилах контроля запуска программ" на стр. 390) и применение правил контроля запуска программ.
- Базовая настройка правил и использование KSN (см. раздел "Настройка использования KSN" на стр. 430) для контроля запуска программ.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Kaspersky Embedded Systems Security для Windows также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ фиксирует запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

# О правилах контроля запуска программ

**Как работают правила контроля запуска программ**

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешить или запретить запуск программы. Соответственно, они называются *разрешающими* или *запрещающими*. Для создания списка разрешающих правил контроля запуска программ можно использовать задачу формирования разрешающих правил или задачу Контроль запуска программ в режиме **Только статистика**. Можно также добавлять разрешающие правила вручную.

- Пользователь или группа пользователей.

  Правила контроля запуска программ контролируют запуск указанных программ пользователем или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут применяться к *исполняемым файлам*, *скриптам* и *пакетам MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих хотя бы одному из критериев, указанных в параметрах правила: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256*, расположены по указанному *пути*, соответствуют указанным аргументам *командной строки*. Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

  Если в качестве критерия срабатывания правила выбран **Цифровой сертификат**, созданное правило контролирует запуск всех доверенных программ в операционной системе. Вы можете задать более строгие условия для этого критерия, установив следующие флажки:

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

    Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

    По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывание правил запуска программ на основе цифрового сертификата, поскольку отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для определенных разрешающих правил: например, если требуется разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

### Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

# О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программного обеспечения на защищаемых устройствах, например, на защищаемых устройствах, где происходит регулярное автоматическое обновление установленного программного обеспечения. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения можно использовать подсистему Контроль пакетов установки.

*Пакет установки* (далее также "пакет") представляет собой программу, устанавливаемую на защищаемое устройство. В каждом пакете содержится как минимум одна программа, а также могут содержаться отдельные файлы, обновления и отдельные команды, в частности, когда выполняется установка программы или обновления.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. При добавлении пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Embedded Systems Security для Windows контролирует только полный цикл распространения программного обеспечения. Программа не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен компонент Контроль пакетов установки или не был установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в параметрах задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

### Кеш распространения программного обеспечения

Kaspersky Embedded Systems Security для Windows использует динамически формируемый кеш распространения программного обеспечения (далее "кеш распространения") для связи между доверенными пакетами и файлами, созданными во время распространения программного обеспечения. При первом запуске пакета Kaspersky Embedded Systems Security для Windows обнаруживает все файлы, созданные этим пакетом во время распространения программного обеспечения, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем, по умолчанию, разрешается запуск всех файлов в кеше распространения.

Кеш распространения нельзя просматривать, очищать и изменять вручную через пользовательский интерфейс. Kaspersky Embedded Systems Security для Windows самостоятельно наполняет его, а также контролирует его актуальность.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и очищать с помощью команд командной строки.

► *Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Чтобы полностью очистить кеш распространения, выполните команду:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security для Windows обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла программа удаляет запись для этого файла из кеша распространения. При активном режиме работы задачи Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

**Обработка извлеченных файлов**

Все извлеченные из доверенного пакета файлы наследуют атрибут доверенности при первом запуске пакета. При снятии флажка после первого запуска все извлеченные из пакета файлы сохраняют атрибут наследования. Чтобы отменить признак наследования для всех извлеченных файлов, необходимо очистить кеш распространения и снять флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** перед следующим запуском доверенного пакета установки.

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки, наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными. По умолчанию количество уровней наследования признака доверенности не ограничено.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 406) с помощью флажка **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и установлен флажок, то все пакеты и программы, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** не установлен, программа присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (только первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

### Работа со списком правил контроля запуска программ

Список доверенных пакетов подсистемы Контроля пакетов установки – это список исключений, который дополняет, но не заменяет основной список правил контроля запуска программ.

Запрещающие правила контроля запуска программ имеют абсолютный приоритет: распаковка доверенного пакета или запуск созданных и измененных им файлов будут заблокированы, если такие пакеты и файлы подпадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

### Использование заключений KSN

Заключения KSN о том, что файл является недоверенным, имеют более высокий приоритет, чем исключения Контроля пакетов установки. Распаковка доверенных пакетов и запуск файлов, созданных или измененных доверенными пакетами, будет заблокирован, если для таких файлов получено заключение KSN о том, что файл является недоверенным.

При распаковке из доверенного пакета, запуск всех вложенных файлов будет разрешен, независимо от использования KSN в задаче Контроль запуска программ. При этом значение флажков **Запрещать запуск программ, недоверенных в KSN** и **Разрешать запуск программ, доверенных в KSN** не влияет на флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

## Об использовании KSN в задаче Контроль запуска программ

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

Если данные KSN о репутации программы используются в задаче Контроль запуска программ, репутация программы по данным KSN считается основным критерием для разрешения или запрета запуска этой программы. Если KSN передает Kaspersky Embedded Systems Security для Windows данные о том, что программа не является доверенной, то попытка пользователя запустить программу блокируется. Если KSN передает Kaspersky Embedded Systems Security для Windows данные о том, что программа является доверенной, то разрешается запуск программы пользователем. KSN можно применять совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

### Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом устройстве без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Embedded Systems Security для Windows вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

> При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом запрета по умолчанию. Применение KSN при отсутствии правил позволяет защитить устройство от программ, которые по данным KSN представляют угрозу.

**Применение заключений KSN совместно с правилами контроля запуска программ**

При использовании заключений KSN совместно с правилами контроля запуска программ применяются следующие условия:

- Kaspersky Embedded Systems Security для Windows всегда блокирует запуск программы, если она подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволит расширить список заблокированных программ.
- Kaspersky Embedded Systems Security для Windows всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для этой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить устройство от программ, которые по данным KSN представляют угрозу, но не были учтены при первоначальной настройке правил.

# О формировании правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых устройств и групп защищаемых устройств в сети организации. Рекомендуется использовать перечисленные сценарии, если в сети организации нет эталонной машины и вы не можете сформировать список разрешающих правил на основе программ, установленным на такой эталонной машине.

Можно запустить задачу Формирование правил контроля запуска программ локально с помощью Консоли программы для создания списка правил на основе программ, запущенных на отдельном защищаемом устройстве.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающее правило для скриптов и пакетов установщика Windows с сертификатом, доверенным в операционной системе.
- Разрешающее правило для исполняемых файлов с сертификатом, доверенным в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи Формирование правил контроля запуска программ.

  В рамках этого сценария групповая задача формирует собственный список правил контроля запуска программ для каждого защищаемого устройства в сети и сохраняет эти списки в XML-файл в указанной папке общего доступа. XML-файл, созданный задачей Формирование правил контроля запуска программ, содержит разрешающие правила, указанные при настройке параметров задачи, до ее запуска. Для программ, запуск которых не разрешен в параметрах указанной задачи, не будет создано ни одного правила. Запуск таких программ будет заблокирован по умолчанию. Затем вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ для политики Kaspersky Security Center.

Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Рекомендуется использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

- На основе отчета о событиях в работе задачи Контроль запуска программ в режиме **Только статистика**, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Embedded Systems Security для Windows не блокирует запуск программ. Когда задача Контроль запуска программ работает в режиме **Только статистика**, все разрешенные и запрещенные запуски программ на всех защищаемых устройствах сети регистрируются на закладке **События** в рабочей области узла Сервера администрирования в Kaspersky Security Center. С помощью отчетов в Kaspersky Security Center формируется единый список событий о заблокированных запусках программ.

  Вам нужно настроить период выполнения задачи так, чтобы за указанный промежуток времени выполнились все возможные сценарии работы защищаемых устройств и групп защищаемых устройств и хотя бы одна перезагрузка. После завершения выполнения задачи можно импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

  Рекомендуется использовать этот сценарий, если в сети организации имеется большое количество защищаемых устройств разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на защищаемом устройстве должна находиться под управлением активной политики Kaspersky Security Center. При этом все события на защищаемом устройстве передаются на Сервер администрирования.

Рекомендуется обновить список правил при изменении состава программ, установленных на управляемых компьютерах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется сформировать обновленный список правил, запустив задачу Формирование правил контроля запуска программ или задачу Контроль запуска программ в режиме **Только статистика** на защищаемых устройствах тестовой группы администрирования. Тестовая группа администрирования включает защищаемые устройства, необходимые для тестового запуска новых программ перед их установкой на остальные защищаемые устройства сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом устройстве. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуется запускать задачи Формирование правил контроля запуска программ и Контроль запуска программ в режиме **Только статистика** на эталонной машине.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.

# Параметры по умолчанию для задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 61. Параметры по умолчанию для задачи Контроль запуска программ*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Режим работы**. | **Только статистика**. Задача регистрирует события, соответствующие попыткам запуска программ, запрещенным или разрешенным на основе набора правил. Фактическая блокировка запуска программ не выполняется. | Вы можете выбрать режим **Активный** после того, как будет сформирован окончательный список правил. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска** | Не применяется | Можно повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках. |
| **Запрещать запуск командных интерпретаторов без команды к исполнению** | Не применяется. | Вы можете запрещать запуск командных интерпретаторов без исполняемых команд. |
| **Правила** | **Добавить правила политики к локальным правилам** | Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на защищаемом устройстве. |
| **Область применения правил** | Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов. Кроме того, задача контролирует загрузку DLL-модулей. | Вы можете указывать типы файлов, запуск которых будет контролироваться правилами. |
| **Использование KSN** | Данные KSN о репутации программы не используются. | Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ. |
| **Автоматически разрешать распространение с помощью указанных программ и пакетов установки** | Не применяется. | Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию распространение программ разрешено только с помощью служб установщика Windows. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Всегда разрешать распространение программ с помощью установщика Windows** | Применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**. | Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются с помощью установщика Windows. |
| **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи** | Не применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**. | Можно включить или выключить автоматическое распространение программного обеспечения с помощью решения System Center Configuration Manager. |
| **Параметры запуска задачи** | Время первого запуска не задано. | Задача Контроль запуска программ не запускается автоматически сразу после Kaspersky Embedded Systems Security для Windows. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |

*Таблица 62. Заданные по умолчанию параметры задачи Формирование правил контроля запуска программ*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Префикс для названий разрешающих правил | Совпадает с именем защищаемого устройства, на котором установлена программа Kaspersky Embedded Systems Security для Windows. | Вы можете изменить префикс для названий разрешающих правил. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Область применения разрешающих правил | Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов:<br>• файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files;<br>• пакеты MSI, расположенные в папке C:\Windows;<br>• скрипты, расположенные в папке C:\Windows.<br>Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата. | Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых будет разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы. |
| Критерии формирования разрешающих правил | Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей. | Вы можете использовать хеш SHA256 при формировании разрешающих правил.<br>Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила. |
| Действия по завершении задачи | Разрешающие правила добавляются в список правил контроля запуска программ; новые правила объединяются с существующими правилами; дублирующиеся правила удаляются. | Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующихся правил или заменять существующие правила новыми разрешающими правилами, а также настраивать параметры экспорта разрешающих правил в файл. |
| Параметры запуска задачи с правами | Задача запускается с правами системной учетной записи. | Вы можете разрешить запуск задачи Формирование правил контроля запуска программ с правами системной учетной записи или с правами указанного пользователя. |
| Расписание запуска задачи | Время первого запуска не задано. | Задача Формирование правил контроля запуска программ не запускается автоматически при запуске Kaspersky Embedded Systems Security для Windows. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |

kaspersky

# Управление контролем запуска программ с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

## В этом разделе


Навигация ..... 401

Настройка параметров задачи Контроль запуска программ ..... 403

Настройка Контроля пакетов установки ..... 406

Настройка задачи Формирование правил контроля запуска программ ..... 409

Настройка правил контроля запуска программ в Kaspersky Security Center ..... 411

Создание задачи Формирование правил контроля запуска программ ..... 421


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам политики для задачи Контроль запуска программ ..... 401

Переход к списку правил контроля запуска программ ..... 402

Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам ..... 402


### Переход к параметрам политики для задачи Контроль запуска программ

► *Чтобы перейти к параметрам задачи Контроль запуска программ в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.

Настройте политику в соответствии с вашими требованиями.

## Переход к списку правил контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

Настройте список правил в соответствии с вашими требованиями.

## Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам

► *Чтобы создать задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
5. Выберите задачу **Формирование правил контроля запуска программ**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.

4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля запуска программ**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля запуска программ.

## Настройка параметров задачи Контроль запуска программ

► *Чтобы настроить общие параметры задачи Контроль запуска программ:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 401).
2. На закладке **Общие** в разделе **Режим работы** настройте следующие параметры:
   - В раскрывающемся списке **Режим работы** выберите режим работы задачи.

     В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:

     - **Активный**. Kaspersky Embedded Systems Security для Windows использует определенные правила контроля запуска всех программ.
     - **Только статистика**. Kaspersky Embedded Systems Security для Windows не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.

     По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

   - Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

     Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет программу при каждой попытке ее запуска.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

- Запуск командного интерпретатора разрешен.
- Исполняемая команда разрешена.

Если флажок снят, Kaspersky Embedded Systems Security для Windows учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Embedded Systems Security для Windows работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

3. В блоке **Правила** настройте параметры применения правил:

   a. Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила в задачу Контроль запуска программ.

   Kaspersky Embedded Systems Security для Windows не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

   b. Выберите режим применения правил:

   - **Заменить правилами политики локальные правила**

     Программа применяет список правил, заданных в политике, для централизованного контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.

   - **Добавить правила политики к локальным правилам**

     Программа применяет список правил, заданный в политике, совместно с локальными списками правил. Вы можете редактировать локальные списки правил с помощью задач автоматического формирования правил контроля запуска программ.

4. В разделе **Область применения правил** укажите следующие параметры:

   - **Использовать правила для исполняемых файлов**.

     Флажок включает или выключает контроль запуска исполняемых файлов.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

     По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**.

  Флажок включает или выключает контроль загрузки DLL-модулей.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

  Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

  По умолчанию флажок установлен.

  Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**.

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

5. В блоке параметров **Использование KSN** настройте следующие параметры запуска программ:

- **Запрещать запуск программ, недоверенных в KSN**.

  Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

  По умолчанию флажок снят.

- **Разрешать запуск программ, доверенных в KSN**.

  Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows

разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ:
  a. В контекстном меню кнопки **Изменить** выберите способ добавления пользователей.

     Откроется окно **Выбор пользователя или группы пользователей**.

  b. Выберите пользователя или группу пользователей.

  c. Нажмите на кнопку **OK**.

6. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 406).
7. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания задач" на стр. 145).
8. В окне **Контроль запуска программ** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## Настройка Контроля пакетов установки

► *Чтобы добавить доверенный пакет установки с помощью Плагина управления:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 401).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки, разрешенных к запуску, доступен для редактирования.

   Если флажок снят, программа не применяет указанные в списке исключения.

   По умолчанию флажок снят.

Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Использовать правила для исполняемых файлов** в параметрах задачи **Общие** установлен флажок **Контроль запуска программ**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, добавленных в список разрешенных и запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

   Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

   По умолчанию флажок установлен.

   Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы создать список разрешенных или изменить существующий список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

     Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

     d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

     - **Использовать цифровой сертификат**
     - **Использовать хеш SHA256**

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security для Windows учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

   - **Изменить выбранный**

     Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

   - **Импортировать из текстового файла**.

     Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Embedded Systems Security для Windows такой файл должен удовлетворять следующим условиям:

     - иметь расширение TXT;
     - содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
     - содержать список, соответствующий одному из двух форматов:
       - <имя файла>:<хеш SHA256>.
       - <хеш SHA256>*<имя файла>.

     В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

Если вы создаете доверенный пакет установки на основе исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для задачи Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Embedded Systems Security для Windows запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 402).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:
   - Укажите префикс для названий правил.
   - Выберите способ создания разрешающих правил:
     - **Создавать разрешающие правила на основе запущенных программ**

       Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

       Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

       Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

       По умолчанию флажок снят.

       Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

     - **Создавать разрешающие правила для программ из папок**

       В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

4. В разделе **Параметры** можно указать действия при формировании разрешающих правил контроля запуска программ:

   - **Использовать цифровой сертификат**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

     Этот вариант выбран по умолчанию.

   - **Использовать заголовок и отпечаток цифрового сертификата**

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

     Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security для Windows разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

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

     Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

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

     По умолчанию флажок установлен.

   - **Если сертификат отсутствует, использовать**

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

     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

     - **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

   - **Использовать хеш SHA256**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем

программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

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

  По умолчанию выбрана группа **Все**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security для Windows создает по завершении задач.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
7. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

# Настройка правил контроля запуска программ в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

## В этом разделе

Добавление правила контроля запуска программ ..... 412
Включение режима разрешения по умолчанию ..... 415
Формирование разрешающих правил контроля запуска программ на основе событий Kaspersky Security Center ..... 416
Импорт правил из отчета Kaspersky Security Center о заблокированных программах ..... 417
Импорт правил контроля запуска программ из XML-файла ..... 418
Проверка запуска программ ..... 420

## Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ с помощью Плагина управления:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 402).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила:
      i. В контекстном меню кнопки **Выбрать** выберите способ добавления доверенных пользователей.

         Откроется окно **Выбор пользователя или группы пользователей**.
      ii. Выберите пользователя или группу пользователей.
      iii. Нажмите на кнопку **OK**.
   e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:
      i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.
      ii. Выберите файл.
      iii. Нажмите на кнопку **Открыть**.

         Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке параметров **Критерий срабатывания правила** выберите как минимум один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.
  - **Командная строка**, чтобы правило контролировало запуск программ, осуществляемый с помощью аргументов, указанных в поле командной строки. Поле доступно при выборе варианта **Путь к файлу**. При указании аргументов командной строки для запущенных процессов в качестве критерия можно использовать маску, включающую символы ? и *.

> Kaspersky Embedded Systems Security для Windows не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.
> При указании объектов можно использовать символы ? и * в качестве маски файлов.

Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

i. В разделе **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения.

iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  Этот вариант выбран по умолчанию.

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

  Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

  Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **хеш SHA256**

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

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

iv. Нажмите на кнопку **OK**.

v. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

## Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 402).
2. Нажмите на кнопку **Добавить** и в открывшемся контекстном меню выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
3. В поле **Название** введите название правила.
4. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
5. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
6. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
7. Введите следующую маску: `?:\`
8. В окне **OK** нажмите на кнопку **Параметры правила**.

Kaspersky Embedded Systems Security для Windows применяет режим разрешения по умолчанию.

## Формирование разрешающих правил контроля запуска программ на основе событий Kaspersky Security Center

► *Чтобы сформировать разрешающие правила контроля запуска программ на основе событий Kaspersky Security Center:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 402).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
4. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется окно **Формирование правил контроля запуска программ**.
5. Выберите типы событий, на основе которых программа будет создавать правила контроля запуска программ:
   - **Только статистика: запуск программы запрещен**.
   - **Запуск программы запрещен**.
6. Выберите период из раскрывающегося списка **Учитывать события, сформированные в течение периода**.
7. Если необходимо, в поле **Использовать события, сформированные для группы управляемых устройств** введите имя или фрагмент имени группы управляемых с помощью Kaspersky Security Center устройств, события для которых будут основой для формирования правил контроля запуска программ.
8. Снимите или установите флажок **Приоритизировать использование контрольной суммы при создании правил**.
9. Нажмите на кнопку **Создать правила**.
10. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

    Список правил в задаче Контроль запуска программ будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

    > Правила с повторяющимся хешем не добавляются, поскольку все правила в списке должны быть уникальными.

## Импорт правил из отчета Kaspersky Security Center о заблокированных программах

Вы можете импортировать данные о заблокированных запусках программ из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль запуска программ в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил запуска программ в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль запуска программ, вы можете отслеживать программы, запуск которых был заблокирован.

При импорте из отчета данных о заблокированных программах в свойства политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

► *Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 401).
2. В блоке **Режим работы** выберите режим **Только статистика**.
3. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что:
   - Для событий с уровнем важности **Критический** срок хранения событий **Запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).
   - Для событий с уровнем важности **Предупреждение** срок хранения событий **Только статистика: запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

     По истечении срока хранения событий информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль запуска программ в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленный срок хранения указанных событий.
4. По завершении задачи выполните экспорт зарегистрированных событий в файл формата TXT:
   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.
   b. Нажмите на кнопку **Создать выборку**, чтобы создать выборку событий по критерию Заблокировано и просмотреть, запуск каких программ будет заблокирован задачей Контроль запуска программ.
   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых требуется разрешить.

5. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку настроенных ранее правил контроля запуска программ:

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

   a. **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила. В открывшемся стандартном окне Microsoft Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

   b. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

## Импорт правил контроля запуска программ из XML-файла

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Формирование правил контроля запуска программ, и применить их в качестве списка разрешающих правил в настраиваемой политике.

По завершении групповой задачи формирования правил контроля запуска программ выполняется экспорт созданных разрешающих правил в XML-файлы в указанную папку общего доступа. Каждый файл со списком правил создается на основе анализа исполняемых файлов и запущенных программ на каждом отдельном защищаемом устройстве в сети организации. Списки содержат разрешающие правила для файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче формирования правил контроля запуска программ.

► *Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** в панели результатов настраиваемой группы защищаемых устройств создайте групповую задачу Формирование правил контроля запуска программ или выберите уже созданную задачу (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 402).

2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
   - В разделе **Уведомление** настройте параметры сохранения отчета выполнения задачи.

     Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

   - В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Можно изменить набор папок, содержащих разрешенные для запуска программы: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
   - В разделе **Параметры** укажите действия, выполняемые задачей во время работы и после завершения. Укажите критерий формирования правил и имя файла, в который будут экспортированы эти правила.
   - В разделе **Расписание** настройте параметры запуска задачи по расписанию.
   - В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
   - В разделе **Исключения из области действия задачи** задайте группы защищаемых устройств, которые вы хотите исключить из области действия задачи.

     Kaspersky Embedded Systems Security для Windows не будет создавать разрешающие правила по программам, запускаемым на исключенных защищаемых устройствах.

3. На закладке **Задачи** в панели результатов настраиваемой группы защищаемых устройств в списке групповых задач выберите созданную задачу Формирование правил контроля запуска программ и нажмите на кнопку **Запустить** для запуска задачи.

   После завершения задачи, автоматически сформированные списки разрешающих правил будут сохранены в XML-файлы в папке общего доступа.

   Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

4. Чтобы добавить сформированные списки разрешающих правил в задачу Контроль запуска программ, выполните следующие действия:
   a. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 402).
   b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:

- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
- **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

d. В открывшемся стандартном окне Microsoft Windows выберите XML-файлы, созданные по завершении групповой задачи Формирование правил контроля запуска программ.

e. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

5. Если вы хотите применять созданные правила для контроля запуска программ, в политике в свойствах задачи Контроль запуска программ выберите режим **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном защищаемом устройстве, будут применены на всех защищаемых устройствах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых устройств программа разрешит запуск только тех программ, для которых созданы разрешающие правила.

## Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу, чтобы определить, какие правила контроля запуска программ срабатывают для выбранной программы.

По умолчанию Kaspersky Embedded Systems Security для Windows блокирует программы, запуск которых не разрешен хотя бы одним правилом. Чтобы избежать блокировки запуска важных программ, необходимо создать для них разрешающие правила.

Если запуск программы контролируется несколькими правилами разных типов, запрещающие правила имеют больший приоритет: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы проверить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 402).
2. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
3. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все правила, которые сработают при запуске указанного файла.

## Создание задачи Формирование правил контроля запуска программ

► *Чтобы создать задачу Формирование правил контроля запуска программ и настроить ее параметры, выполните следующие действия:*

1. Откройте окно **Настройка** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 402).
2. Настройте следующие параметры:
   - Укажите **Префикс для названий правил**.

     Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

     По умолчанию в качестве префикса указано имя защищаемого устройства, на котором установлена программа Kaspersky Embedded Systems Security для Windows. Вы можете изменить префикс для названий разрешающих правил.
   - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 442).
3. Нажмите на кнопку **Далее**.
4. Укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security для Windows:
   - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. 442);
   - по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. 445).
5. В окне **Расписание** укажите параметры запуска задачи по расписанию.
6. Нажмите на кнопку **Далее**.
7. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
8. Нажмите на кнопку **Далее**.
9. Укажите название задачи.
10. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
11. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
12. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

► *Чтобы настроить существующее правило в Kaspersky Security Center,*

откройте окно **Свойства: Формирование правил контроля запуска программ** и настройте параметры, как описано выше.

Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе

Ограничение области действия задачи ..... 422
Действия при автоматическом формировании правил ..... 423
Действия по завершении автоматического формирования правил ..... 424

## Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 402)
2. Выберите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных программ**

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок снят.

     Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.
   - **Создавать разрешающие правила для программ из папок**

     В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Действия при автоматическом формировании правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security для Windows во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 402).
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:
   - **Использовать цифровой сертификат**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

     Этот вариант выбран по умолчанию.

   - **Использовать заголовок и отпечаток цифрового сертификата**

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

     Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security для Windows разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

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

     Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

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

     По умолчанию флажок установлен.

   - **Если сертификат отсутствует, использовать**

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

     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

- **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**

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

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

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

  По умолчанию выбрана группа **Все**.

4. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security для Windows по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 402).
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не добавляет новые сформированные разрешающие правила в список правил контроля запуска

программ. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

- **Принцип добавления**.

  Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.
- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

  По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

# Управление контролем запуска программ с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе

Навигация ..... 426
Настройка параметров задачи Контроль запуска программ ..... 427
Настройка правил контроля запуска программ ..... 434
Настройка задачи Формирование правил контроля запуска программ ..... 441

kaspersky

# Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам задачи Контроль запуска программ ..... 426

Переход к окну с правилами контроля запуска программ..... 426

Переход к параметрам задачи Формирование правил контроля запуска программ..... 426


### Переход к параметрам задачи Контроль запуска программ

► *Чтобы перейти к общим параметрам задачи Контроль запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

### Переход к окну с правилами контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Настройте список правил в соответствии с вашими требованиями.

### Переход к параметрам задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

kaspersky

# Настройка параметров задачи Контроль запуска программ

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

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 426).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 428).
     - Область применения правил в задаче (см. раздел "Настройка области действия задачи Контроль запуска программ" на стр. 429).
     - Использование KSN (см. раздел "Настройка использования KSN" на стр. 430).
   - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. 432) на закладке **Контроль пакетов установки**.
   - Расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165) на закладках **Расписание** и **Дополнительно**.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## В этом разделе


Выбор режима работы задачи Контроль запуска программ ..... 428

Настройка области действия задачи Контроль запуска программ ..... 429

Настройка использования KSN ..... 430

Контроль пакетов установки ..... 432

## Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 426).
2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим работы задачи.

   В раскрывающемся списке вы можете выбрать режим работы задачи Контроль запуска программ:

   - **Активный**. Kaspersky Embedded Systems Security для Windows контролирует все запускаемые программы с помощью заданных правил.
   - **Только статистика**. Kaspersky Embedded Systems Security для Windows не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о блокировках, зарегистрированной в журнале выполнения задачи.

   По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.
3. Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

   Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет программу при каждой попытке ее запуска.

   По умолчанию флажок снят.

Kaspersky Embedded Systems Security для Windows заводит новый список событий в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом, контроль запуска программ осуществляется в соответствии с актуальными параметрами безопасности.

4. Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

   - Запуск командного интерпретатора разрешен.
   - Исполняемая команда разрешена.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

   Kaspersky Embedded Systems Security для Windows работает со следующими командными интерпретаторами:

   - cmd.exe;
   - powershell.exe;
   - python.exe;
   - perl.exe.

   По умолчанию флажок снят.

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

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

## Настройка области действия задачи Контроль запуска программ

► *Чтобы задать область действия задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 426).
2. На закладке **Общие** в блоке **Область применения правил** задайте следующие параметры:
   - **Использовать правила для исполняемых файлов**

     Флажок включает или выключает контроль запуска исполняемых файлов.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**

  Флажок включает или выключает контроль загрузки DLL-модулей.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

  Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

  По умолчанию флажок установлен.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Настройка использования KSN

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 426).

2. На закладке **Общие** в блоке **Использование KSN** укажите параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.
   - Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.
   - Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, укажите пользователей и группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

     a. Нажмите на кнопку **Изменить**.

     Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

     По умолчанию доступ к доверенным в KSN программам разрешен всем пользователям.

     b. Задайте список пользователей и / или групп пользователей.

     c. Нажмите на кнопку **OK**.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Контроль пакетов установки

► *Чтобы добавить доверенный пакет установки с помощью Консоли программы:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 426).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки, разрешенных к запуску, доступен для редактирования.

   Если флажок снят, программа не применяет указанные в списке исключения.

   По умолчанию флажок снят.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Использовать правила для исполняемых файлов** в параметрах задачи **Общие** установлен флажок **Контроль запуска программ**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, добавленных в список разрешенных и запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

   Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

   По умолчанию флажок установлен.

   Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

   Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы создать список разрешенных или изменить существующий список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

        Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

     d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

        - **Использовать цифровой сертификат**
        - **Использовать хеш SHA256**

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security для Windows учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

   - **Изменить выбранный**

     Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**.

  Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Embedded Systems Security для Windows такой файл должен удовлетворять следующим условиям:

  - иметь расширение TXT;
  - содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
  - содержать список, соответствующий одному из двух форматов:
    - <имя файла>:<хеш SHA256>.
    - <хеш SHA256>*<имя файла>.

  В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

> Если вы создаете доверенный пакет установки на основе исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для задачи Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Embedded Systems Security для Windows запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

> Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

# Настройка правил контроля запуска программ

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

## В этом разделе

Добавление правила контроля запуска программ ..... 435
Включение режима разрешения по умолчанию ..... 438
Формирование разрешающих правил по событиям задачи Контроль запуска программ ..... 439
Экспорт правил контроля запуска программ ..... 439
Импорт правил контроля запуска программ из XML-файла ..... 440
Удаление правил контроля запуска программ ..... 440

## Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ с помощью Консоли программы:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к окну с правилами контроля запуска программ**" на стр. 426).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила:
      i. В контекстном меню кнопки **Выбрать** выберите способ добавления доверенных пользователей.

         Откроется окно **Выбор пользователя или группы пользователей**.
      ii. Выберите пользователя или группу пользователей.
      iii. Нажмите на кнопку **OK**.
   e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:
      i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.
      ii. Выберите файл.
      iii. Нажмите на кнопку **Открыть**.

         Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке параметров **Критерий срабатывания правила** выберите как минимум один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.
  - **Командная строка**, чтобы правило контролировало запуск программ, осуществляемый с помощью аргументов, указанных в поле командной строки. Поле доступно при выборе варианта **Путь к файлу**. При указании аргументов командной строки для запущенных процессов в качестве критерия можно использовать маску, включающую символы ? и *.

> Kaspersky Embedded Systems Security для Windows не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.
> При указании объектов можно использовать символы ? и * в качестве маски файлов.

Требуется выбрать хотя бы один вариант. В противном случае правило контроля запуска программ не будет добавлено.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

i. В разделе **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения.

iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  Этот вариант выбран по умолчанию.

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

  Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

  Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **хеш SHA256**

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

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Путь к файлу**

  Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

iv. Нажмите на кнопку **OK**.

v. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

## Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. В поле **Название** введите название правила.
5. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
6. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
7. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
8. Введите следующую маску: `?:\`
9. В окне **OK** нажмите на кнопку **Параметры правила**.

Kaspersky Embedded Systems Security для Windows применяет режим разрешения по умолчанию.

## Формирование разрешающих правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл с разрешающими правилами, сформированный по событиям задачи Контроль запуска программ, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел "**Выбор режима работы задачи Контроль запуска программ**" на стр. 428), чтобы регистрировать в журнале выполнения задачи информацию обо всех запусках программ на защищаемом устройстве.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security для Windows создаст конфигурационный файл в формате XML со списком правил, сформированных на основе событий задачи Контроль запуска программ, отработавшей в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. 440) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть и обработать вручную список правил, чтобы убедиться, что запуск важных файлов (например, файлов операционной системы) разрешен заданными правилами.

Все события задачи фиксируются в журнале выполнения задачи, независимо от режима работы задачи. Вы можете создать конфигурационный файл со списком правил на основе журнала, сформированного во время выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, поскольку финальный список правил должен быть сформирован перед запуском задачи в режиме **Активный**, чтобы правила работали эффективно.

## Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, при экспорте правил его содержимое будет перезаписано.
4. Нажмите на кнопку **Сохранить**.

Параметры правил будут экспортированы в указанный файл.

## Импорт правил контроля запуска программ из XML-файла

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, содержащий правила контроля запуска программ.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

## Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. В списке выберите правила, которые требуется удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

# Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 426) для задачи **Формирование правил контроля запуска программ**.
2. Настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите **Префикс для названий правил**.

       Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя защищаемого устройства, на котором установлена программа Kaspersky Embedded Systems Security для Windows. Вы можете изменить префикс для названий разрешающих правил.
     - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 442).
   - На закладке **Действия** укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security для Windows (см. раздел "Действия при автоматическом формировании правил" на стр. 442).
   - На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165).
   - На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после их изменения.

## В этом разделе

Ограничение области действия задачи ..... 442
Действия при автоматическом формировании правил ..... 442
Действия по завершении автоматического формирования правил ..... 445

## Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 426) для задачи **Формирование правил контроля запуска программ**.
2. Выберите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных программ**.

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на защищаемом устройстве имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок снят.

     Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.
   - **Создавать разрешающие правила для программ из папок**.

     В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

## Действия при автоматическом формировании правил

► *Чтобы настроить действия, которые программа Kaspersky Embedded Systems Security для Windows должна выполнять во время работы и по завершении задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 426) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:
   - **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Этот вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

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

  Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security для Windows разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

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

  Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

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

  По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

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

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

- **Использовать хеш SHA256**

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

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя или группы пользователей**.

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

  По умолчанию выбрана группа **Все**.

4. В блоке **По завершении задачи** настройте следующие параметры:

- **Добавлять разрешающие правила в список правил контроля запуска программ**.

  Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

  По умолчанию флажок установлен.

- **Принцип добавления**.

  Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом

устройстве в имя файла экспорта.

По умолчанию флажок установлен.

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

Настроенные параметры будут сохранены.

## Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security для Windows по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 426) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:
   - **Добавлять разрешающие правила в список правил контроля запуска программ**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

   - **Принцип добавления**.

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
     - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

     По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.
- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

  По умолчанию флажок установлен.

4. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

# Управление контролем запуска программ с помощью Веб-плагина

► *Чтобы настроить задачи контроля запуска программ с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 63. Параметры задачи Контроль запуска программ*

| Параметр | Описание |
|---|---|
| **Режим работы задачи**. | В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:<br>• **Активный**. Kaspersky Embedded Systems Security для Windows использует определенные правила контроля запуска всех программ.<br>• **Только статистика**. Kaspersky Embedded Systems Security для Windows не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.<br>По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**. |
| **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска** | Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет программу при каждой попытке ее запуска.<br>По умолчанию флажок снят. |

| Параметр | Описание |
| --- | --- |
| **Запрещать запуск командных интерпретаторов без команды к исполнению** | Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:<br>• Запуск командного интерпретатора разрешен.<br>• Исполняемая команда разрешена.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.<br>Kaspersky Embedded Systems Security для Windows работает со следующими командными интерпретаторами:<br>• cmd.exe;<br>• powershell.exe;<br>• python.exe;<br>• perl.exe.<br>По умолчанию флажок снят. |
| **Использовать правила для исполняемых файлов** | Флажок включает или выключает контроль запуска исполняемых файлов.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.<br>По умолчанию флажок установлен. |

| Параметр | Описание |
| --- | --- |
| **Контролировать загрузку DLL-модулей** | Флажок включает или выключает контроль загрузки DLL-модулей.<br><br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.<br><br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.<br><br>Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.<br><br>По умолчанию флажок установлен. |
| **Использовать правила для скриптов и пакетов MSI** | Флажок включает или выключает запуск скриптов и пакетов MSI.<br><br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения **Скрипты и пакеты MSI**.<br><br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.<br><br>По умолчанию флажок установлен. |
| **Запрещать запуск программ, недоверенных в KSN** | Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.<br><br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.<br><br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.<br><br>По умолчанию флажок снят. |

| Параметр | Описание |
| --- | --- |
| **Разрешать запуск программ, доверенных в KSN** | Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.<br>Если флажок установлен, Kaspersky Embedded Systems Security для Windows разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.<br>Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.<br>По умолчанию флажок снят. |
| **Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ** | Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, в этом поле можно указать пользователей и группы пользователей, которым разрешен запуск программ, доверенных в KSN.<br>По умолчанию указаны следующие пользователи: **Все** и **NT AUTHORITY\SYSTEM**. |
| **Правила** | Настройте разрешающие и запрещающие правила (см. раздел "Настройка правил контроля запуска программ в Kaspersky Security Center" на стр. 411) для задачи контроля запуска программ. |
| **Контроль пакетов установки** | Можно добавлять доверенные пакеты установки (см. раздел "Настройка Контроля пакетов установки" на стр. 406). |
| **Управление задачей** | Вы можете настроить расписание запуска задачи. |

kaspersky

# Контроль устройств

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

## В этом разделе


О задаче Контроль устройств ..... 451

О правилах контроля устройств ..... 453

О формировании правил контроля устройств ..... 455

О задаче Формирование правил контроля устройств ..... 457

Параметры по умолчанию для задачи Контроль устройств ..... 457

Управление контролем устройств с помощью Плагина управления ..... 458

Управление Контролем устройств с помощью Консоли программы ..... 471

Управление Контролем устройств с помощью Веб-плагина Консоли программы ..... 480


## О задаче Контроль устройств

Kaspersky Embedded Systems Security для Windows контролирует регистрацию и использование внешних устройств и CD/DVD-дисководов в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемыми флеш-накопителями или внешними устройствами другого типа.

Kaspersky Embedded Systems Security для Windows контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители, в том числе поддерживающие технологию UAS;
- устройства чтения CD/DVD-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые сетевые адаптеры;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Embedded Systems Security для Windows сообщает обо всех устройствах, подключенных по USB, с помощью соответствующего события в журнале событий и в журнале выполнения задачи. Описание события включает тип устройства и путь подключения. При запуске задачи Контроль устройств Kaspersky Embedded Systems Security для Windows проверяет и перечисляет все устройства, подключенные по USB. Уведомления можно настроить в блоке параметров уведомлений Kaspersky Security Center.

Задача Контроль устройств отслеживает попытки подключения внешних устройств к защищаемому устройству и блокирует их подключение, если не находит разрешающих правил для этих устройств. После блокировки соединения устройство становится недоступно.

Программа присваивает каждому подключаемому внешнему устройству один из следующих статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. При формировании списка правил значение *Путь к экземпляру устройства* подпадает под область применения хотя бы одного правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область применения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Формирование правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Embedded Systems Security для Windows идентифицирует регистрируемое в системе внешнее устройство по значению пути к экземпляру устройства. Путь к экземпляру устройства является уникальным признаком для каждого устройства. Информация о пути к экземпляру устройства содержится в свойствах внешнего устройства в операционной системе Windows и определяется Kaspersky Embedded Systems Security для Windows в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Embedded Systems Security для Windows контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

  Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до запуска задачи Контроль устройств в режиме **Активный**, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Embedded Systems Security для Windows не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

  Этот режим можно использовать для формирования правил на основе информации о блокировании устройств, зарегистрированной во время выполнения задачи (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 475).

# О правилах контроля устройств

Kaspersky Embedded Systems Security для Windows не использует разрешающие правила для MTP-подключаемых мобильных устройств.

Правила создаются индивидуально для каждого устройства, подключенного в данный момент или подключавшегося ранее к защищаемому устройству, если данные об этом устройстве сохранились в системе.

Для формирования разрешающих правил контроля устройств можно:

- Использовать задачу Формирование правил контроля устройств (см. раздел "О задаче Формирование правил контроля устройств" на стр. 457).
- Запустить задачу Контроль устройств в режиме Только статистика (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 475).
- Использовать данные системы о подключавшихся устройствах (см. раздел "Добавление разрешающего правила для одного или нескольких внешних устройств" на стр. 475).
- Расширить область применения уже созданных правил (см. раздел "Расширение области применения правил контроля устройств" на стр. 477).

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Embedded Systems Security для Windows, составляет 3072.

Правила контроля устройств описаны ниже.

**Тип правила**

Тип правила – всегда *разрешающее*. Задача Контроль устройств по умолчанию блокирует подключение всех флеш-накопителей и других внешних устройств, если они не подпадают под область действия ни одного разрешающего правила.

**Критерий срабатывания и область применения правила**

Правила контроля устройств идентифицируют подключаемые флеш-накопители и другие внешние устройства по значению параметра *Путь к экземпляру устройства*. Путь к экземпляру устройства является уникальным идентификатором, который система присваивает устройству в момент его подключения и регистрации в качестве внешнего устройства или устройства чтения CD/DVD-дисков (например, IDE или SCSI).

Kaspersky Embedded Systems Security для Windows контролирует подключение внешних устройств чтения CD/DVD дисков вне зависимости от шины подключения. При монтировании таких устройств по USB, операционная система регистрирует два значения пути к экземпляру устройства: для внешнего устройства и для устройства чтения CD/DVD-дисков (например, IDE или SCSI). Для корректного подключения таких устройств требуется наличие разрешающих правил для каждого значения пути к экземпляру устройства.

Kaspersky Embedded Systems Security для Windows автоматически определяет путь к экземпляру устройства и разбивает найденное значение на следующие составляющие:

- производитель устройства (VID);
- тип контроллера устройства (PID);
- серийный номер устройства.

Вы не можете задавать путь к экземпляру устройства вручную. Заданные в свойствах разрешающего правила критерии срабатывания правила определяют область применения этого правила. По умолчанию в область применения только что созданного разрешающего правила включено одно устройство, на основе свойств которого Kaspersky Embedded Systems Security для Windows сформировал разрешающее правило. Вы можете настраивать значения параметров созданного правила с помощью маски, чтобы расширить область применения правила (см. раздел "Расширение области применения правил контроля устройств" на стр. 477).

### Данные исходного устройства

Данные устройства, на основе которых программа Kaspersky Embedded Systems Security для Windows сформировала разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Путь к экземпляру устройства**. На основании этого свойства Kaspersky Embedded Systems Security для Windows определяет критерий срабатывания правила и заполняет следующие поля: **Производитель (VID)**, **Тип контроллера (PID)**, **Серийный номер** в блоке **Область применения правила** окна **Параметры правила**.
- **Адаптированное имя**. Имя, которое задается в свойствах устройства производителем.

При создании правила Kaspersky Embedded Systems Security для Windows автоматически определяет исходные значения для устройства. В дальнейшем вы можете использовать эти значения, чтобы определить, на основе данных какого устройства было создано правило. Данные исходного устройства недоступны для редактирования.

### Описание

Вы можете добавить дополнительную информацию для каждого созданного правила контроля устройств в поле **Пользователь или группа пользователей**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующем поле в окне **Правила контроля устройств**.

Комментарий и данные исходного устройства не учитываются при работе правила и служат только для упрощения идентификации устройств и правил пользователем.

# О формировании правил контроля устройств

Вы можете импортировать списки разрешающих правил контроля устройств из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль устройств или задачи Формирование правил контроля устройств.

По умолчанию Kaspersky Embedded Systems Security для Windows запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие заданных правил контроля устройств.

*Таблица 64. Цели и сценарии формирования правил контроля устройств*

| Сценарий формирования списка правил | Решаемая задача |
|---|---|
| Задача Формирование правил контроля устройств | • Создать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском задачи Контроль устройств.<br>• Нужно сформировать список правил для доверенных устройств в сети защищаемых устройств. |
| Создание правил на основе данных системы | Создать разрешающие правила для внешних устройств, данные о которых хранятся в системе. |
| Формирование правил по данным о подключенных в текущий момент устройствах | Обновление списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств. |
| Режим **Только статистика** задачи Контроль устройств | Добавить разрешающие правила для большого количества доверенных устройств. |

**Использование задачи Формирование правил контроля устройств**

XML-файл, сформированный по завершении задачи Формирование правил контроля устройств, содержит разрешающие правила для флеш-накопителей и других внешних устройств, данные о подключении которых сохранились в системе.

Используйте этот способ, чтобы учесть при формировании правил данные обо всех когда-либо подключавшихся внешних устройствах, сохранившиеся в системах на всех защищаемых устройствах сети, или данные только об устройствах, подключенных в настоящее время. Задача также учитывает все внешние устройства, подключенные в момент выполнения задачи. По завершении выполнения групповой задачи, Kaspersky Embedded Systems Security для Windows формирует списки разрешающих правил для всех зарегистрированных в сети внешних устройств и сохраняет эти списки в XML-файл в указанной папке. Далее вы можете вручную импортировать сформированные правила в свойства задачи Контроль устройств. В отличие от задачи на защищаемом устройстве, в политике невозможно настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи Формирование правил контроля устройств.

Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств, чтобы созданные разрешающие правила учитывали все внешние устройства, используемые на защищаемом устройстве.

### Использование данных системы обо всех подключаемых устройствах

В ходе выполнения задачи Kaspersky Embedded Systems Security для Windows получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому устройству в данный момент, и отображает обнаруженные устройства в списке в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Embedded Systems Security для Windows определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Можно сформировать разрешающие правила для любого внешнего устройства, данные о котором хранятся в системе, и сразу добавить новые правила в список правил контроля устройств.

При использовании этого сценария Kaspersky Embedded Systems Security для Windows формирует разрешающие правила для внешних устройств, подключавшихся ранее или подключенных в текущий момент к защищаемому устройству, на котором установлена программа Kaspersky Security Center.

Рекомендуется использовать этот сценарий для обновления списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств.

### Использование данных о подключенных в текущий момент устройствах

При использовании этого сценария Kaspersky Embedded Systems Security для Windows формирует разрешающие правила только для внешних устройств, подключенных в текущий момент. Вы можете выбрать одно или несколько внешних устройств, для которых вы хотите сформировать разрешающие правила.

### Использование задачи Контроль устройств в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль устройств в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Embedded Systems Security для Windows фиксирует информацию обо всех подключениях флеш-накопителей и других внешних устройств к защищаемому устройству в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** рекомендуется настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные подключения внешних устройств к защищаемому устройству.

Рекомендуется использовать этот сценарий для обновления существующего списка правил, если нужно разрешить использование большого количества новых внешних устройств.

Если формирование списка правил по этому сценарию выполняется на эталонной машине, вы можете применить сформированный список разрешающих правил при настройке задачи Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на защищаемых устройствах.

# О задаче Формирование правил контроля устройств

Задача Формирование правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других внешних устройств на основе данных системы обо всех внешних устройствах, которые ранее подключались к защищаемому устройству.

По завершении выполнения задачи Kaspersky Embedded Systems Security для Windows создает конфигурационный файл в формате XML со списком разрешающих правил для обнаруженных внешних устройств или сразу добавляет сформированные правила в задачу Контроль устройств в зависимости от параметров задачи Формирование правил контроля устройств. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются в окне **Правила контроля устройств**.

# Параметры по умолчанию для задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 65. Параметры по умолчанию для задачи Контроль устройств*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Режим работы**. | **Только статистика** | Задача фиксирует в журнале выполнения события запрета и разрешения подключения внешних устройств в соответствии с заданными правилами. Фактическая блокировка использования внешних устройств не выполняется.<br>Вы можете выбрать режим **Активный** для защиты устройства, чтобы применять фактическую блокировку использования внешних устройств. |
| **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется** | Не применяется | Kaspersky Embedded Systems Security для Windows запрещает использование внешних устройств вне зависимости от статуса выполнения задачи Контроль устройств. Это обеспечивает максимальную защиту от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.<br>Вы можете настраивать параметр таким образом, чтобы программа Kaspersky Embedded Systems Security для Windows разрешала использование всех внешних устройств, если задача Контроль устройств не выполняется. |
| Расписание запуска задачи | Время первого запуска не задано. | Задача Контроль устройств не запускается автоматически при запуске программы Kaspersky Embedded Systems Security для Windows.<br>Вы можете настроить запуск задачи по расписанию. |

*Таблица 66. Параметры задачи Формирование правил контроля устройств по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Режим генерации**. | **Учитывать данные системы обо всех когда-либо подключавшихся устройствах** | Режим работы задачи.<br>Можно выбрать режим **Учитывать данные только об устройствах, подключенных в текущий момент**. |
| Действия по завершении задачи | Разрешающие правила добавляются в список правил задачи Контроль устройств; новые правила объединяются с существующими правилами; дублирующие правила удаляются. | Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл. |
| Расписание запуска задачи | Время первого запуска не задано. | Задача Формирование правил контроля устройств не запускается автоматически сразу при запуске программы Kaspersky Embedded Systems Security для Windows. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |

# Управление контролем устройств с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и управление подключением внешних устройств ко всем защищаемым устройствам в сети с помощью списков правил в Kaspersky Security Center для групп защищаемых устройств.

## В этом разделе

Навигация ..... 459
Настройка задачи Контроль устройств ..... 461
Настройка задачи Формирование правил контроля устройств ..... 462
Настройка правил контроля устройств в Kaspersky Security Center ..... 463

kaspersky

# Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам политики для задачи Контроль устройств ..... 459

Переход к списку правил контроля устройств ..... 459

Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам ..... 460


## Переход к параметрам политики для задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.
7. Настройте политику в соответствии с вашими требованиями.

## Переход к списку правил контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

Откроется окно **Контроль устройств**.

7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.

8. Настройте политику в соответствии с вашими требованиями.

## Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам

► *Чтобы создать задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.

5. Выберите задачу **Формирование правил контроля устройств**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля устройств**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля устройств.

## Настройка задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Контроль устройств** (см. раздел "**Переход к параметрам политики для задачи Контроль устройств**" на стр. 459).
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Embedded Systems Security для Windows контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до запуска задачи Контроль устройств в режиме Активный, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**.

       Kaspersky Embedded Systems Security для Windows не контролирует подключение съемных дисков и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.
   - Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.

     Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется.

     Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security для Windows разрешает использовать любые внешние устройства на защищаемом устройстве.

     Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом устройстве в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

     По умолчанию флажок снят.
3. Нажмите на кнопку **Список правил**, чтобы изменить список правил контроля устройств (см. раздел "Настройка правил контроля устройств в Kaspersky Security Center" на стр. 463).

4. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**.
5. Нажмите на кнопку **OK** в окне **Контроль устройств**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

## Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля устройств** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам**" на стр. 460).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:
   - Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.
   - Настройте параметры для конфигурационных файлов со списком разрешающих правил, которые Kaspersky Embedded Systems Security для Windows создает по завершении задачи.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
6. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

kaspersky

# Настройка правил контроля устройств в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

## В этом разделе


Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center ..... 463

Формирование правил для подключенных устройств ..... 464

Формирование правил на основе реестра Kaspersky Security Center ..... 464

Просмотр свойств правил Контроля устройств ..... 464

Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах ..... 466

Создание правил с помощью задачи Формирование правил контроля устройств ..... 468

Добавление сформированных правил в список правил контроля устройств ..... 470


## Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила на основе данных системы** задачи Контроль устройств, выполните следующие действия:*

1. Если требуется, подключите к защищаемому устройству с установленной Консолью администрирования Kaspersky Security Center новое внешнее устройство, использование которого вы хотите разрешить.
2. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 459).
3. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.
4. Выберите устройство в списке устройств в окне **Сформировать правила на основе данных системы**.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.
6. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

## Формирование правил для подключенных устройств

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 459).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.
3. В списке обнаруженных устройств, которые подключены к защищаемому устройству, выберите устройства, для которых вы хотите сформировать разрешающие правила.
4. Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

## Формирование правил на основе реестра Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 459).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.
3. Нажмите на кнопку **Обновить список**, чтобы отобразился список доступных устройств, и выберите устройства, для которых требуется сформировать разрешающие правила. В поле **Поиск** можно также указать **Адаптированное имя**, чтобы отфильтровать устройства и упростить их выбор.
4. Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе реестра Kaspersky Security Center.

## Просмотр свойств правил Контроля устройств

Чтобы просмотреть свойства правил задачи **Контроль устройств**, выполните следующие действия:

1. Откройте окно **Контроль устройств**.
2. На закладке **Общие** нажмите на кнопку **Список правил** и дважды щелкните выбранное правило.

   Откроется окно **Свойства правила**.

*Таблица 67. Свойства правил Контроля устройств*

| Свойство | Описание |
|---|---|
| Применять правило | Этот параметр используется, чтобы включать и выключать применение правила. |
| Производитель (VID) | Вы можете указать полный VID производителя устройства или использовать символ * в качестве маски. Символ * используется для указания любого производителя.<br>Если в поле Производитель (VID) установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила. |
| Тип контроллера (PID) | Вы можете указать полный PID контроллера или использовать символ * в качестве маски. Символ * используется для указания любого типа контроллера.<br>Если в поле Тип контроллера (PID) установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила. |
| Серийный номер | Вы можете указать полный серийный номер устройства или использовать символы * или ? в качестве маски.<br>Символ * обозначает любую последовательность символов, включая пустую последовательность.<br>Символ ? обозначает один символ в последовательности.<br><br>Если в поле Серийный номер установлен флажок Использовать маску, данные в поле, в котором установлен этот флажок, заменяются символом * и не учитываются при применении правила.<br>Если вы выбрали вариант **Использовать маску**, но не ввели никаких символов в поле **Серийный номер**, после чего сохранили параметры и закрыли окно, программа применит * в качестве маски для поля **Серийный номер** и не будет учитывать его при применении правила. |
| Путь к экземпляру устройства | Идентификатор подключенного устройства.<br>Это свойство нельзя изменить. Поле предназначено только для справки. Это поле не используется программой для управления устройством. |

| Свойство | Описание |
|---|---|
| Адаптированное имя | Название устройства, заданное производителем. Это свойство нельзя изменить. Поле предназначено только для справки. Это поле не используется программой для управления устройством. |
| Пользователь или группа пользователей | Вы можете указать учетную запись пользователя или группу пользователей, у которых есть доступ к выбранным USB-устройствам, несколькими способами:<br>с помощью доменной службы Active Directory;<br>с помощью списка пользователей и групп пользователей Сервера администрирования;<br>добавлением вручную.<br>Операционная система отображает все подключенные USB-устройства. Вы можете получить доступ только к USB-устройствам, для которых у вас есть соответствующие права доступа. |
| Описание | Описание устройства, заданное по умолчанию. При необходимости укажите в поле Описание дополнительную информацию о правиле. Например, уточните, на какие устройства должно распространяться правило. |

## Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах

Можно импортировать данные о заблокированных попытках подключения устройств из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика** (см. раздел "**Настройка задачи Контроль устройств**" на стр. 461), и применить эти данные для формирования списка разрешающих правил контроля устройств в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль устройств, вы можете отследить, подключение каких устройств будет блокироваться.

► *Чтобы задать разрешающие правила подключения устройств для группы защищаемых устройств на основе отчета Kaspersky Security Center о заблокированных устройствах, выполните следующие действия:*

1. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что выполняются следующие условия:
   - Для событий с уровнем важности **Критическое событие** срок хранения событий *Обнаружено и запрещено недоверенное устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

- Для событий с уровнем важности **Предупреждение** срок хранения событий *Только статистика: обнаружено недоверенное устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

  По завершении периода хранения событий, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль устройств в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленное время хранения указанных событий.

2. Запустите задачу Контроль устройств в режиме **Только статистика**.

   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.

   b. Нажмите на кнопку **Создать выборку** и создайте выборку событий по критерию *Обнаружено и запрещено недоверенное устройство*. Просмотрите, подключения каких устройств заблокированы задачей Контроль устройств.

   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных подключениях в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех устройствах, подключение которых вы хотите разрешить.

3. Импортируйте данные о заблокированных попытках подключения устройств в задачу Контроль устройств.

   a. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 459).

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать правила из файла отчета KSC о заблокированных устройствах**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля устройств:

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

   a. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

   b. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

4. Нажмите на кнопку **OK** в окне **Контроль устройств**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

## Создание правил с помощью задачи Формирование правил контроля устройств

► *Чтобы задать разрешающие правила контроля устройств для группы защищаемых устройств с помощью задачи Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Настройка** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам" на стр. 460).
2. Настройте следующие параметры:
   - В блоке **Режим**:
     - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
     - **Учитывать данные только об устройствах, подключенных в текущий момент**
   - В блоке **После завершения задачи**:
     - **Добавлять разрешающие правила в список правил контроля устройств**.

       Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

       Если флажок снят, Kaspersky Embedded Systems Security для Windows не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

       По умолчанию флажок снят.
     - **Принцип добавления**.

       Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

       - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
       - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
       - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

       По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

  Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Embedded Systems Security для Windows экспортирует разрешающие правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

  По умолчанию флажок снят.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

  По умолчанию флажок установлен.

3. Нажмите на кнопку **Далее**.
4. В окне **Расписание** укажите параметры запуска задачи по расписанию.
5. Нажмите на кнопку **Далее**.
6. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
7. Нажмите на кнопку **Далее**.
8. Укажите название задачи.
9. Нажмите на кнопку **Далее**.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

   Откроется окно **Завершение создания задачи**.

10. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
11. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.
12. На закладке **Задачи** в рабочей области настраиваемой группы защищаемых устройств в списке групповых задач выберите созданную задачу Формирование правил контроля устройств.

13. Нажмите на кнопку **Запустить** для запуска задачи.

    По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в папке общего доступа в файлах формата XML.

    При применении политики контроля устройств в сети убедитесь, что для всех защищаемых устройств настроен доступ к общей сетевой папке. Если применение сетевой папки общего доступа не предусмотрено политикой организации, рекомендуется запускать задачу Формирование правил контроля устройств в тестовой группе защищаемых устройств или на эталонной машине организации.

## Добавление сформированных правил в список правил контроля устройств

► *Чтобы добавить сформированные списки разрешающих правил в задачу Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 459).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки **Добавить** выберите пункт **Импортировать правила из файла XML**.
4. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля устройств:
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
5. **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

   Все сформированные правила из XML-файла добавляются в список в соответствии с выбранным принципом.
7. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.
8. Если вы хотите применять созданные правила контроля устройств, в свойствах политики **Активный** выберите режим выполнения задачи **Контроль устройств**.

Разрешающие правила, автоматически сформированные на основе данных системы на каждом отдельном защищаемом устройстве, будут применены на всех защищаемых устройствах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых устройств программа будет разрешать подключение только тех устройств, для которых созданы разрешающие правила.

# Управление Контролем устройств с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе


Навигация ..... 471

Настройка параметров задачи Контроль устройств ..... 472

Настройка правил контроля устройств ..... 474

Настройка задачи Формирование правил контроля устройств ..... 478


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам задачи Контроль устройств ..... 471

Переход к окну с правилами контроля устройств ..... 472

Переход к параметрам задачи Формирование правил контроля устройств ..... 472


### Переход к параметрам задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

### Переход к окну с правилами контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. Настройте список правил в соответствии с вашими требованиями.

### Переход к параметрам задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

## Настройка параметров задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Контроль устройств**" на стр. 471).
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Embedded Systems Security для Windows контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до запуска задачи Контроль устройств в режиме Активный, это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика**.

  Kaspersky Embedded Systems Security для Windows не контролирует подключение съемных дисков и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

- Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.

  Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется.

  Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security для Windows разрешает использовать любые внешние устройства на защищаемом устройстве.

  Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом устройстве в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

  По умолчанию флажок снят.

3. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания задач" на стр. 165).
4. Чтобы изменить список правил контроля устройств (см. раздел "О формировании правил контроля устройств" на стр. 455), перейдите по ссылке **Правила контроля устройств** в нижней части панели результатов узла **Контроль устройств**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

kaspersky

# Настройка правил контроля устройств

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

## В этом разделе


Импорт правил контроля устройств из файла формата XML ..... 474

Формирование списка правил по событиям задачи Контроль устройств ..... 475

Добавление разрешающего правила для одного или нескольких внешних устройств ..... 475

Удаление правил контроля устройств ..... 476

Экспорт правил контроля устройств ..... 476

Активация и выключение правила контроля устройств ..... 477

Расширение области применения правил контроля устройств ..... 477


## Импорт правил контроля устройств из файла формата XML

► *Чтобы импортировать правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла XML**:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, который содержит параметры правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля устройств**.

## Формирование списка правил по событиям задачи Контроль устройств

► *Чтобы создать конфигурационный файл со списком правил контроля устройств, сформированным по событиям задачи Контроль устройств, выполните следующие действия:*

1. Запустите задачу Контроль устройств в режиме **Только статистика** (см. раздел "**Настройка параметров задачи Контроль устройств**" на стр. 472), чтобы зафиксировать в журнале выполнения задачи все события подключения флеш-накопителей и других внешних устройств к защищаемому устройству.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в разделе **Управление** в панели результатов узла **Контроль устройств**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security для Windows создаст конфигурационный файл в формате XML со списком правил на основе событий, зарегистрированных при работе задачи Контроль устройств в режиме **Только статистика**. Можно применить этот список в задаче Контроль устройств (см. раздел "Импорт правил контроля устройств из файла формата XML" на стр. 474).

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что подключение недоверенных устройств не разрешено заданными правилами.

При конвертации XML-файла с событиями выполнения задачи в список правил контроля устройств, программа создает разрешающие правила для всех зафиксированных событий, в том числе для событий блокирования устройств.

Все события, возникшие в ходе выполнения задачи, фиксируются в журнале выполнения задачи, независимо от режима. Вы можете создать конфигурационный файл со списком правил по результатам выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется сформировать финальную версию списка правил до запуска задачи в активном режиме.

## Добавление разрешающего правила для одного или нескольких внешних устройств

В задаче контроля устройств не предусмотрена функция добавления одного правила вручную. Однако в случае, если вам необходимо добавить правила для новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка разрешающих правил программа использует данные Windows обо всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает подключенные в текущий момент устройства.

► *Чтобы добавить разрешающее правило для внешних устройств, подключенных в данный момент, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню выберите пункт **Сформировать правила на основе данных системы**.
4. В открывшемся окне в списке обнаруженных устройств выберите устройство или несколько устройств, использование которых вы хотите разрешить на защищаемом устройстве.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

## Удаление правил контроля устройств

► *Чтобы удалить правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля устройств будут удалены.

## Экспорт правил контроля устройств

► *Чтобы экспортировать правила контроля устройств в конфигурационный файл, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
4. Нажмите на кнопку **Сохранить**.

Правила и их параметры будут экспортированы в указанный файл.

## Активация и выключение правила контроля устройств

Вы можете включать и выключать применение созданных разрешающих правил контроля устройств, не удаляя их.

► *Чтобы включить или выключить созданное правило контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
3. В открывшемся окне снимите или установите флажок **Применять правило**.

   Флажок включает или выключает применение конкретного правила контроля устройств.

   Если флажок установлен в параметрах правила, такое правило будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет разрешено.

   Если флажок снят в параметрах правила, такое правило не будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет запрещено.

   По умолчанию флажок установлен в параметрах каждого созданного правила.
4. Нажмите на кнопку **OK**.

Статус применения правила будет сохранен и отобразится для указанного правила.

## Расширение области применения правил контроля устройств

Каждое автоматически созданное правило контроля устройств разрешает подключение только одного внешнего устройства. Вы можете вручную расширить область применения правила, применив маску пути к экземпляру устройства в свойствах любого заданного правила контроля устройств.

Применение маски пути к экземпляру устройства уменьшает количество разрешающих правил контроля устройств и упрощает процесс их обработки вручную. Однако расширение области применения правил может снижать эффективность контроля внешних устройств.

► *Чтобы применить маску пути к экземпляру устройства в свойствах правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 472).
2. В открывшемся окне выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
3. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.

4. В открывшемся окне выполните следующие действия:
   - Установите флажок **Использовать маску** рядом с полем **Производитель (VID)**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанным производителем устройства.
   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанным типом контроллера.
   - Установите флажок **Использовать маску** рядом с полем **Серийный номер**, чтобы выбранное правило разрешало подключение всех внешних устройств с указанными данными о серийном номере устройства.

   Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых установлен этот флажок, заменяются символом * и не учитываются при применении правила.
5. Укажите учетную запись пользователя или группу пользователей, у которых есть доступ к выбранным USB-устройствам. Операционная система отображает все подключенные USB-устройства. Вы можете получить доступ только к USB-устройствам, к которым у вас есть соответствующие права доступа.
6. Если требуется, введите дополнительную информацию о правиле в поле **Пользователь или группа пользователей**. Например, уточните, на какие устройства должно распространяться правило.
7. Нажмите на кнопку **OK**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

## Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Формирование правил контроля устройств**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Режим генерации** выберите режим работы задачи:
   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
   - **Учитывать данные только об устройствах, подключенных в текущий момент**

5. В разделе **По завершении задачи** укажите действия, которые программа Kaspersky Embedded Systems Security для Windows должна выполнять по завершении задачи:

   - **Добавлять разрешающие правила в список правил контроля устройств**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

     По умолчанию флажок снят.

   - **Принцип добавления**.

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля устройств.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируются.
     - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
     - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

     По умолчанию выбран способ **Объединять с существующими правилами**.

   - **Экспортировать разрешающие правила в файл**.

     Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

     Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Embedded Systems Security для Windows экспортирует разрешающие правила в файл, указанный в поле ниже.

     Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

     По умолчанию флажок снят.

- **Добавлять информацию о защищаемом устройстве в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом устройстве в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого устройства, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом устройстве в имя файла экспорта.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165).
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

# Управление Контролем устройств с помощью Веб-плагина Консоли программы

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров задачи на защищаемом устройстве.

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 68. Параметры задачи Контроль устройств*

| Параметр | Описание |
|---|---|
| **Активный** | Kaspersky Embedded Systems Security для Windows контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию. |
| **Только статистика** | Kaspersky Embedded Systems Security для Windows не контролирует подключение съемных дисков и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию. |
| **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется** | Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется.<br>Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security для Windows разрешает использовать любые внешние устройства на защищаемом устройстве.<br>Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом устройстве в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.<br>По умолчанию флажок снят. |
| **Правила контроля устройств** | Можно настраивать список правил контроля устройств (см. раздел "Настройка правил контроля устройств в Kaspersky Security Center" на стр. 463). |
| Управление задачами | Вы можете настроить расписание запуска задачи. |

# Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

## В этом разделе


О задаче Управление сетевым экраном ..... 482

О правилах сетевого экрана ..... 484

Параметры по умолчанию для задачи Управление сетевым экраном ..... 485

Настройка задачи Управление сетевым экраном с помощью Плагина управления ..... 486

Настройка задачи Управление сетевым экраном с помощью Консоли программы ..... 493

Настройка задачи Управление сетевым экраном с помощью Веб-плагина ..... 499


# О задаче Управление сетевым экраном

Если при установке Kaspersky Embedded Systems Security для Windows брандмауэр Windows выключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы брандмауэр Windows включен, задача Управление сетевым экраном выполняется по завершении установки.

Запуск задачи Управление сетевым экраном невозможен, если брандмауэр Windows находится под управлением групповой политики Kaspersky Security Center.

Задача Управление сетевым экраном не фильтрует сетевой трафик самостоятельно, но предоставляет возможность управления брандмауэром Windows с помощью графического интерфейса Kaspersky Embedded Systems Security для Windows.

Задача регулярно опрашивает брандмауэр Windows. По умолчанию интервал опроса составляет одну минуту и не может быть изменен.

В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security для Windows выполняет действия, определенные режимом взаимодействия с брандмауэром Windows:

- **Отслеживать статус работы брандмауэра Windows**. Программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.
- **Контролировать работу брандмауэра Windows**. Программа контролирует работу брандмауэра Windows в объеме, определенном следующими функциями:
    - **Поддерживать статус работы брандмауэра Windows**;

Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью раскрывающегося списка **Включен/Выключен** состоянии.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает состояние брандмауэра Windows.
- Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
- Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

По умолчанию функция включена и выбрано состояние **Включено**.

- **Управлять параметрами и правилами брандмауэра Windows**.

Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
- Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
- Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

  Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
- Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

# О правилах сетевого экрана

Задача Управление сетевым экраном через брандмауэр Windows фильтрует сетевой трафик с помощью правил сетевого экрана, если установлен режим взаимодействия с брандмауэром Windows **Контролировать работу брандмауэра Windows**.

Правила сетевого экрана для приложений контролируют сетевые соединения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу приложения.

Правила сетевого экрана для портов контролируют сетевые соединения для указанных портов и протоколов (TCP/UDP). Критериями срабатывания таких правил являются порт или диапазон портов и тип протокола.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая сетевые соединения с помощью правил для портов, вы снижаете уровень безопасности защищаемого устройства.

Вы можете управлять правилами сетевого экрана:

- создавать и удалять правила сетевого экрана;
- изменять параметры правил сетевого экрана;
- включать и выключать правила сетевого экрана.

**Создаваемые по умолчанию правила сетевого экрана**

При установке Kaspersky Embedded Systems Security для Windows создает набор разрешающих правил, предотвращающих блокировку программ, устанавливаемых вместе с Kaspersky Embedded Systems Security для Windows. Ниже приведена подробная информация и описаны ограничения.

При установке на устройство с любой поддерживаемой версией Windows Kaspersky Embedded Systems Security для Windows создает набор правил для входящих сетевых соединений:

- Разрешающие правила для Консоли Kaspersky Embedded Systems Security для Windows (kavfsgt.exe), расположенной в папке установки программы. Статус: включено. Область применения правил: все адреса. Протоколы: TCP и UDP, по одному правилу на протокол.
- Два разрешающих правила для локального порта 15000, если на устройстве установлен Агент администрирования Kaspersky Security Center. Состояние: включено. Область применения правил: все адреса. Протоколы: TCP и UDP, по одному правилу на протокол.

При установке на устройство с Windows 7 и выше Kaspersky Embedded Systems Security для Windows создает набор правил для исходящих сетевых соединений:

- Разрешающие правила для Консоли Kaspersky Embedded Systems Security для Windows (kavfsgt.exe), расположенной в папке установки программы. Статус: включено. Область применения правил: все адреса. Протоколы: TCP и UDP, по одному правилу на протокол.
- Разрешающие правила для Kaspersky Embedded Systems Security для Windows (kavfswp.exe), расположенной в папке установки программы. Состояние: включено. Область применения правил: все адреса. Протоколы: TCP и UDP, по одному правилу на протокол.
- Два разрешающих правила для локального порта 13000, если на устройстве установлен Агент администрирования Kaspersky Security Center. Состояние: включено. Область применения правил: все адреса. Протоколы: TCP и UDP, по одному правилу на протокол.

При удалении Kaspersky Embedded Systems Security для Windows программа удаляет все созданные правила сетевого экрана, кроме правил, созданных агентом администрирования Kaspersky Security Center, таких как Kaspersky Security Center WDS и Kaspersky Administration Kit. Также программа удаляет правила для ICMPv4 и ICMPv6 для Windows 7 и более поздних версий.

При удалении Kaspersky Embedded Systems Security для Windows программа разрешает все ICMP-соединения для операционных систем более ранних версий, чем Windows 7.

# Параметры по умолчанию для задачи Управление сетевым экраном

По умолчанию в задаче Управление сетевым экраном используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 69. Параметры по умолчанию для задачи Управление сетевым экраном*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Режим взаимодействия Kaspersky Embedded Systems Security для Windows с брандмауэром Windows | **Отслеживать статус работы брандмауэра Windows** | Программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center уведомление, если брандмауэр Windows выключен. |
| **Входящие соединения** | **Блокировать** | Вы можете создавать и настраивать правила сетевого экрана для входящих соединений, чтобы блокировать или разрешать входящие соединения. |
| **Исходящие соединения** | **Разрешать** | Вы можете создавать и настраивать правила сетевого экрана для исходящих соединений, чтобы блокировать или разрешать исходящие соединения. |
| **Разрешить ICMP-соединения** | **Выключено** | Параметр разрешает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений. |
| Расписание запуска задачи | Недоступно | Задача Управление сетевым экраном не запускается автоматически при запуске Kaspersky Embedded Systems Security для Windows.<br>Вы можете настроить запуск задачи по расписанию. |

# Настройка задачи Управление сетевым экраном с помощью Плагина управления

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью Плагина управления.

## В этом разделе


Настройка общих параметров задачи Управление сетевым экраном ..... 486

Создание и настройка правил сетевого экрана ..... 489

Включение и выключение правил сетевого экрана ..... 491

Удаление правил сетевого экрана ..... 492


## Настройка общих параметров задачи Управление сетевым экраном

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Контроль активности в сети** в блоке **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
5. На вкладке **Общие** в блоке **Интеграция с брандмауэром Windows** выберите режим взаимодействия Kaspersky Embedded Systems Security для Windows с брандмауэром Windows:
   - **Отслеживать статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого устройства.

- **Контролировать работу брандмауэра Windows**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:
  - **Поддерживать статус работы брандмауэра Windows**;

    Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью раскрывающегося списка **Включен/Выключен** состоянии.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает состояние брандмауэра Windows.
    - Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
    - Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

    Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

    По умолчанию функция включена и выбрано состояние **Включено**.

  - **Управлять параметрами и правилами брандмауэра Windows**;

    Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
    - Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
    - Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

      Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
    - Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

    Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

- **Разрешить ICMP-соединения**.

  Функция разрешает или запрещает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

  Если функция включена, брандмауэр Windows разрешает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.

В операционных системах версии ниже Windows 7 брандмауэр Windows разрешает только входящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

По умолчанию функция выключена.

6. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 489).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
7. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.
   - При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 489).

     Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.
8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

## Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Контроль активности в сети** в блоке **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
5. На вкладке **Общие** в блоке **Входящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. Создайте и настройте правила сетевого экрана для входящих соединений.
7. На вкладке **Приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для приложения**.
8. Настройте параметры правила:
   a. В поле **Имя правила** введите название правила.

   > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для входящих сетевых соединений.

   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
      - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для приложения.

   c. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

d. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

e. Нажмите на кнопку **OK**, чтобы сохранить правило.

9. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для портов**.

10. Настройте параметры правила:

    a. В поле **Имя правила** введите название правила.

    b. В раскрывающемся списке **Действие правила** выберите один из вариантов:

    - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для портов.
    - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для портов.

    c. В блоке **Локальные порты** укажите порт или диапазон портов.

    Для входящих сетевых соединений укажите порт или диапазон портов для локального устройства.

    Для исходящих сетевых соединений укажите порт или диапазон портов для удаленных устройств.

    Для номера порта доступны значения 1–65535.

    Для диапазона номеров портов доступны значения 1–10, 20–30000 и 1–65535.

> Windows XP не поддерживает диапазон портов. Поэтому для устройств из области применения правила, работающих по управлением Windows XP, программа применяет правило только к первому порту указанного диапазона.

d. Выберите тип протокола (TCP/UDP), для которого программа контролирует входящие сетевые соединения.

e. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

f. Нажмите на кнопку **OK**, чтобы сохранить правило.

11. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.

12. На вкладке **Общие** в блоке **Исходящие соединения** нажмите на кнопку **Список правил**.

    Откроется окно **Правила сетевого экрана для исходящих соединений**.

13. Создайте и настройте правила сетевого экрана для исходящих соединений.
14. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

## Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. В зависимости от типа правила, статус которого вы хотите изменить, перейдите по ссылке **Входящее** или **Исходящее**, а затем выберите закладку **Приложения** или **Порты**.
7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.
8. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.
9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
10. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

# Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
7. В списке правил выберите правило, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
9. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.
10. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
11. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

# Настройка задачи Управление сетевым экраном с помощью Консоли программы

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью интерфейса Консоли программы.

## В этом разделе


Настройка общих параметров задачи Управление сетевым экраном ..... 493

Создание и настройка правил сетевого экрана ..... 496

Включение и выключение правил сетевого экрана ..... 497

Удаление правил сетевого экрана ..... 498


## Настройка общих параметров задачи Управление сетевым экраном

Некоторые параметры правил сетевого экрана для входящих и исходящих соединений могут быть недоступны, если Консоль программы подключена к локальному хосту (на котором запущена) и параметры не поддерживаются операционной системой хоста.

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Параметры**.

   Откроется окно **Параметры задачи**.
4. На вкладке **Общие** в блоке **Фильтрация сетевого трафика** выберите вариант взаимодействия Kaspersky Embedded Systems Security для Windows с брандмауэром Windows:
   - **Отслеживать статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого устройства.

- **Контролировать работу брандмауэра Windows**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:
  - **Поддерживать статус работы брандмауэра**;

    Функция включает или выключает поддержание брандмауэра Windows в указанном с помощью раскрывающегося списка **Включен/Выключен** состоянии.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает состояние брандмауэра Windows.
    - Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
    - Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

    Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

    По умолчанию функция включена и выбрано состояние **Включено**.

  - **Управлять параметрами и правилами брандмауэра Windows**;

    Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

    Если функция включена, программа выполняет следующие действия:

    - Опрашивает брандмауэр Windows с интервалом в одну минуту.
    - Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
    - Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
    - Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

      Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
    - Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

    Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

По умолчанию функция включена.

- **Разрешить ICMP-соединения**.

  Функция разрешает или запрещает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

  Если функция включена, брандмауэр Windows разрешает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.

В операционных системах версии ниже Windows 7 брандмауэр Windows разрешает только входящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

По умолчанию функция выключена.

5. В блоке **Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже** настройте следующие параметры:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 496).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.
   - При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 496).

     Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

## Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Входящие**.

   Откроется окно **Правила сетевого экрана для входящих соединений**.
4. Создайте и настройте правила сетевого экрана для входящих соединений.
5. На вкладке **Приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для приложения**.
6. Настройте параметры правила:
   a. В поле **Имя правила** введите название правила.

   > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для входящих сетевых соединений.

   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
      - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для приложения.

   c. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

   d. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

   > Для IP-адресов поддерживается только формат IPv4.

   e. Нажмите на кнопку **ОК**, чтобы сохранить правило.
7. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило сетевого экрана для портов**.
8. Настройте параметры правила:
   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие правила** выберите один из вариантов:
      - **Разрешать**. Если выбран этот вариант, программа разрешает входящие сетевые соединения для портов.
      - **Блокировать**. Если выбран этот вариант, программа блокирует входящие сетевые соединения для портов.

c. В блоке **Локальные порты** укажите порт или диапазон портов.

Для входящих сетевых соединений укажите порт или диапазон портов для локального устройства.

Для исходящих сетевых соединений укажите порт или диапазон портов для удаленных устройств.

Для номера порта доступны значения 1–65535.

Для диапазона номеров портов доступны значения 1–10, 20–30000 и 1–65535.

Windows XP не поддерживает диапазон портов. Поэтому для устройств из области применения правила, работающих по управлением Windows XP, программа применяет правило только к первому порту указанного диапазона.

d. Выберите тип протокола (TCP/UDP), для которого программа контролирует входящие сетевые соединения.

e. В поле **Действие правила** укажите сетевые адреса. Программа контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

Для IP-адресов поддерживается только формат IPv4.

f. Нажмите на кнопку **OK**, чтобы сохранить правило.

9. В окне **Правила сетевого экрана для входящих соединений** нажмите на кнопку **OK**.
10. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Исходящие соединения**.

    Откроется окно **Правила сетевого экрана для исходящих соединений**.
11. Создайте и настройте правила сетевого экрана для исходящих соединений.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров задачи сохранится в журнале системного аудита.

## Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, статус которого вы хотите изменить, перейдите по ссылке **Входящее** или **Исходящее**, а затем выберите закладку **Приложения** или **Порты**.

5. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.
6. В окне **Сохранить** нажмите на кнопку **Правила сетевого экрана**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

## Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
5. В списке правил выберите правило, которое вы хотите удалить.
6. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
7. В окне **Сохранить** нажмите на кнопку **Правила сетевого экрана**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

# Настройка задачи Управление сетевым экраном с помощью Веб-плагина

В этом разделе приведены инструкции по настройке общих параметров задачи Управление сетевым экраном и созданию и настройке правил сетевого экрана с помощью Веб-плагина.

## В этом разделе


Настройка общих параметров задачи Управление сетевым экраном ..... 499

Создание и настройка правил сетевого экрана ..... 502

Включение и выключение правил сетевого экрана ..... 503

Удаление правил сетевого экрана ..... 503


## Настройка общих параметров задачи Управление сетевым экраном

► *Чтобы настроить общие параметры задачи Управление сетевым экраном с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. В разделе **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
6. На вкладке **Общие** в блоке **Интеграция с брандмауэром Windows** выберите вариант взаимодействия Kaspersky Embedded Systems Security для Windows с брандмауэром Windows:
   - **Отслеживать статус работы брандмауэра Windows Программа только отслеживает статус работы брандмауэра Windows**. Если выбран этот вариант, программа только отслеживает статус работы брандмауэра Windows и отправляет в Kaspersky Security Center событие-предупреждение, если брандмауэр Windows не запущен.

     Если этот вариант выбран на смену варианта **Контролировать работу брандмауэра Windows Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже**, программа восстанавливает внутренние параметры брандмауэра Windows при следующей загрузке операционной системы защищаемого устройства.
   - **Контролировать работу брандмауэра Windows Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже**. Если выбран этот вариант, программа контролирует работу брандмауэра Windows в объеме, определенном следующими параметрами:
     - **Поддерживать статус работы брандмауэра Windows**;

       Функция включает или выключает поддержание брандмауэра Windows в указанном с

помощью раскрывающегося списка **Включен/Выключен** состоянии.

Если функция включена, программа выполняет следующие действия:

- Опрашивает брандмауэр Windows с интервалом в одну минуту.
- Считывает состояние брандмауэра Windows.
- Включает брандмауэр Windows в случае его выключения, если выбрано состояние **Включено**.
- Выключает брандмауэр Windows в случае его включения, если выбрано состояние **Выключено**.

Функцию нельзя выключить, если выключена функция **Управлять параметрами и правилами брандмауэра Windows**.

По умолчанию функция включена и выбрано состояние **Включено**.

- **Управлять параметрами и правилами брандмауэра Windows**;

  Функция включает или выключает управление параметрами и правилами брандмауэра Windows.

  Если функция включена, программа выполняет следующие действия:

  - Опрашивает брандмауэр Windows с интервалом в одну минуту.
  - Считывает и копирует параметры брандмауэра Windows, включая правила сетевого экрана.
  - Устанавливает значения параметров брандмауэра Windows в соответствии со значениями параметров задачи Управление сетевым экраном.
  - Создает список правил сетевого экрана Kaspersky Security Group в оснастке брандмауэра Windows. Этот набор содержит все правила сетевого экрана задачи Управление сетевым экраном.

    Далее при опросах брандмауэра Windows программа не синхронизирует список правил сетевого экрана Kaspersky Security Group со списком правил задачи Управление сетевым экраном. Для синхронизации списков правил сетевого экрана необходимо перезапустить задачу Управление сетевым экраном.
  - Ограничивает возможность изменять параметры и правила брандмауэра Windows сторонними средствами или непосредственно в оснастке (wf.msc). Если параметры или правила брандмауэра Windows изменены, в течение минуты программа откатывает изменения до значений параметров, заданных с помощью задачи Управление сетевым экраном.

  Если функция выключена, программа восстанавливает параметры и правила брандмауэра Windows до значений, которые программа сохранила после первого опроса брандмауэра Windows, и более не управляет параметрами и правилами брандмауэра Windows.

  Функцию нельзя выключить, если выключена функция **Поддерживать статус работы брандмауэра Windows**.

  По умолчанию функция включена.

- **Разрешить ICMP-соединения**.

  Функция разрешает или запрещает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

  Если функция включена, брандмауэр Windows разрешает входящие и исходящие сетевые соединения по протоколам ICMPv4 и ICMPv6, независимо от параметров задачи для входящих и исходящих соединений.

В операционных системах версии ниже Windows 7 брандмауэр Windows разрешает только входящие сетевые соединения по протоколам ICMPv4 и ICMPv6.

По умолчанию функция выключена.

7. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет брандмауэр Windows для всех входящих сетевых соединений, если иное не определено в правилах сетевого экрана для входящих соединений.
   - При необходимости добавьте правила сетевого экрана для входящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 502).

     Правила сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то брандмауэр Windows разрешает входящие сетевые соединения, подпадающие под критерии правила.
8. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:
   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет брандмауэр Windows для всех исходящих сетевых соединений, если иное не определено в правилах сетевого экрана для исходящих соединений.
   - При необходимости добавьте правила сетевого экрана для исходящих соединений (см. раздел "Создание и настройка правил сетевого экрана" на стр. 502).

     Правила сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то брандмауэр Windows блокирует исходящие сетевые соединения, подпадающие под критерии правила.
9. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

*Таблица 70.*

| Параметр | Описание |
|---|---|
| **Правила сетевого экрана для приложений** | Вы можете управлять правилами для программ.<br>Правила этого типа выборочно разрешают сетевые подключения для указанных программ. Критерием срабатывания таких правил является путь к исполняемому файлу. |
| **Правила сетевого экрана для портов** | Вы можете управлять правилами для портов.<br>Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола. |
| **Управление задачей** | Вы можете настроить расписание запуска задачи. |

## Создание и настройка правил сетевого экрана

► *Чтобы создать и настроить правила сетевого экрана с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. В блоке **Управление сетевым экраном** нажмите на кнопку **Настройка**.

   Откроется окно **Управление сетевым экраном**.
6. Создайте и настройте правило сетевого экрана для входящих соединений для приложения.
7. Создайте и настройте правило сетевого экрана для входящих соединений для портов.
8. Создайте и настройте правило сетевого экрана для исходящих соединений для приложения.
9. Создайте и настройте правило сетевого экрана для исходящих соединений для портов.
10. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

## Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Правила сетевого экрана для приложений** или **Правила сетевого экрана для портов**.
7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, включите переключатель слева от имени правила.
   - Если вы хотите, чтобы активное правило не применялось, выключите переключатель слева от имени правила.
8. Нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

## Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Правила сетевого экрана для приложений** или **Правила сетевого экрана для портов**.
7. В списке правил выберите правило, которое вы хотите удалить.

8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.

9. Нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

kaspersky

# Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Мониторинг файловых операций.

## В этом разделе


О задаче Мониторинг файловых операций ..... 505

О правилах мониторинга файловых операций ..... 506

Параметры по умолчанию для задачи Мониторинг файловых операций ..... 509

Управление мониторингом файловых операций с помощью Плагина управления ..... 510

Управление мониторингом файловых операций с помощью Консоли программы ..... 516

Управление мониторингом файловых операций с помощью Веб-плагина ..... 520


## 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 устройстве. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

*Обрыв мониторинга* – это период, когда область мониторинга временно выпадает из поля действия задачи, например, из-за приостановки выполнения задачи или из-за физического отсутствия внешнего устройства на защищаемом устройстве. Kaspersky Embedded Systems Security для Windows сообщит об обнаружении файловых операций в области мониторинга, как только внешнее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

**Требования к среде**

Для запуска задачи Мониторинг файловых операций должны быть соблюдены следующие условия:

- На защищаемом устройстве должна использоваться файловая система ReFS или NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN-журнала компонент получает данные о файловых операциях.

  Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинг файловых операций, вам нужно перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

**Исключения для области мониторинга**

Вы можете создать исключения из области мониторинга (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 536). Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижнеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

# О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания правила и регулировать уровень важности событий для обнаруженных файловых операций, регистрируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- Доверенные пользователи
- Маркеры файловых операций

**Доверенные пользователи**

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Статус *Недоверенный пользователь* присваивается всем пользователям, не указанным в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Embedded Systems Security для Windows обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи.

Статус *Доверенный пользователь* присваивается пользователю или группе пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Embedded Systems Security для Windows обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Информационное событие в журнале выполнения задачи.

Kaspersky Embedded Systems Security для Windows не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Статус *Неизвестный пользователь* присваивается пользователю в случае, когда Kaspersky Embedded Systems Security для Windows не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа зарегистрирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Embedded Systems Security для Windows учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см. таблицу ниже).

*Таблица 71. Маркеры файловых операций*

| ID файловой операции | Маркер файловой операции | Поддерживаемые файловые системы |
|---|---|---|
| BASIC_INFO_CHANGE | изменены атрибуты или метки времени файла или папки | NTFS, ReFS |
| COMPRESSION_CHANGE | изменено сжатие файла или папки | NTFS, ReFS |
| DATA_EXTEND | размер файла или папки увеличен | NTFS, ReFS |
| DATA_OVERWRITE | перезаписаны данные в файле или папке | NTFS, ReFS |
| DATA_TRUNCATION | файл или папка усечены | NTFS, ReFS |
| EA_CHANGE | изменены расширенные атрибуты файла или папки | только NTFS |
| ENCRYPTION_CHANGE | изменен статус шифрования файла или папки | NTFS, ReFS |
| FILE_CREATE | файл или папка созданы впервые | NTFS, ReFS |

| ID файловой операции | Маркер файловой операции | Поддерживаемые файловые системы |
|---|---|---|
| FILE_DELETE | Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL | NTFS, ReFS |
| HARD_LINK_CHANGE | жесткая связь создана или удалена для файла или папки | только NTFS |
| INDEXABLE_CHANGE | изменен статус индексирования файла или папки | NTFS, ReFS |
| INTEGRITY_CHANGE | изменен атрибут целостности для именованного файлового потока | только ReFS |
| NAMED_DATA_EXTEND | размер именованного файлового потока увеличен | NTFS, ReFS |
| NAMED_DATA_OVERWRITE | именованный файловый поток перезаписан | NTFS, ReFS |
| NAMED_DATA_TRUNCATION | именованный файловый поток усечен | NTFS, ReFS |
| OBJECT_ID_CHANGE | изменен идентификатор файла или папки | NTFS, ReFS |
| RENAME_NEW_NAME | присвоено новое имя для файла или папки | NTFS, ReFS |
| REPARSE_POINT_CHANGE | создана новая или изменена существующая точка повторного анализа для файла или папки | NTFS, ReFS |
| SECURITY_CHANGE | изменены права доступа к файлу или папке | NTFS, ReFS |
| STREAM_CHANGE | создан новый или изменен существующий именованный файловый поток | NTFS, ReFS |
| TRANSACTED_CHANGE | именованный файловый поток изменен транзакцией TxF | только ReFS |

# Параметры по умолчанию для задачи Мониторинг файловых операций

По умолчанию в задаче Мониторинг файловых операций используются параметры, описанные в таблице ниже. Вы можете изменять значения параметров с помощью:

- Плагина управления (см. раздел "Управление мониторингом файловых операций с помощью Плагина управления" на стр. 510)
- Консоли программы
- Веб-плагина (см. раздел "Управление мониторингом файловых операций с помощью Веб-плагина" на стр. 520)

*Таблица 72. Параметры по умолчанию для задачи Мониторинг файловых операций*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Область мониторинга** | Не задано | Этот параметр используется, чтобы задавать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга. |
| Список **Доверенные пользователи** | Не задано | Этот параметр используется, чтобы задавать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные. |
| **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга** | Применяется | Этот параметр используется для включения или выключения записи в журнал файловых операций, выполненных в указанных областях мониторинга в периоды простоя задачи.<br><br>По умолчанию собирается статистика для недоверенных и неизвестных пользователей и объектов. |
| **Блокировать попытки компрометации журнала USN** | Применяется | Этот параметр используется, чтобы включать и выключать защиту USN-журнала. |
| **Обнаруживать и блокировать все файловые операции в выбранной области** | Выключено | Установите или снимите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**, чтобы блокировать все изменения для выбранной области мониторинга. |
| **Исключить следующие папки из области контроля** | Не применяется | Этот параметр используется, чтобы контролировать применение исключений для папок, в которых не требуется контролировать за файловые операции. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security для Windows пропускает области мониторинга, заданные в качестве исключений. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Контрольная сумма** | Не применяется | Этот параметр используется, чтобы настроить расчет контрольной суммы файла после внесения изменений. |
| **Маркеры файловых операций** | Учитываются все доступные маркеры файловых операций | Этот параметр используется, чтобы указать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security для Windows формирует событие аудита. |
| Расписание запуска задачи | Время первого запуска не задано. | Вы можете настроить расписание запуска задачи. |

# Управление мониторингом файловых операций с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Плагина управления.

## В этом разделе


Настройка парметров задачи Мониторинг файловых операций ..... 510

Создание и настройка правила мониторинга файловых операций ..... 512

Экспорт и импорт правил мониторинга файловых операций ..... 515


## Настройка парметров задачи Мониторинг файловых операций

► *Чтобы настроить параметры задачи Мониторинг файловых операций с помощью Плагина управления:*

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

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.
5. На вкладке **Параметры мониторинга файловых операций** настройте следующие параметры:
   - Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

     Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

     Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

     По умолчанию флажок установлен.
   - Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

     Этот флажок включает или выключает защиту USN-журнала.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

     Если флажок снят, программа не контролирует изменения в USN-журнале.

     По умолчанию флажок установлен.
6. Добавьте правила мониторинга файловых операций (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 536), в соответствии с которыми работает задача.
7. На вкладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. 145).
8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

## Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. Выполните одно из следующих действий:
   - Если вы создаете правило мониторинга файловых операций в политике, в разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
   - Если вы создаете правило мониторинга файловых операций для локальной задачи, в окне **Свойства: Мониторинг файловых операций** перейдите в раздел **Настройка**.
5. В блоке **Область мониторинга** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга файловых операций**.
6. Добавьте область мониторинга файловых операций одним из следующих способов:
   - Если вы хотите выбрать папку или диск через стандартный диалог Microsoft Windows:
     a. Нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Выбрать папку**.

     b. Выберите папку, файловые операции в которой вы хотите контролировать.

     c. Нажмите на кнопку **OK**.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.
     - <\dir*> – все файлы в папке <\dir>.
     - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security для Windows не добавит указанную область мониторинга.

7. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** в контекстном меню кнопки **Добавить** выберите способ добавления доверенных пользователей.

      Откроется окно **Выбор пользователя или группы пользователей**.
   b. Выберите пользователя или группу пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга.
   c. Нажмите на кнопку **OK**.

По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 506), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

8. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:
   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 506) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security для Windows обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

9. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.
10. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:
    a. Установите флажок **Рассчитывать контрольную сумму файла после файловой операции, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

       Если флажок снят, Kaspersky Embedded Systems Security для Windows не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

- **Хеш MD5**;
- **Хеш SHA256**.

11. Если необходимо, добавьте папки или диски для исключения из выбранной области контроля файловых операций:

a. На вкладке **Исключения** установите флажок **Исключить следующие папки из области контроля**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security для Windows пропускает области мониторинга, указанные в списке исключений.

Если флажок снят, Kaspersky Embedded Systems Security для Windows фиксирует события для всех указанных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

b. Нажмите на кнопку **Добавить**.

Откроется окно **Исключение из области контроля**.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Выбрать папку**.

d. Выберите папку или диск.

e. Нажмите на кнопку **OK**.

Указанная папка или диск отобразится в списке исключений на вкладке **Исключения**.

> Вы можете добавить исключения для области мониторинга файловых операций вручную, используя те же маски, что и для задания областей мониторинга файловых операций.

12. В окне **OK** нажмите на кнопку **Правило мониторинга файловых операций**.

Настроенное правило мониторинга файловых операций отобразится в окне **Мониторинг файловых операций** / **Свойства: Мониторинг файловых операций** в блоке **Область мониторинга**.

## Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. Выполните одно из следующих действий:
   - Если вы хотите импортировать или экспортировать правила мониторинга файловых операций в политике, в разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
   - Если вы хотите импортировать или экспортировать правила мониторинга файловых операций для локальной задачи, в окне **Свойства: Мониторинг файловых операций** перейдите в раздел **Настройка**.
5. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

kaspersky

# Управление мониторингом файловых операций с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Консоли программы.

## В этом разделе


Настройка параметров задачи Мониторинг файловых операций ..... 516

Создание и настройка правила мониторинга файловых операций ..... 517

Экспорт и импорт правил мониторинга файловых операций ..... 519


## Настройка параметров задачи Мониторинг файловых операций

► *Чтобы настроить общие параметры задачи Мониторинг файловых операций с помощью Консоли программы*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На вкладке **Общие** настройте следующие параметры:
   a. Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

      Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

      Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

      По умолчанию флажок установлен.

   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

      Этот флажок включает или выключает защиту USN-журнала.

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

      Если флажок снят, программа не контролирует изменения в USN-журнале.

      По умолчанию флажок установлен.

5. На вкладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 145).
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

## Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Правила мониторинга файловых операций** перейдите по ссылке **Мониторинг файловых операций**.

   Откроется окно **Правила мониторинга файловых операций**.
4. Укажите путь для области мониторинга файловых операций одним из следующих способов:
   - Если вы хотите выбрать папку или диск через стандартный диалог Microsoft Windows:
     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Выбрать папку**.

     b. Выберите папку, файловые операции в которой вы хотите контролировать.

     c. Нажмите на кнопку **OK**.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.
     - <\dir*> – все файлы в папке <\dir>.
     - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security для Windows не добавит указанную область мониторинга.

5. Нажмите на кнопку **Добавить**.

   Область мониторинга отобразится в списке в левой части окна **Правила мониторинга файловых операций**.

6. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

      Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
   b. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами из выбранной области мониторинга.
   c. Нажмите на кнопку **OK**.

   По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 506), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

7. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:
   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 506) установите флажки напротив тех операций, которые вы хотите контролировать.

   По умолчанию Kaspersky Embedded Systems Security для Windows обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

8. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области мониторинга, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.
9. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:
   a. В блоке **Контрольная сумма** выберите **Рассчитывать контрольную сумму измененного файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

      Если флажок установлен, Kaspersky Embedded Systems Security для Windows рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

      Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows не рассчитывает контрольную сумму измененных файлов.

      Расчет контрольной суммы не выполняется в следующих случаях:

      - если файл стал недоступен (например, в результате изменения прав доступа к файлу);
      - если файловая операция обнаружена в файле, который впоследствии был удален.

      По умолчанию флажок снят.

b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих вариантов:

- **Хеш MD5**;
- **Хеш SHA256**.

10. Если необходимо, добавьте папки или диски для исключения из мониторинга файловых операций:

a. На вкладке **Исключения** установите флажок **Учитывать исключенные области мониторинга**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security для Windows пропускает области мониторинга, указанные в списке исключений.

Если флажок снят, Kaspersky Embedded Systems Security для Windows фиксирует события для всех указанных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

b. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Выбрать папку**.

c. Выберите папку или диск.

d. Нажмите на кнопку **OK**.

e. Нажмите на кнопку **Добавить**.

Указанная папка или диск отобразится в списке исключений.

Вы можете добавить исключения для области мониторинга файловых операций вручную, используя те же маски, что и для задания областей мониторинга файловых операций.

11. Нажмите на кнопку **Сохранить**.

## Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.

3. В панели результатов узла **Правила мониторинга файловых операций** перейдите по ссылке **Мониторинг файловых операций**.

   Откроется окно **Правила мониторинга файловых операций**.

4. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

# Управление мониторингом файловых операций с помощью Веб-плагина

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Веб-плагина.

## В этом разделе

Настройка параметров задачи Мониторинг файловых операций ..... 520
Создание и настройка правила мониторинга файловых операций ..... 521
Экспорт и импорт правил мониторинга файловых операций ..... 524

## Настройка параметров задачи Мониторинг файловых операций

► *Чтобы настроить параметры задачи Мониторинг файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.

6. На вкладке **Параметры мониторинга файловых операций** настройте следующие параметры:
   a. Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

      Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

Если флажок установлен, Kaspersky Embedded Systems Security для Windows будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

По умолчанию флажок установлен.

b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

Этот флажок включает или выключает защиту USN-журнала.

Если флажок установлен, Kaspersky Embedded Systems Security для Windows блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

Если флажок снят, программа не контролирует изменения в USN-журнале.

По умолчанию флажок установлен.

7. На вкладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 145).
8. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

## Создание и настройка правила мониторинга файловых операций

► *Чтобы создать и настроить правило мониторинга файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
6. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга файловых операций**.
7. В поле **Выполнять мониторинг файловых операций для области** укажите путь с помощью одной из поддерживаемых масок:
   - <*.ext> – все файлы с расширением <ext>, независимо от их расположения.
   - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения.
   - <\dir*> – все файлы в папке <\dir>.

- <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

> При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security для Windows не добавит указанную область мониторинга.

8. На вкладке **Доверенные пользователи**, если необходимо, задайте доверенных пользователей одним из следующих способов:
   - С помощью кнопки **Добавить**:
     a. Нажмите на кнопку **Добавить**.
     b. В открывшемся окне в поле **Имя пользователя** укажите пользователя или группу пользователей в формате SID.
     c. Нажмите на кнопку **OK**.
   - С помощью кнопки **Добавить из списка Сервера администрирования**:
     a. Нажмите на кнопку **Добавить из списка Сервера администрирования**.
     b. В открывшемся окне выберите пользователя или группу пользователей из списка.
     c. Нажмите на кнопку **OK**.

   Доверенным пользователям разрешены операции с файлами из выбранной области мониторинга.

> По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 506), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

9. На вкладке **Маркеры файловых операций**, если необходимо, укажите маркеры файловых операций, которые вы хотите контролировать:
   a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
   b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 506) установите флажки напротив тех операций, которые вы хотите контролировать.

> По умолчанию Kaspersky Embedded Systems Security для Windows обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы программа блокировала все файловые операции для выбранной области мониторинга, установите флажок **Обнаруживать и блокировать все файловые операции в выбранной области**.
11. Если вы хотите, чтобы программа рассчитывала контрольную сумму файла после его изменения:
    a. Установите флажок **Рассчитывать контрольную сумму файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

       Если флажок установлен, Kaspersky Embedded Systems Security для Windows

рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Embedded Systems Security для Windows не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция обнаружена в файле, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

- **Хеш SHA256**;
- **Хеш MD5**.

12. Если необходимо, добавьте папки или диски для исключения из мониторинга файловых операций:

a. На вкладке **Исключения** установите флажок **Исключить следующие папки из области контроля**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security для Windows пропускает области мониторинга, указанные в списке исключений.

Если флажок снят, Kaspersky Embedded Systems Security для Windows фиксирует события для всех указанных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

b. Нажмите на кнопку **Добавить**.

c. В открывшемся справа окне в поле **Имя папки** введите путь к папке или диску, который вы хотите исключить из области мониторинга файловых операций.

d. Нажмите на кнопку **OK**.

Путь к указанной папке или диску отобразится в списке.

13. В окне **Правило мониторинга файловых операций** нажмите на кнопку **OK**.

Настроенное правило мониторинга файловых операций отобразится в окне **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.

## Экспорт и импорт правил мониторинга файловых операций

Вы можете экспортировать в XML-файл правила мониторинга файловых операций, созданные вручную в свойствах задачи Мониторинг файловых операций.

Вы можете импортировать правила мониторинга файловых операций, ранее экспортированные в XML-файл, в свойства задачи Мониторинг файловых операций.

► *Чтобы экспортировать или импортировать правила мониторинга файловых операций с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций** на вкладке **Параметры мониторинга файловых операций**.
6. Экспортируйте или импортируйте правила мониторинга файловых операций:
   - Как экспортировать правила мониторинга файловых операций.
   - Как импортировать правила мониторинга файловых операций.
7. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

# AMSI-защита

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

## В этом разделе


О задаче AMSI-защита ..... 525

Параметры задачи AMSI-защита, установленные по умолчанию ..... 526

Настройка параметров задачи AMSI-защита с помощью Плагина управления ..... 526

Настройка параметров задачи AMSI-защита с помощью Консоли программы ..... 527

Настройка параметров задачи AMSI-защита с помощью Веб-плагина ..... 529

Статистика задачи AMSI-защита ..... 530


## О задаче AMSI-защита

В ходе выполнения задачи AMSI-защита Kaspersky Embedded Systems Security для Windows контролирует выполнение скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript®. Программа может также обрабатывать скрипты PowerShell™ и скрипты, работающие в программах Microsoft Office в операционных системах с установленным компонентом Antimalware Scan Interface (далее "AMSI"). Можно разрешить или запретить исполнение опасных или предположительно опасных скриптов. Если программа Kaspersky Embedded Systems Security для Windows признала скрипт предположительно опасным, она выполняет выбранное вами действие: запрещает или разрешает выполнение скрипта. Если выбрано действие **Блокировать выполнение**, программа разрешает выполнение скрипта, только если этот скрипт считается безопасным.

Начиная с операционных систем Microsoft Windows 10 и Microsoft Windows Server 2016, Kaspersky Embedded Systems Security для Windows поддерживает технологию AMSI. Технология AMSI позволяет интегрировать программы и службы с любым установленным на устройстве антивирусным программным обеспечением, чтобы это программное обеспечение могло перехватывать и проверять все исполняемые скрипты.

Более подробная информация о технологии AMSI приведена на сайте Microsoft Windows https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal.

Вы можете настраивать параметры задачи AMSI-защита (см. раздел "Настройка параметров задачи AMSI-защита с помощью Консоли программы" на стр. 527).

# Параметры задачи AMSI-защита, установленные по умолчанию

По умолчанию локальная системная задача AMSI-защита имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 73. Параметры задачи AMSI-защита, установленные по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Действия над опасными скриптами** | **Блокировать выполнение** | Вы можете указывать действия, выполняемые при обнаружении предположительно опасных скриптов: запрещать или разрешать их выполнение. |
| **Эвристический анализатор** | Применяется уровень безопасности **Средний**. | Можно включать и выключать эвристический анализатор. Можно настраивать уровень анализа. |
| **Доверенная зона** | Применяется | Единый список исключений, который можно применять в выбранных задачах. |

# Настройка параметров задачи AMSI-защита с помощью Плагина управления

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Постоянная защита сервера** окна **Свойства: <Имя политики>** нажмите на кнопку **Настройка** в подразделе **AMSI-защита**.

5. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
6. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

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

       Этот уровень выбран по умолчанию.
     - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
7. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
8. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

# Настройка параметров задачи AMSI-защита с помощью Консоли программы

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **AMSI-защита**.
3. В панели результатов узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В разделе **Действия над опасными скриптами** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
5. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень анализа с помощью ползунка.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

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

       Этот уровень выбран по умолчанию.
     - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
6. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
7. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

# Настройка параметров задачи AMSI-защита с помощью Веб-плагина

► *Чтобы настроить задачу AMSI-защита, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита сервера**.
5. Нажмите на кнопку **Настройка** в подразделе **AMSI-защита**.
6. В разделе **Действия над опасными скриптами** на закладке **Общие** выполните одно из следующих действий:
   - Чтобы разрешить выполнение предположительно опасных скриптов, выберите вариант **Разрешать**.
   - Чтобы запретить выполнение предположительно опасных скриптов, выберите вариант **Блокировать выполнение**.
7. В разделе **Эвристический анализатор** выполните одно из следующих действий:
   - Снимите или установите флажок **Использовать эвристический анализатор**.
   - Если требуется, отрегулируйте уровень эвристического анализа.

     Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

     Существуют следующие уровни чувствительности проверки:

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

       Этот уровень выбран по умолчанию.
     - **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

       Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
8. В разделе **Доверенная зона** снимите или установите флажок **Применять доверенную зону**.
9. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

# Статистика задачи AMSI-защита

В ходе выполнения задачи **AMSI-защита** вы можете просматривать информацию о количестве скриптов, обработанных программой Kaspersky Embedded Systems Security для Windows с момента запуска задачи.

► *Чтобы просмотреть статистику задачи AMSI-защита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **AMSI-защита**.

   Текущая статистика задачи отобразится в панели результатов узла, в разделах **Управление** и **Статистика**.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Embedded Systems Security для Windows обработала за время выполнения задачи (см. таблицу ниже).

*Таблица 74. Статистика задачи AMSI-защита*

| Поле | Описание |
|---|---|
| **Заблокировано скриптов** | Количество скриптов, заблокированных Kaspersky Embedded Systems Security для Windows. |
| **Обнаружено опасных скриптов** | Количество обнаруженных опасных скриптов. |
| **Обнаружено предположительно опасных скриптов** | Количество обнаруженных предположительно опасных скриптов. |
| **Обработано скриптов** | Общее количество обработанных скриптов. |

kaspersky

# Мониторинг доступа к реестру

В этом разделе описано, как запустить и настроить задачу Мониторинг доступа к реестру.

## В этом разделе


О задаче Мониторинг доступа к реестру ..... 531

О правилах мониторинга доступа к реестру ..... 531

Параметры по умолчанию для задачи Мониторинг доступа к реестру ..... 534

Управление мониторингом доступа к реестру с помощью Плагина управления ..... 535

Управление мониторингом доступа к реестру с помощью Консоли программы ..... 538

Управление мониторингом доступа к реестру с помощью Веб-плагина ..... 541


## О задаче Мониторинг доступа к реестру

Задача Мониторинг доступа к реестру предназначена для отслеживания действий, выполненных с указанными ветвями и разделами реестра, в областях мониторинга, заданных в параметрах задачи. Задача отслеживает действия в операционной системе, установленной на устройстве, или в контейнерах Windows Server 2016 и более поздних версий, указанных в области мониторинга. Вы можете использовать задачу, чтобы обнаруживать изменения, указывающие на нарушение безопасности на защищаемом устройстве.

Чтобы запустить задачу Мониторинг доступа к реестру, необходимо настроить хотя бы одно правило мониторинга.

## О правилах мониторинга доступа к реестру

Задача **Мониторинг доступа к реестру** запускается в соответствии с правилами мониторинга доступа к реестру. Вы можете использовать критерии срабатывания правила, чтобы настроить условия запуска задачи, и установить уровень важности обнаруженных событий, записываемых в журнал задачи.

Правило мониторинга доступа к реестру задается для каждой области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- **Действия**
- **Контролируемые значения**
- **Доверенные пользователи**

**Действия**

При запуске задачи Мониторинг доступа к реестру Kaspersky Embedded Systems Security для Windows использует список действий для мониторинга реестра (см. таблицу ниже).

При обнаружении действия, указанного в качестве критерия срабатывания правила, программа регистрирует соответствующее событие.

Уровень важности фиксируемых событий не зависит от выбранных действий и количества событий.

По умолчанию Kaspersky Embedded Systems Security для Windows учитывает все действия. Вы можете настроить список действий вручную в параметрах правила задачи.

*Таблица 75. Действия*

| Действие | Ограничения | Операционная система |
|---|---|---|
| **Создать раздел** | • Для Windows XP и Windows Server 2003, если вы добавляете в список **Создать раздел** действие **Действия**, а затем выбираете режим **Блокировать операции согласно правилам**, в указанных операционных системах создание раздела не блокируется из-за их системных ограничений. Раздел создается с соответствующим уведомлением, отправляемым в журнал событий.<br>• Если вы хотите запретить создание определенного раздела с помощью редактора реестра, создайте правило для родительского раздела реестра и добавьте в список **Создание вложенных разделов** действие **Действия**, а затем выберите режим **Блокировать операции согласно правилам**. | Windows XP и выше |
| **Удалить раздел** | Если вы хотите удалить родительский раздел, убедитесь, что в списке **Удалить раздел** для настраиваемого раздела реестра сняты оба флажка: **Удаление вложенных разделов** и **Действия**, поскольку родительский раздел можно удалить, только включая подразделы. | Windows XP и выше |
| **Переименование ключа** | Недоступно | Windows XP и выше |
| **Изменение параметров безопасности раздела** | Недоступно | Windows Vista и выше |
| **Удаление значений** | Недоступно | Windows XP и выше |

| Действие | Ограничения | Операционная система |
|---|---|---|
| **Задать значения** | Если вы добавляете в список **Задать значения** действие **Действия**, в правиле для раздела указываете **Значение или маска значения** по умолчанию, а затем выбираете режим **Блокировать операции согласно правилам**, раздел не будет создан, поскольку новый раздел может быть создан только со значением по умолчанию. | Windows XP и выше |
| **Создать вложенные разделы** | Недоступно | Windows XP и выше |
| **Удалить вложенные разделы** | Недоступно | Windows XP и выше |
| **Переименовать вложенные разделы** | Недоступно | Windows XP и выше |
| **Изменить параметры безопасности вложенных разделов** | Недоступно | Windows Vista и выше |

**Значения реестра**

В дополнение к мониторингу разделов реестра можно блокировать или контролировать изменения существующих значений реестра. Доступны следующие варианты:

- **Изменение значения** – создать новые или изменить существующие значения реестра.
- **Удалить значение** – удалить существующие значения реестра.

Переименование и изменение параметров безопасности не применимо к значениям реестра.

**Доверенные пользователи**

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности событий, формируя список доверенных пользователей в параметрах правила мониторинга системного реестра.

*Недоверенный пользователь* – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Embedded Systems Security для Windows обнаруживает действие, выполненное недоверенным пользователем, задача Мониторинг доступа к реестру фиксирует критическое событие в журнале выполнения задачи.

*Доверенный пользователь* – пользователь или группа пользователей, которым разрешено выполнение действий в указанной области мониторинга. Если Kaspersky Embedded Systems Security для Windows обнаруживает действие, выполненное доверенным пользователем, задача Мониторинг доступа к реестру фиксирует информационное событие в журнале выполнения задачи.

# Параметры по умолчанию для задачи Мониторинг доступа к реестру

В следующей таблице приведены параметры по умолчанию для задачи Мониторинг доступа к реестру. Вы можете изменять значения параметров с помощью:

- Плагина управления (см. раздел "Управление мониторингом доступа к реестру с помощью Плагина управления" на стр. 535)
- Консоли программы (см. раздел "Управление мониторингом доступа к реестру с помощью Консоли программы" на стр. 538)
- Веб-плагина (см. раздел "Управление мониторингом доступа к реестру с помощью Веб-плагина" на стр. 541)

*Таблица 76. Параметры по умолчанию для задачи Мониторинг доступа к реестру*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Область мониторинга** | Не задано | Этот параметр используется, чтобы задать родительские и вложенные разделы реестра для мониторинга. Обязательный параметр. Если параметр не задан, задача не запустится. События мониторинга создаются для родительских и вложенных разделов реестра в указанной области мониторинга. |
| **Действия** | Выбраны все пункты списка действий | Этот параметр используется, чтобы настроить список требуемых действий посредством установки или снятия соответствующих флажков. |
| **Контролируемые значения** | Не задано | Этот параметр используется, чтобы добавлять, изменять и удалять значения реестра, которые требуется отслеживать для определенной области мониторинга. |
| **Доверенные пользователи** | Не задано | Вы можете указать пользователей и группы пользователей, которым разрешено выполнять определенные действия для указанных разделов реестра. |
| **Режим работы задачи**. | Только статистика | Вы можете выбрать режим работы задачи **Блокировать операции согласно правилам** или, для получения уведомлений, режим **Только статистика**. |
| Расписание запуска задачи | Не задано | Вы можете настроить параметры запуска задачи по расписанию. |

kaspersky

# Управление мониторингом доступа к реестру с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Плагина управления.

## В этом разделе


Настройка параметров задачи Мониторинг доступа к реестру ..... 535

Создание и настройка правила мониторинга доступа к реестру ..... 536

Экспорт и импорт правил мониторинга доступа к реестру ..... 537


## Настройка параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить параметры задачи Мониторинг доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг доступа к реестру**.
5. На вкладке **Параметры мониторинга доступа к реестру** в блоке **Режим работы задачи** выберите требуемый вариант из списка:
   - **Блокировать операции согласно правилам**;
   - **Только статистика**.
6. Добавьте правила мониторинга доступа к реестру (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 536), в соответствии с которыми работает задача.
7. На вкладке **Управление задачей** настройте параметры расписания запуска (см. раздел "Работа с расписанием задач" на стр. 145) задачи.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

# Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. Выполните одно из следующих действий:
   - Если вы создаете правило мониторинга доступа к реестру в политике, в разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
   - Если вы создаете правило мониторинга доступа к реестру для локальной задачи, в окне **Свойства: Мониторинг доступа к реестру** перейдите в раздел **Настройка**.
5. В блоке **Правила мониторинга доступа к реестру** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга доступа к реестру**.
6. В поле **Выполнять мониторинг доступа к реестру для указанной области с параметрами** введите путь с помощью поддерживаемой маски.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы. Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.
7. На вкладке **Добавить** настройте список действий в соответствии с вашими требованиями.

8. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для значения реестра**.
   b. В одноименном поле введите маску значения реестра.
   c. В блоке **Контролируемые операции** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **OK**, чтобы сохранить изменения.
9. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** в контекстном меню кнопки **Добавить** выберите способ добавления доверенных пользователей.

      Откроется окно **Выбор пользователя или группы пользователей**.
   b. Выберите пользователя или группу пользователей, которым разрешено выполнять выбранные действия.
   c. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 531), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.
10. В окне **Правило мониторинга доступа к реестру** нажмите на кнопку **OK**.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** / **Свойства: Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

## Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать или импортировать правила мониторинга доступа к реестру с помощью Плагина управления:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).

- Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).

4. Выполните одно из следующих действий:
   - Если вы хотите импортировать или экспортировать правила мониторинга доступа к реестру в политике, в разделе **Диагностика системы** в блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

     Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
   - Если вы хотите импортировать или экспортировать правила мониторинга доступа к реестру для локальной задачи, в окне **Свойства: Мониторинг доступа к реестру** перейдите в раздел **Настройка**.
5. Экспортируйте или импортируйте правила мониторинга доступа к реестру:
   - Как экспортировать правила мониторинга доступа к реестру.
   - Как импортировать правила мониторинга доступа к реестру.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

# Управление мониторингом доступа к реестру с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Консоли программы.

## В этом разделе

Настройка общих параметров задачи Мониторинг доступа к реестру ..... 538
Создание и настройка правила мониторинга доступа к реестру ..... 539
Экспорт и импорт правил мониторинга доступа к реестру ..... 540

## Настройка общих параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить общие параметры задачи Мониторинг доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Мониторинг доступа к реестру** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на вкладке **Общие**.

4. В блоке **Режим работы** выберите требуемый вариант из списка:
   - **Блокировать операции согласно правилам**;
   - **Только статистика**.
5. На вкладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 145).
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

## Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Правила мониторинга реестра** перейдите по ссылке **Мониторинг доступа к реестру**.

   Откроется окно **Мониторинг доступа к реестру**.
4. В поле **Добавьте раздел системного реестра для мониторинга** введите путь к разделу реестра с помощью поддерживаемой маски.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы.
   Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.
5. Нажмите на кнопку **Добавить**.
6. На вкладке **Действия** для выбранной области мониторинга настройте список действий в соответствии с вашими требованиями.

7. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило обработки значений реестра**.
   b. В одноименном поле введите значение реестра или маску значения реестра.
   c. В блоке **Контролируемые операции** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **OK**, чтобы сохранить изменения.
8. Если необходимо, задайте доверенных пользователей:
   a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.
   b. В окне **Выбор пользователей или групп** выберите пользователей или группы пользователей, которым разрешено выполнять выбранные действия.
   c. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 531), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.
9. В окне **Мониторинг доступа к реестру** нажмите на кнопку **Сохранить**.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

## Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать и импортировать правила мониторинга доступа к реестру с помощью Консоли программы:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг доступа к реестру**.
3. В панели результатов узла **Правила мониторинга реестра** перейдите по ссылке **Мониторинг доступа к реестру**.

   Откроется окно **Мониторинг доступа к реестру**.
4. Как экспортировать правила мониторинга доступа к реестру.
5. Как импортировать правила мониторинга доступа к реестру.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

kaspersky

# Управление мониторингом доступа к реестру с помощью Веб-плагина

В этом разделе описана настройка параметров задачи Мониторинг доступа к реестру с помощью Веб-плагина.

## В этом разделе


Настройка параметров задачи Мониторинг доступа к реестру ..... 541

Создание и настройка правила мониторинга доступа к реестру ..... 542

Экспорт и импорт правил мониторинга доступа к реестру ..... 543


## Настройка параметров задачи Мониторинг доступа к реестру

► *Чтобы настроить задачу Мониторинг доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
6. В блоке **Режим работы** выберите требуемый вариант из списка:
   - **Блокировать операции согласно правилам;**
   - **Только статистика.**
7. Добавьте правила мониторинга доступа к реестру (см. раздел "Создание и настройка правила мониторинга доступа к реестру" на стр. 542), в соответствии с которыми работает задача.
8. На вкладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 145).
9. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Kaspersky Embedded Systems Security для Windows применит новые значения параметров в выполняющейся задаче. Информация о дате и времени изменения параметров сохраняется в журнале системного аудита.

## Создание и настройка правила мониторинга доступа к реестру

Правила мониторинга доступа к реестру применяются в том порядке, в котором они перечислены в блоке **Правила мониторинга доступа к реестру**.

► *Чтобы создать и настроить правило мониторинга доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В подразделе **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
6. В блоке **Правила мониторинга доступа к реестру** нажмите на кнопку **Добавить**.

   Откроется окно **Правило мониторинга доступа к реестру**.
7. В поле **Выполнять мониторинг доступа к реестру для области** введите путь, используя поддерживаемую маску.

   При создании правил избегайте использования поддерживаемых масок для корневых разделов.
   Если вы укажете только корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, будет создано огромное количество уведомлений с адресацией указанных вложенных разделов, что приведет к проблемам с производительностью системы.
   Если вы укажете корневой раздел, например, HKEY_CURRENT_USER, или корневой раздел с маской для всех вложенных разделов, например HKEY_CURRENT_USER*, и выберите режим **Блокировать операции согласно правилам**, система не сможет читать и изменять разделы, необходимые для работы операционной системы, и перестанет отвечать.
8. На вкладке **Действия** для выбранной области мониторинга настройте список действий в соответствии с вашими требованиями.
9. Определите значения реестра, которые будет контролировать правило:
   a. На вкладке **Контролируемые значения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило обработки значений реестра**.
   b. В одноименном поле введите маску значения реестра.
   c. В блоке **Контролируемые действия** выберите действия над значением реестра, которые будет контролировать правило.
   d. Нажмите на кнопку **OK**, чтобы сохранить изменения.

10. Если необходимо, задайте доверенных пользователей:
    a. На вкладке **Доверенные пользователи** нажмите на кнопку **Добавить**.
    b. Введите **Имя пользователя** или нажмите на кнопку **Установить SID для группы Все**, чтобы задать пользователей, которым разрешено выполнять выбранные действия.
    c. Нажмите на кнопку **OK**, чтобы сохранить изменения.

    По умолчанию Kaspersky Embedded Systems Security для Windows считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга доступа к реестру" на стр. 531), и формирует для них события с уровнем важности Критический. Для доверенных пользователей осуществляется сбор статистики.

11. В окне **Правило мониторинга доступа к реестру** нажмите на кнопку **OK**, чтобы сохранить изменения.

Настроенное правило мониторинга доступа к реестру отобразится в окне **Мониторинг доступа к реестру** в блоке **Правила мониторинга доступа к реестру**.

## Экспорт и импорт правил мониторинга доступа к реестру

Вы можете экспортировать в XML-файл правила мониторинга доступа к реестру, созданные вручную в свойствах задачи Мониторинг доступа к реестру.

Вы можете импортировать правила мониторинга доступа к реестру, ранее экспортированные в XML-файл, в свойства задачи Мониторинг доступа к реестру.

► *Чтобы экспортировать или импортировать правила мониторинга доступа к реестру с помощью Веб-плагина:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. В блоке **Мониторинг доступа к реестру** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг доступа к реестру** на вкладке **Параметры мониторинга доступа к реестру**.
6. Экспортируйте или импортируйте правила мониторинга доступа к реестру:
   - Как экспортировать правила мониторинга доступа к реестру.
   - Как импортировать правила мониторинга доступа к реестру.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

kaspersky

# Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

## В этом разделе


О задаче Анализ журналов ..... 544

Параметры по умолчанию для задачи Анализ журналов ..... 546

Управление правилами анализа журналов с помощью Плагина управления ..... 547

Управление правилами анализа журналов с помощью Консоли программы ..... 550

Управление правилами анализа журналов с помощью Веб-плагина ..... 553


## О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Embedded Systems Security для Windows контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках кибератак.

Kaspersky Embedded Systems Security для Windows анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами, заданными пользователем, или с параметрами эвристического анализатора, который применяется задачей для анализа журналов.

**Стандартные правила и эвристический анализ**

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью стандартных правил, осуществляющих анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом устройстве, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь стандартных правил. Вы можете включать и выключать любые правила. Нельзя удалять существующие правила и создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Embedded Systems Security для Windows не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

**Пользовательские правила задачи Анализ журналов**

С помощью параметров правил вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил анализа журналов содержит четыре правила. Вы можете включать и выключать эти правила, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при создании новой записи в журнале событий Windows, если в свойствах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать журнал в журнале событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом журнале. Вы можете выбрать один из стандартных журналов (Программа, Безопасность или Система) или указать пользовательский журнал, введя его имя в поле выбора источника.

  Программа не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows.

При срабатывании правила Kaspersky Embedded Systems Security для Windows фиксирует событие с уровнем важности Критический в журнале выполнения задачи Анализ журналов.

По умолчанию в задаче Анализ журналов применяются пользовательские правила.

Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробная информация приведена в статье Microsoft https://technet.microsoft.com/ru-ru/library/cc952128.aspx.

# Параметры по умолчанию для задачи Анализ журналов

По умолчанию в задаче Анализ журналов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 77. Параметры по умолчанию для задачи Анализ журналов*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Применять пользовательские правила для анализа журналов** | Не применяется. | Пользовательские правила можно включать, отключать, добавлять или изменять. |
| **Использовать предзаданные правила для анализа журналов** | Применяется. | Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве. |
| **Обработка перебора пароля** | 10 неудачных попыток входа в течение 300 секунд. | Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора. |
| **Обработка сетевого входа** | 00:00:00 | Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security для Windows расценивает данное действие как аномальную активность. |
| **Исключения** | Не применяется. | Можно указать пользователей и IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора. |
| Расписание запуска задачи | Время первого запуска не задано. | Вы можете настроить расписание запуска задачи. |

kaspersky

# Управление правилами анализа журналов с помощью Плагина управления

В этом разделе описано добавление и настройка правил анализа журналов с помощью Плагина управления.

## В этом разделе


Управление стандартными правилами задачи с помощью Плагина управления ..... 547

Добавление правил анализа журналов с помощью Плагина управления ..... 549


## Управление стандартными правилами задачи с помощью Плагина управления

► *Чтобы настроить параметры стандартных правил для задачи Анализ журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Диагностика системы** в подразделе **Настройка** нажмите на кнопку **Анализ журналов**.

   Откроется окно **Анализ журналов**.
5. Выберите закладку **Предзаданные правила**.
6. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security для Windows применяет эвристический анализатор для обнаружения аномальной активности на защищаемом устройстве.

   Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Embedded Systems Security для Windows применяет стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок снят.

Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.

7. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
8. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Анализ журналов**.
9. В разделе **Обработка подбора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
10. В разделе **Обработка атипичной аутентификации** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Embedded Systems Security для Windows как аномальная активность.
11. Выберите закладку **Исключения**.
12. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

       Указанный пользователь будет добавлен в список доверенных.
13. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.
14. Указанный IP-адрес будет добавлен в список доверенных.
15. На закладке **Управление задачей** настройте расписание запуска задачи (см. раздел "Настройка расписания задач" на стр. 145).
16. В окне **Анализ журналов** нажмите на кнопку **OK**.

Параметры задачи Анализ журналов будут сохранены.

## Добавление правил анализа журналов с помощью Плагина управления

► *Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "**Настройка политики**" на стр. 127).
   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам программы (см. раздел "Переход к параметрам локальной задачи и общим параметрам программы для отдельного компьютера" на стр. 131).
4. В разделе **Диагностика системы** в подразделе **Настройка** нажмите на кнопку **Анализ журналов**.

   Откроется окно **Анализ журналов**.
5. На закладке **Пользовательские правила** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security для Windows применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Embedded Systems Security для Windows применяет параметры правил по умолчанию.

   По умолчанию флажок снят. Активно только правило обнаружения всплывающих окон программ.

   Вы можете контролировать применение стандартных правил для анализа журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.
6. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

   Откроется окно **Пользовательское правило**.
7. В разделе **Общие** укажите следующие данные нового правила:
   - **Имя правила**
   - **Правило срабатывает на появление новых записей в журнале событий Windows, если в параметрах события обнаружен указанный идентификатор (ID)**

     Выберите журнал, события которого будут использоваться для анализа. Доступны следующие журналы событий Windows: Программа, Безопасность, Система.

Вы можете добавить новый пользовательский журнал, указав название журнала в поле **Правило срабатывает на появление новых записей в журнале событий Windows, если в параметрах события обнаружен указанный идентификатор (ID)**.

8. В разделе **Критерии срабатывания** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
   a. Укажите идентификатор.
   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
9. Нажмите на кнопку **OK**.

   Правило анализа журналов добавится в список правил.

# Управление правилами анализа журналов с помощью Консоли программы

В этом разделе описано добавление и настройка правил анализа журналов с помощью Консоли программы.

## В этом разделе

Управление стандартными правилами задачи с помощью Консоли программы ..... 550
Добавление правил анализа журналов с помощью Консоли программы ..... 552

## Управление стандартными правилами задачи с помощью Консоли программы

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Свойства** перейдите по ссылке **Анализ журналов**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security для Windows применяет эвристический анализатор для обнаружения аномальной активности на защищаемом устройстве.

   Если этот флажок не установлен, то эвристический анализатор не используется, и Kaspersky Embedded Systems Security для Windows применяет стандартные или

пользовательские правила для обнаружения аномальной активности.

По умолчанию флажок снят.

Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.

6. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
7. Чтобы настроить параметры выбранных правил, выберите закладку **Расширенные**.
8. В разделе **Обработка перебора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
9. В разделе **Обработка сетевого входа** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Embedded Systems Security для Windows как аномальная активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

    Указанный пользователь будет добавлен в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.

    Указанный IP-адрес будет добавлен в список доверенных.
13. Выберите закладки **Расписание** и **Дополнительно**, чтобы настроить расписание запуска задачи.
14. В окне **Параметры задачи** нажмите на кнопку **OK**.

    Параметры задачи Анализ журналов будут сохранены.

## Добавление правил анализа журналов с помощью Консоли программы

► *Чтобы добавить и настроить пользовательское правило анализа журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.
4. Откроется окно **Правила анализа журналов**.
5. Снимите или установите флажок **Применять пользовательские правила для анализа журналов. Настроенные параметры правил не применяются, если флажок снят**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security для Windows применяет пользовательские правила анализа журналов в соответствии с параметрами правил. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Embedded Systems Security для Windows применяет параметры правил по умолчанию.

   По умолчанию флажок снят. Активно только правило обнаружения всплывающих окон программ.

   Вы можете контролировать применение стандартных правил в задаче Анализ журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы создать пользовательское правило, выполните следующие действия:
   a. Введите имя нового правила.
   b. Нажмите на кнопку **Добавить**.

      Созданное правило добавится в общий список правил.
7. Чтобы настроить правило, выполните следующие действия:
   a. Выберите правило в списке.

      В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

      Комментарии для нового правила пусты.

   b. Выберите закладку **Параметры правила**.
8. В разделе **Общие** укажите следующие данные нового правила:
   - **Имя правила**
   - **Имя журнала**

     Выберите журнал, события которого будут использоваться для анализа. Доступны следующие журналы событий Windows: Программа, Безопасность, Система.

     Вы можете добавить новый пользовательский журнал, указав название журнала в

поле **Правило срабатывает на появление новых записей в журнале событий Windows, если в параметрах события обнаружен указанный идентификатор (ID)**.

- **Правило срабатывает на появление новых записей в журнале событий Windows, если в параметрах события обнаружен указанный идентификатор (ID)**

  Укажите программу, события которой будут использоваться для анализа.

9. В разделе **Идентификаторы событий** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
   a. Укажите идентификатор события.
   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
10. Нажмите на кнопку **Сохранить**.

    Настроенные параметры правил анализа журналов будут применены.

# Управление правилами анализа журналов с помощью Веб-плагина

► *Чтобы добавить и настроить правила анализа журналов с помощью Веб-плагина, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Настройка** в подразделе **Анализ журналов**.
6. Настройте параметры, приведены в следующей таблице.

*Таблица 78. Параметры задачи Анализ журналов*

| Параметр | Описание |
|---|---|
| **Применять пользовательские правила для анализа журналов** | Пользовательские правила можно включать, отключать, добавлять или изменять.<br>Этот параметр доступен в таблице со списком пользовательских правил. |
| **Использовать предзаданные правила для анализа журналов** | Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве.<br>Этот параметр доступен в таблице со списком пользовательских правил. |
| **Считать попытки неудачного ввода пароля потенциальной атакой, если они выполняются с указанной частотой** | Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора. |
| **Обнаруживать сетевую сессию, если вход выполнен в указанный интервал** | Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security для Windows расценивает данное действие как аномальную активность. |
| **Исключения** | Можно указать пользователей, которые не будут являться критериями срабатывания эвристического анализатора. |
| **Исключения IP-адресов** | Можно указать IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора. |
| **Управление задачей** | Вы можете настроить расписание запуска задачи. |

# Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке задач проверки по требованию и по настройке параметров безопасности защищаемого устройства.

## В этом разделе


О задачах проверки по требованию ... 555

Об области проверки и параметрах безопасности задачи ... 556

Стандартные области проверки ... 558

Проверка файлов в интернет-хранилище ... 559

Стандартные уровни безопасности ... 561

Проверка съемных дисков ... 563

О задаче Мониторинг целостности файлов на основе эталона ... 564

Включение запуска задачи проверки по требованию из контекстного меню ... 566

Заданные по умолчанию параметры задач проверки по требованию ... 567

Управление задачами проверки по требованию с помощью Плагина управления ... 570

Управление задачами проверки по требованию с помощью Консоли программы ... 588

Управление задачами проверки по требованию с помощью Веб-плагина ... 608


## О задачах проверки по требованию

Kaspersky Embedded Systems Security для Windows проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Embedded Systems Security для Windows проверяет файлы и оперативную память защищаемого устройства, а также объекты автозапуска.

В Kaspersky Embedded Systems Security для Windows предусмотрены следующие задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Embedded Systems Security для Windows. Программа проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Embedded Systems Security для Windows создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет их резервными копиями.

  Задача Проверка при старте операционной системы создается автоматически после установки. По умолчанию применяется режим Только уведомлять. В этом случае после развертывания Kaspersky Embedded Systems Security для Windows на устройствах можно включить задачу Проверка при старте операционной системы, если во время проверки не было обнаружено проблем с сервисами операционной системы. Если программа определяет, что критические сервисы операционной системы являются зараженными или возможно зараженными, режим Только уведомлять позволяет выяснить причину и решить проблему. Если программа применяет режим Выполнять рекомендуемое действие, выполняется действие Лечить.

Действие Удалять, если не удалось вылечить, лечение или удаление системных файлов могут привести к критическим проблемам при запуске операционной системы.

Задача Проверка при старте операционной системы может не выполняться, если защищаемое устройство выходит из спящего режима или режима гибернации. Задача выполняется только при перезагрузке защищаемого устройства или при его запуске после полного выключения.

- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Embedded Systems Security для Windows проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы в системных папках, например, в папке %windir%\system32. Kaspersky Embedded Systems Security для Windows применяет параметры безопасности, соответствующие рекомендуемому уровню (см. раздел "Стандартные уровни безопасности" на стр. 561). Вы можете изменять параметры задачи Проверка важных областей.
- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Embedded Systems Security для Windows на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом устройстве.

Kaspersky Embedded Systems Security для Windows может одновременно выполнять несколько задач проверки по требованию.

# Об области проверки и параметрах безопасности задачи

В Консоли программы область проверки выбранной задачи проверки по требованию представляет собой дерево или список файловых ресурсов защищаемого устройства, которые может контролировать Kaspersky Embedded Systems Security для Windows. По умолчанию файловые ресурсы защищаемого устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы включить отображение сетевых файловых ресурсов в виде дерева в Консоли программы,*

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

Элементы и узлы в дереве или списке файловых ресурсов защищаемого устройства отображаются следующим образом:

☑ Узел включен в область проверки.

☐ Узел исключен из области проверки.

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

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

С помощью Консоли программы можно также добавлять виртуальные диски (см. раздел "Создание виртуальной области проверки" на стр. 595) в область проверки. Имена виртуальных узлов отображаются шрифтом синего цвета.

**Параметры безопасности**

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию параметры безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

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

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

# Стандартные области проверки

Дерево или список файловых ресурсов зачищаемого устройства для выбранной задачи проверки по требованию отображается в окне **Настройка области проверки**.

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security для Windows предусмотрены следующие стандартные области проверки:

- **Мой компьютер**. Kaspersky Embedded Systems Security для Windows проверяет защищаемое устройство целиком.
- **Локальные жесткие диски**. Kaspersky Embedded Systems Security для Windows проверяет объекты на жестких дисках защищаемого устройства. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Kaspersky Embedded Systems Security для Windows проверяет файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, используемая для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются с правами системной учетной записи.

  Подключенные сетевые диски также не отображаются в дереве файловых ресурсов защищаемого устройства. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Системная память**. Kaspersky Embedded Systems Security для Windows проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Embedded Systems Security для Windows проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули, которые автоматически запускаются при запуске защищаемого устройства.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом устройстве.
- **Виртуальные диски**. Вы можете включать в область проверки виртуальные папки, файлы и диски, подключенные к защищаемому устройству, например, общие диски кластера.

  Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы проверить объекты на виртуальном диске, включите в область проверки папку на защищаемом устройстве, с которой связан этот виртуальный диск.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов. Они доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**.
  - **Съемные диски**.
  - **Системная память**.
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows).
  - **Съемные диски**.
  - **Системная память**.
  - **Объекты автозапуска**.
- Прочие задачи:
  - **Локальные жесткие диски** (исключая папки Windows).
  - **Съемные диски**.
  - **Системная память**.
  - **Объекты автозапуска**.
  - **Папки общего доступа**.

# Проверка файлов в интернет-хранилище

### Об облачных файлах

Kaspersky Embedded Systems Security для Windows может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы из OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Embedded Systems Security для Windows не поддерживает другие интернет-хранилища.

Функция "файлы из OneDrive по запросу" помогает получить доступ к вашим файлам OneDrive без необходимости загружать их и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы из OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

Этот значок показывает, что файл доступен *только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, не удастся открыть файлы, доступные только через интернет.

Этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ( ).

Этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

**Проверка облачных файлов**

Kaspersky Embedded Systems Security для Windows может выполнять проверку только облачных файлов, сохраненных локально на защищаемом устройстве. Такие файлы OneDrive имеют статус или . Проверка файлов со статусом не выполняется, поскольку физически они не хранятся на защищаемом устройстве.

Во время проверки Kaspersky Embedded Systems Security для Windows не выполняет автоматическую загрузку файлов со статусом из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Embedded Systems Security для Windows в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область задачи Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан задачей Постоянная защита файлов.
- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.
- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами и с помощью задачи Формирование правил контроля запуска программ. Задача Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

Задача Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом ☁ не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

# Стандартные уровни безопасности

Параметры безопасности **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** не входят в набор параметров стандартных уровней безопасности. При изменении параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов**, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов узла можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый**, **Максимальная защита** или **Только сообщать**. Каждый из этих уровней имеет свои стандартные параметры безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Embedded Systems Security для Windows на защищаемых устройствах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

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

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Только сообщать

Уровень безопасности **Только уведомлять** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

*Таблица 79. Стандартные уровни безопасности и соответствующие им значения параметров безопасности*

| Параметры | Уровень безопасности | | | |
|---|---|---|---|---|
| | Максимальное быстродействие | Рекомендуемый | Максимальная защита | Только сообщать |
| Проверка объектов | По формату | Все объекты | Все объекты | Все объекты |
| **Проверка только новых и измененных файлов** | Включено | Выключено | Выключено | Выключено |
| **Действия над зараженными и другими обнаруженными объектами** | Лечить. Удалить, если не удалось вылечить. | Выполнять рекомендованное специалистами "Лаборатории Касперского" действие | Лечить. Удалить, если не удалось вылечить. | Только сообщать |
| **Действия над возможно зараженными объектами** | Карантин | Выполнять рекомендованное специалистами "Лаборатории Касперского" действие | Карантин | Только сообщать |
| Системно-критические объекты – это файлы, необходимые для работы операционной системы и Kaspersky Embedded Systems Security для Windows. Такие объекты нельзя удалить. Процессы, относящиеся к таким объектам, не могут быть прекращены. | | | | |
| **Исключать файлы** | Нет | Нет | Нет | Нет |
| **Не обнаруживать** | Нет | Нет | Нет | Нет |
| **Останавливать проверку, если она длится более (сек.)** | 60 сек. | Нет | Нет | Нет |
| **Не проверять составные объекты размером более (МБ)** | 8 МБ | Нет | Нет | Нет |

| Параметры | Уровень безопасности | | | |
|---|---|---|---|---|
| **Альтернативные потоки NTFSЗагрузочные секторы дисков и MBR** | Да | Да | Да | Да |
| **Загрузочные секторы дисков и MBR** | Да | Да | Да | Да |
| **Проверка составных объектов** | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Только новые и измененные | • Архивы*<br>• SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Все объекты | • Архивы*<br>• SFX-архивы*<br>• Почтовые базы*<br>• Файлы почтовых форматов*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Все объекты | • Архивы*<br>• SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Все объекты |

# Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.

Kaspersky Embedded Systems Security для Windows выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу Проверка по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Если программа Kaspersky Embedded Systems Security для Windows была установлена без антивирусных баз, проверка съемных дисков будет недоступна.

Kaspersky Embedded Systems Security для Windows запускает проверку подключенных съемных дисков при их регистрации в операционной системе в качестве внешних устройств, подключаемых по USB. Программа не выполняет проверку съемного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Embedded Systems Security для Windows не блокирует доступ к съемному диску на время проверки.

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

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

*Таблица 80. Параметры проверки съемных дисков*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Проверять съемные диски при их подключении по USB** | Флажок снят | Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому устройству. |
| **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** | 8192 МБ | Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на проверяемом диске.<br>Kaspersky Embedded Systems Security для Windows не выполняет проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение. |
| **Запускать проверку с уровнем безопасности** | Максимальная защита | Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности:<br>• **Максимальная защита**<br>• **Рекомендуемый**<br>• **Максимальное быстродействие**<br>Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию. |

# О задаче Мониторинг целостности файлов на основе эталона

Во время выполнения задачи Мониторинг целостности файлов на основе эталона Kaspersky Embedded Systems Security для Windows не проверяет заблокированные файлы, папки, ярлыки файлов и облачные файлы.

В задаче Мониторинг целостности файлов на основе эталона выполняется контроль целостности файлов в области мониторинга посредством сравнения хеша файлов (MD5 или SHA256) с эталонным значением.

При первом запуске задачи Мониторинг целостности файлов на основе эталона, Kaspersky Embedded Systems Security для Windows создает эталон, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При изменении области задачи Мониторинг целостности файлов на основе эталона,

Kaspersky Embedded Systems Security для Windows обновляет эталон при следующем запуске задачи Мониторинг целостности файлов на основе эталона, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При удалении задачи Мониторинг целостности файлов на основе эталона, Kaspersky Embedded Systems Security для Windows удаляет эталон этой задачи.

С помощью командной строки можно удалить эталон (см. раздел "Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE" на стр. 701), не удаляя задачу Мониторинг целостности файлов на основе эталона.

Задача Мониторинг целостности файлов на основе эталона отслеживает следующие изменения файлов в области мониторинга:

- область мониторинга содержит файл, который отсутствует в эталоне;
- в области мониторинга отсутствует файл, который присутствует в эталоне;
- хеш файла в области мониторинга отличается от хеша этого файла в эталоне.

Задача Мониторинг целостности файлов на основе эталона не отслеживает изменения атрибутов файлов и изменения альтернативных потоков.

Если файл или папка недоступны, Kaspersky Embedded Systems Security для Windows не добавляет этот файл или папку в эталон при создании, а формирует событие о невозможности рассчитать хеш при запуске задачи Мониторинг целостности файлов на основе эталона.

Файл или папка могут быть недоступны по следующим причинам:

- указанный путь не существует;
- тип файлов, указанный в маске, отсутствует по указанному пути;
- указанный файл заблокирован;
- указан пустой файл.

# Включение запуска задачи проверки по требованию из контекстного меню

Можно включить запуск задачи проверки по требованию из контекстного меню файла в проводнике Windows.

► *Чтобы включить запуск задачи проверки по требованию из контекстного меню, выполните следующие действия:*

1. Создайте следующие REG-файлы:

```
Windows Registry Editor Version 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Проверить с помощью Kaspersky Embedded Systems Security для Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded
Systems Security для Windows\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security для Windows\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Проверить с помощью Kaspersky Embedded Systems Security для Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded
Systems Security для Windows\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security для Windows\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security для Windows\\kavshell.exe"="~ RUNASADMIN"
```

> Необходимо указать реальное местоположение папки, в которую установлена программа Kaspersky Embedded Systems Security для Windows.

2. Создайте файл `scan.cmd` со следующим содержимым:

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security
для Windows\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Выполняется проверка...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

   Файл `scan.cmd` должен содержать следующую информацию:

   - Местоположение файла `kavshell.exe`.
   - Местоположение временного файла, содержащего результаты проверки.
   - Параметры команды `KAVSHELL SCAN`.
   - Значение времени ожидания закрытия окна консоли после завершения задачи.

3. Скопируйте файл `scan.cmd` в папку, указанную в REG-файле как значение параметра `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]`.

   В примере указана папка `C:\Temp`.

Перезагрузка операционной системы не требуется.

# Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать локальные системные и пользовательские задачи проверки по требованию.

*Таблица 81. Заданные по умолчанию параметры задач проверки по требованию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Область проверки | Применяется в следующих локальных системных и пользовательских задачах:<br>• **Проверка при старте операционной системы**: защищаемое устройство целиком, за исключением папок общего доступа и объектов автозапуска.<br>• **Проверка важных областей**: защищаемое устройство целиком, за исключением папок общего доступа и некоторых файлов операционной системы.<br>• **Проверка по требованию** (пользовательские задачи): защищаемое устройство целиком. | Вы можете изменить область проверки. Область проверки нельзя настроить для локальных системных задач **Проверка объектов на карантине** и **Проверка целостности программы**.<br><br>Задача **Проверка при старте операционной системы** создается автоматически после установки. По умолчанию применяется режим **Только уведомлять**. В этом случае после развертывания Kaspersky Embedded Systems Security для Windows на устройствах можно включить задачу **Проверка при старте операционной системы**, если во время проверки не было обнаружено проблем с сервисами операционной системы. Если программа определяет, что критические сервисы операционной системы являются зараженными или возможно зараженными, режим **Только уведомлять** позволяет выяснить причину и решить проблему. Если программа применяет режим **Выполнять рекомендуемое действие**, выполняется действие **Лечить.** Действие **Удалять, если не удалось вылечить**, лечение или удаление системных файлов могут привести к критическим проблемам при запуске операционной системы. |
| Параметры безопасности | Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**. | Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия:<br>• выбрать другой стандартный уровень безопасности;<br>• вручную изменить параметры безопасности.<br>Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла. |
| **Использовать эвристический анализатор** | Применяется с уровнем анализа **Средний** для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач.<br>Применяется с уровнем анализа **Глубокий** для задачи Проверка объектов на карантине. | Вы можете включать и выключать применение эвристического анализатора и регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине.<br>Эвристический анализатор не используется в задачах Проверка целостности программы и Мониторинг целостности файлов на основе эталона. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Применять доверенную зону** | Применяется (не применяется для задачи Проверка объектов на карантине) | Единый список исключений, который можно применять в выбранных задачах. |
| **Использовать KSN для проверки** | Применяется. | Вы можете увеличить эффективность защиты устройства с помощью инфраструктуры облачных служб Kaspersky Security Network. |
| Параметры запуска задачи с определенными правами | Задача запускается с правами системной учетной записи. | Вы можете изменять параметры запуска задач с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы. |
| **Выполнять задачу в фоновом режиме** (низкий приоритет) | Не применяется | Вы можете настраивать приоритетность выполнения задач проверки по требованию. |
| Расписание запуска задачи | Применяется в локальных системных задачах:<br>• Проверка при старте операционной системы – **При запуске программы**;<br>• Проверка важных областей – **Еженедельно**;<br>• Проверка объектов на карантине – **После обновления баз программы**;<br>• Проверка целостности программы – **Ежесуточно**.<br>Не применяется во вновь созданных пользовательских задачах. | Можно настроить параметры для запуска задачи по расписанию. |
| Регистрация выполнения проверки и обновление статуса защиты устройства | Статус защиты устройства обновляется еженедельно после выполнения задачи Проверка важных областей. | Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами:<br>• изменяя параметры расписания запуска задачи Проверка важных областей;<br>• изменяя область проверки задачи Проверка важных областей;<br>• создавая пользовательские задачи проверки по требованию. |

kaspersky

# Управление задачами проверки по требованию с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

## В этом разделе


Навигация ..... 570

Создание задачи проверки по требованию ..... 572

Настройка области проверки для задачи ..... 577

Выбор стандартных уровней безопасности в задачах проверки по требованию ..... 578

Настройка параметров безопасности вручную ..... 579

Настройка проверки съемных дисков ..... 586

Настройка задачи Мониторинг целостности файлов на основе эталона ..... 587


# Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к мастеру создания задачи проверки по требованию ..... 570

Переход к свойствам задачи проверки по требованию ..... 571


### Переход к мастеру создания задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Для создания локальной задачи:
   a. Разверните узел **Управляемые устройства** в Консоли администрирования Kaspersky Security Center.
   b. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
   c. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства.
   d. Выберите пункт меню **Свойства**.
   e. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.

2. Для создания групповой задачи:
   a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
   b. Выберите группу администрирования, для которой требуется создать задачу.
   c. Выберите закладку **Задачи**.
   d. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
3. Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:
   a. В Консоли администрирования Kaspersky Security Center в панели результатов узла **Выборки устройств** нажмите на кнопку **Запустить выборку**, чтобы выбрать устройства.
   b. Выберите закладку **Результаты выборки "имя выборки"**.
   c. В раскрывающемся списке **Сделать выборку** выберите вариант **Создать задачу для результатов выборки**.

   Откроется окно **Мастер создания задачи**.
4. Выберите задачу **Проверка по требованию** в списке доступных задач для Kaspersky Embedded Systems Security для Windows.
5. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

Настройте параметры задачи в соответствии с вашими требованиями.

► *Чтобы настроить задачу проверки по требованию,*

откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач Kaspersky Security Center.

Откроется окно **Свойства: Проверка по требованию**.

## Переход к свойствам задачи проверки по требованию

► *Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите закладку **Устройства**.
4. Дважды щелкните мышью по имени защищаемого устройства, для которого вы хотите настроить область проверки.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. Выберите раздел **Задачи**.
6. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.

7. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Проверка по требованию**.

Настройте параметры задачи в соответствии с вашими требованиями.

## Создание задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка** (см. раздел "**Переход к мастеру создания задачи проверки по требованию**" на стр. 570) в мастере создания задачи.
2. Выберите требуемый **Способ создания задачи**.
3. Нажмите на кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки.

   По умолчанию область проверки включает критические области защищаемого устройства. Проверяемые области помечены в таблице значком ☑. Области, являющиеся исключениями из проверки, помечены в таблице значком ☐.
   Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

   - Чтобы исключить из проверки все важные области, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
   - Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
     a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить область** или нажмите на кнопку **Добавить**.
     b. В окне **Добавление в область проверки** выберите стандартную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом устройстве в сети и нажмите на кнопку **OK**.
   - Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:
     a. Откройте контекстное меню и выберите пункт **Настроить**.
     b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
     c. На закладке **Общие** в окне **Настройка проверки по требованию** снимите флажки **Вложенные папки** и **Вложенные файлы**.

- Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
  a. Откройте контекстное меню области проверки, параметры которой требуется изменить, и выберите пункт **Настроить**.
  b. В окне **Настройка проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

  Параметры безопасности настраиваются таким же образом, как и для задачи Постоянная защита файлов (см. раздел "Настройка параметров безопасности вручную" на стр. 327).

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

5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:

- Настройте применение эвристического анализатора (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. 322).
- Установите флажок **Применить Доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону.

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

  По умолчанию флажок установлен.

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

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

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

  Если флажок снят, задача проверки по требованию не использует службы KSN.

  По умолчанию флажок установлен.

- Чтобы присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**.

  Флажок изменяет приоритет задачи.

  Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Embedded Systems Security для Windows и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

  Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security для Windows и другие программы. В этом случае скорость выполнения задачи увеличивается.

  По умолчанию флажок снят.

  По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security для Windows, имеют приоритет *Средний*.

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

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых устройств по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security для Windows. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок снят для пользовательских задач проверки по требованию.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** укажите параметры запуска задачи по расписанию.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
10. Нажмите на кнопку **Далее**.
11. Укажите название задачи.
12. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

    Откроется окно **Завершение создания задачи**.

13. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
14. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача проверки по требованию для выбранного защищаемого устройства или группы защищаемых устройств.

## В этом разделе

Присвоение задаче проверки по требованию статуса Проверка важных областей ..... 575
Выполнение задач проверки по требованию в фоновом режиме ..... 576
Регистрация выполнения задачи Проверка важных областей..... 576

## Присвоение задаче проверки по требованию статуса Проверка важных областей

По умолчанию Kaspersky Security Center присваивает защищаемому устройству статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано параметром для порога формирования события в Kaspersky Embedded Systems Security для Windows – *Проверка важных областей защищаемого устройства давно не выполнялась*.

► *Чтобы настроить проверку всех защищаемых устройств, входящих в одну группу администрирования, выполните следующие действия:*

1. Создайте групповую задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 572).
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей**. Указанные параметры задачи (область проверки и параметры безопасности) будут применены ко всем защищаемым устройствам в группе. Настройте расписание задачи.

   Флажок **Считать выполнение задачи проверкой важных областей** можно установить при создании задачи проверки по требованию для группы защищаемых устройств или позднее в окне **Свойства: <Название задачи>** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).

3. С помощью новой или существующей политики выключите запуск по расписанию локальных системных задач проверки по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 116) для группы защищаемых устройств.

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

Вы можете присваивать статус *Проверка важных областей* как групповым задачам проверки по требованию, так и задачам для групп защищаемых устройств.

В Консоли программы можно также просмотреть, имеет ли задача проверки по требованию статус Проверка важных областей.

В Консоли программы флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задачи, но не доступен для редактирования.

## Выполнение задач проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Embedded Systems Security для Windows, имеют приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но может положительно повлиять на скорость выполнения процессов других запущенных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Можно указать максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к мастеру создания задачи проверки по требованию**" на стр. 570).
2. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

   Флажок изменяет приоритет задачи.

   Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Embedded Systems Security для Windows и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

   Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security для Windows и другие программы. В этом случае скорость выполнения задачи увеличивается.

   По умолчанию флажок снят.
3. Нажмите на кнопку **OK**.

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

## Регистрация выполнения задачи Проверка важных областей

По умолчанию статус защиты устройства отображается в панели результатов узла **Kaspersky Embedded Systems Security для Windows** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты устройства привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. По умолчанию флажок установлен только для задачи Проверка важных областей и недоступен для редактирования в этой задаче.

Вы можете выбрать задачу проверки по требованию, связанную со статусом защиты устройства, только в Kaspersky Security Center.

## Настройка области проверки для задачи

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security для Windows (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security для Windows** > **Изменение или удаление Kaspersky Embedded Systems Security для Windows**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

► *Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. Чтобы включить элементы в область проверки:
   a. Откройте контекстное меню для списка областей проверки.
   b. В контекстном меню выберите пункт **Добавить область**.
   c. В открывшемся окне **Добавление в область проверки** выберите тип объектов, который вы хотите добавить:
      - **Предопределенная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
      - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
      - **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

   Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.
4. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.

5. Чтобы изменить область проверки или исключение, в контекстном меню требуемой области проверки выберите пункт **Изменить область**.
6. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить область**.

   Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

7. Нажмите на кнопку **OK**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

## Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узлов, выбранных в списке файловых ресурсов защищаемого устройства, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. В списке защищаемых устройств выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

6. Нажмите на кнопку **OK**.
7. В окне **Свойства: Проверка по требованию** нажмите на кнопку **OK**.

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

# Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 561) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. В списке областей проверки выберите элементы, для которых вы хотите настроить параметры безопасности.

   Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 172) можно применить к выбранному узлу или элементу в области проверки.

4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
5. На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
   - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 580)
   - **Действия** (см. раздел "**Настройка действий**" на стр. 583)
   - **Производительность** (см. раздел "**Настройка производительности**" на стр. 585)
   - **Иерархическое хранилище**
6. Нажмите на кнопку **OK** в окне **Настройка проверки по требованию**.
7. Нажмите на кнопку **OK** в окне **Область проверки**.

Новые параметры области проверки будут сохранены.

## В этом разделе

Настройка общих параметров задачи ..... 580
Настройка действий ..... 583
Настройка производительности ..... 585

## Настройка общих параметров задачи

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

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. На закладке **Общие** в блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:
   - **Объекты проверки**:
     - **Все объекты**

       Kaspersky Embedded Systems Security для Windows проверяет все объекты.
     - **Объекты, проверяемые по формату**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
     - **Объекты, проверяемые по указанному списку расширений**

       Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.
   - **Вложенные папки**
   - **Вложенные файлы**
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

     По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

6. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

7. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все / Только новые архивы**

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

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

- **Все / Только новые почтовые базы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

► *Чтобы настроить действия над зараженными и другими обнаруженными объектами во время выполнения задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Действия**.
6. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать.**

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.
   - **Лечить**.
   - **Лечить. Удалять, если не удалось вылечить**. **Лечить. Удалять, если не удалось вылечить**.
   - **Удалять.**

     Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**.
7. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

- **Помещать на карантин**.
- **Удалять**.

  Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.
- **Выполнять рекомендуемое действие**.

  Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

8. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Embedded Systems Security для Windows не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.
9. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

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

   Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.
10. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 571).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Производительность**.
6. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
7. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**

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

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

     Если флажок снят, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

  Исключение из проверки объектов больше указанного размера.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

## Настройка проверки съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.

3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

   В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.
6. В блоке **Параметры проверки при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security для Windows автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

## Настройка задачи Мониторинг целостности файлов на основе эталона

► *Чтобы настроить групповую задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
5. В разделе **Область проверки** выполните следующие действия:
   a. Чтобы добавить папку в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.
      2. Установите или снимите флажок **Проверять эту область**.

3. Нажмите на кнопку **Обзор**, чтобы указать папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.

b. Чтобы добавить или исключить добавленную ранее папку из области задачи Мониторинг целостности файлов на основе эталона, снимите или установите флажок слева от пути к папке в таблице **Область проверки**.

c. Чтобы удалить папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите папку в таблице **Область проверки** и нажмите на кнопку **Удалить**.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
8. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в *Справке Kaspersky Security Center*.

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

# Управление задачами проверки по требованию с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

## В этом разделе

Навигация ..... 589
Создание и настройка задачи проверки по требованию ..... 589
Область проверки в задачах проверки по требованию ..... 592
Настройка параметров безопасности ..... 596
Проверка съемных дисков ..... 605
Статистика задач проверки по требованию ..... 605
Создание и настройка задачи Мониторинг целостности файлов на основе эталона ..... 607

kaspersky

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

### В этом разделе

Переход к параметрам задачи проверки по требованию ..... 589
Переход к параметрам области действия задачи проверки по требованию ..... 589

### Переход к параметрам задачи проверки по требованию

► *Чтобы перейти к общим параметрам задачи проверки по требованию в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

### Переход к параметрам области действия задачи проверки по требованию

► *Чтобы перейти к параметрам области проверки в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

## Создание и настройка задачи проверки по требованию

Вы можете создавать пользовательские задачи для отдельного защищаемого устройства в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Embedded Systems Security для Windows создание пользовательских задач не предусмотрено.

► *Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.

3. Настройте следующие параметры задачи:

- **Имя** – название задачи, содержащее не более 100 символов. Допускаются любые символы, кроме **" * < > & \ : |**.

  Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано название задачи.

- **Описание** – дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.

- **Использовать эвристический анализатор**.

  Флажок включает или выключает использование эвристического анализатора при проверке объектов.

  Если флажок установлен, эвристический анализатор включен.

  Если флажок снят, эвристический анализатор выключен.

  По умолчанию флажок установлен.

- **Выполнять задачу в фоновом режиме**.

  Флажок изменяет приоритет задачи.

  Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Embedded Systems Security для Windows и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

  Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security для Windows и другие программы. В этом случае скорость выполнения задачи увеличивается.

  По умолчанию флажок снят.

- **Применять доверенную зону**.

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

  По умолчанию флажок установлен.

- **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых устройств по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security для Windows. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок снят для пользовательских задач проверки по требованию.

- **Использовать KSN для проверки**.

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

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

  Если флажок снят, задача проверки по требованию не использует службы KSN.

  По умолчанию флажок установлен.

4. Настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165) на закладках **Расписание** и **Дополнительно**.
5. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
6. В окне **Добавить задачу** нажмите на кнопку **OK**.

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 258).
7. Если требуется, в панели результатов выбранного узла выберите **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
8. В дереве или в списке файловых ресурсов защищаемого устройства выберите узлы или элементы, которые вы хотите включить в область проверки.
9. Выберите один из стандартных уровней безопасности (см. раздел "Стандартные уровни безопасности" на стр. 561) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности" на стр. 596).
10. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Настроенные параметры будут применены при последующем запуске задачи.

kaspersky

# Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

## В этом разделе


Настройка отображения сетевых файловых ресурсов ..... 592

Формирование области проверки ..... 592

Включение в область проверки сетевых объектов ..... 594

Создание виртуальной области проверки ..... 595


## Настройка отображения сетевых файловых ресурсов

► *Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области проверки, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

   По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

3. Нажмите на кнопку **Сохранить**.

## Формирование области проверки

Если вы управляете Kaspersky Embedded Systems Security для Windows на защищаемом устройстве удаленно, с помощью Консоли программы, установленной на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом устройстве, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security для Windows (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security для Windows** > **Изменение или удаление Kaspersky Embedded Systems Security для Windows**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от выбранного типа отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 592). Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

► *Чтобы сформировать область проверки с помощью дерева сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область проверки все диски определенного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски защищаемого устройства, установите флажок **Съемные диски**).
     - Если вы хотите включить в область проверки отдельный диск определенного типа, разверните узел, который содержит диски этого типа, и установите флажок рядом с именем требуемого диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

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

► *Чтобы сформировать область проверки с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.
   c. В открывшемся окне **Добавление области проверки** выберите тип объектов, который вы хотите добавить:
      - **Предопределенная область**, если вы хотите включить в область проверки одну из предопределенных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.

- **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
- **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.

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

   Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

6. Нажмите на кнопку **Сохранить**.

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

## Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► *Чтобы включить в область проверки сетевой объект, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
   - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
5. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Создание виртуальной области проверки

Можно включать в область проверки виртуальные диски, папки и файлы, таким образом создавая виртуальную область проверки.

Вы можете включить в область проверки отдельные виртуальные диски, папки или файлы, только если область проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 592).

► *Чтобы включить в область проверки виртуальный диск, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла **Виртуальные диски**, выберите пункт **Добавить виртуальный диск** и в списке доступных имен выберите имя виртуального диска.
4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
5. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► *Чтобы включить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла, в который вы хотите добавить папку или файл, и выберите один из следующих вариантов:
   - **Добавить виртуальную папку**, если вы хотите добавить виртуальную папку в область проверки.
   - **Добавить виртуальный файл**, если вы хотите добавить виртуальный файл в область проверки.
4. В поле ввода задайте имя для папки или файла.
5. В строке с именем папки или файла установите флажок, чтобы включить папку или файл в область проверки.
6. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

## Настройка параметров безопасности

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности (см. раздел "Стандартные уровни безопасности" на стр. 561) **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

При работе с деревом сетевых файловых ресурсов параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► *Чтобы настроить параметры безопасности вручную:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В левой части окна выберите узел или элемент, параметры безопасности которого вы хотите настроить.

   Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 172) можно применить к выбранному узлу или элементу в области проверки.

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов (см. раздел "Настройка отображения сетевых файловых ресурсов" на стр. 592), создать область проверки (см. раздел "Формирование области проверки" на стр. 592) и создать виртуальную область проверки (см. раздел "Создание виртуальной области проверки" на стр. 595).
3. В правой части окна выполните одно из следующих действий:
   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности (см. раздел "Выбор стандартных уровней безопасности в задачах проверки по требованию" на стр. 597).

- На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
  - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 598)
  - **Действия** (см. раздел "**Настройка действий**" на стр. 600)
  - **Производительность** (см. раздел "**Настройка производительности**" на стр. 602)
  - **Иерархическое хранилище**

4. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Новые параметры области проверки будут сохранены.

## В этом разделе

Выбор стандартных уровней безопасности в задачах проверки по требованию ..... 597
Настройка общих параметров задачи ..... 598
Настройка действий ..... 600
Настройка производительности ..... 602
Настройка иерархического хранилища ..... 604

## Выбор стандартных уровней безопасности в задачах проверки по требованию

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

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

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область проверки.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

## Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. Выберите закладку **Общие**.
3. В блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:
   - **Объекты проверки**:
     - **Все объекты**

       Kaspersky Embedded Systems Security для Windows проверяет все объекты.
     - **Объекты, проверяемые по формату**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.
     - **Объекты, проверяемые по указанному списку расширений**

       Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

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

     Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

     Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

     Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

     По умолчанию флажок установлен.

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все** / **Только новые архивы**

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

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

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

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

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

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка действий

► *Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. Выберите закладку **Действия**.

3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.
   - **Лечить**.
   - **Лечить. Удалять, если не удалось вылечить**.**Лечить. Удалять, если не удалось вылечить**.
   - **Удалять**.

     Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**.
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.
   - **Помещать на карантин**.
   - **Удалять**.

     Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.
   - **Выполнять рекомендуемое действие**.

     Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. Однако Kaspersky Embedded Systems Security для Windows не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security для Windows выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.
   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.
6. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

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

   Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.
7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
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 Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
4. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**

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

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

     Если флажок снят, продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки объектов больше указанного размера.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Настройка иерархического хранилища

► *Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "**Переход к параметрам области действия задачи проверки по требованию**" на стр. 589).
2. Выберите закладку **Иерархическое хранилище**.
3. Выберите одно из следующих действий над файлами:
   - **Не проверять**
   - **Проверять только резидентную часть файла**
   - **Проверять файл полностью**

     Если выбрано это действие, доступны следующие параметры проверки:

     - Снимите или установите флажок **Только если обращение к файлу производилось в указанный период (сут)** и укажите количество дней.
     - Снимите или установите флажок **Не копировать файл на локальный жесткий диск, если возможно**.

4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

## Проверка съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

2. В блоке **Параметры проверки при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security для Windows автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.
3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

## Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security для Windows обработала с момента запуска задачи.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security для Windows в журналах выполнения задач" на стр. 263).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

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

В таблице ниже приведена информация об объектах, которые программа Kaspersky Embedded Systems Security для Windows обработала с момента запуска задачи.

*Таблица 82. Статистика задач проверки по требованию*

| Поле | Описание |
|---|---|
| **Обнаружено** | Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security для Windows. Например, если программа Kaspersky Embedded Systems Security для Windows обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу. |
| **Зараженных и других обнаруживаемых объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows обнаружила и признала зараженными, или количество обнаруженных объектов, которые не были исключены из области проверки и были определены как легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным. |
| **Возможно зараженных объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows признала возможно зараженными. |
| **Объектов не вылечено** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows не вылечила по следующим причинам:<br>• Тип обнаруженного объекта не предполагает лечения.<br>• При лечении возникла ошибка. |
| **Объектов не помещено на карантин** | Количество объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось поместить на карантин, например, из-за отсутствия свободного места на диске. |
| **Объектов не удалено** | Количество объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось удалить, например, если доступ к объекту был заблокирован другой программой. |
| **Объектов не проверено** | Количество объектов в области защиты, которые программе Kaspersky Embedded Systems Security для Windows не удалось проверить, например, если доступ к объекту был заблокирован другой программой. |
| **Объектов, не помещенных в резервное хранилище** | Количество объектов, копии которых программе Kaspersky Embedded Systems Security для Windows не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске. |
| **Ошибок обработки** | Количество объектов, во время обработки которых возникла ошибка задачи. |
| **Вылечено объектов** | Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security для Windows. |
| **Помещено на карантин** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows поместила на карантин. |
| **Помещено в резервное хранилище** | Количество объектов, копии которых программа Kaspersky Embedded Systems Security для Windows сохранила в резервном хранилище. |
| **Удалено объектов** | Количество объектов, которые удалила программа Kaspersky Embedded Systems Security для Windows. |
| **Защищенных паролем объектов** | Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security для Windows пропустила, так как эти объекты защищены паролем. |
| **Поврежденных объектов** | Количество объектов, которые программа Kaspersky Embedded Systems Security для Windows пропустила, так как их формат искажен. |

| Поле | Описание |
|---|---|
| **Обработано объектов** | Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security для Windows. |

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в разделе **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

## Создание и настройка задачи Мониторинг целостности файлов на основе эталона

► *Чтобы создать или настроить задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Диагностика системы**.
2. Выберите пункт **Создать задачу Мониторинг файловых операций**.

   Откроется окно **Добавить задачу**.
3. В раскрывающемся списке **Алгоритм расчета контрольных сумм** выберите один из следующих вариантов:
   - **MD5**
   - **SHA256**
4. В таблице **Области проверки** выполните следующие действия:
   a. Чтобы добавить файл или папку в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.
      2. Установите или снимите флажок **Проверять эту область**.
      3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
      4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.
      5. Нажмите на кнопку **OK**.

   b. Чтобы поменять файл или папку, добавленную ранее в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Изменить**.

         Откроется окно **Область проверки**.
      2. Установите или снимите флажок **Проверять эту область**.

3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.
4. Установите или снимите флажок **Также проверять подпапки**, чтобы включить или исключить все вложенные папки из области задачи Мониторинг целостности файлов на основе эталона.
5. Нажмите на кнопку **OK**.

c. Чтобы удалить файл или папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите этот файл или папку в таблице **Области проверки** и нажмите на кнопку **Удалить**.

5. Настройте расписание запуска задачи (см. раздел "Настройка параметров расписания задач" на стр. 165) на закладках **Расписание** и **Дополнительно**.
6. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 168).
7. В окне **Добавить задачу** нажмите на кнопку **OK**.

   Будет создана пользовательская задача Мониторинг целостности файлов на основе эталона. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (см. раздел "Журнал системного аудита" на стр. 258).

► *Чтобы просмотреть параметры задачи Мониторинг целостности файлов на основе эталона, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

# Управление задачами проверки по требованию с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина для защищаемых устройств в сети.

## Переход к мастеру создания задачи проверки по требованию

► *Чтобы создать локальную задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.

5. Нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.

6. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security для Windows**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. 570).

► *Чтобы создать групповую задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.

4. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security для Windows**.
5. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
6. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. 570).

► *Чтобы создать задачу проверки по требованию для произвольной группы, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
2. Выберите выборку устройств, для которой требуется создать задачу.
3. Нажмите на кнопку **Запустить**.
4. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.
5. Нажмите на кнопку **Создать задачу**.
6. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security для Windows**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями (см. раздел "Управление задачами проверки по требованию с помощью Плагина управления" на стр. 570).

► *Чтобы настроить задачу проверки по требованию, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

Откроется окно **<Название задачи>**.

## Переход к свойствам задачи проверки по требованию

► *Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:*

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
5. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
6. Перейдите на закладку **Параметры программы**.

## Настройка области проверки для задачи

► *Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:*

1. Перейдите к свойствам задачи проверки по требованию (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. 610).
2. Выберите раздел **Область проверки**.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, чтобы добавить новое правило.
   - Выберите существующее правило и нажмите на кнопку **Изменить**.

   Откроется окно **Изменить область**.
4. Установите переключатель в положение **Активный** и выберите тип объекта.
5. В разделе **Защита объектов** настройте следующие параметры:
   - **Режим защиты объектов**:
     - **Все объекты**

       Kaspersky Embedded Systems Security для Windows проверяет все объекты.
     - **Объекты, проверяемые по формату**

       Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

  Kaspersky Embedded Systems Security для Windows проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security для Windows.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Embedded Systems Security для Windows проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Вложенные папки**
- **Вложенные файлы**
- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

- Защита только новых и измененных файлов

  Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security для Windows новыми или измененными с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет и защищает файлы, независимо от того, когда они были изменены.

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

6. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Архивы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **SFX-архивы**

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

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

- **Упакованные объекты**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Почтовые базы**

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых баз при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Файлы почтовых форматов**

  Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Вложенные OLE-объекты**

  Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет объекты, встроенные в файлы.

  Если флажок не установлен, Kaspersky Embedded Systems Security для Windows пропускает объекты, встроенные в файлы, при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

7. В разделе **Действия над зараженными и другими обнаруженными объектами** выберите действие, которое будет выполняться над зараженными и другими обнаруженными объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

   - **Лечить**

   - **Лечить. Удалять, если не удалось вылечить**.**Лечить. Удалять, если не удалось вылечить**

   - **Удалять**.

     Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

   - **Рекомендуемое**

8. В разделе **Действия над возможно зараженными объектами** выберите действие, которое будет выполняться над возможно зараженными объектами:

   - **Только сообщать**.

     Если выбран этот режим, Kaspersky Embedded Systems Security для Windows не блокирует доступ к зараженным или другим обнаруженным объектам и не выполняет над ними никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** нужно настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни в одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security для Windows автоматически изменит уровень безопасности на **Другой**.

   - **Помещать на карантин**.

- **Удалять**.

  Kaspersky Embedded Systems Security для Windows удаляет объект и помещает его копию в резервное хранилище.

- **Рекомендуемое**.

  Kaspersky Embedded Systems Security для Windows выполняет действие, рекомендованное специалистами "Лаборатории Касперского".

9. В разделе **Действия над возможно зараженными объектами** снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

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

   Если флажок установлен и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если программа не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security для Windows не выполняет выбранное действие, если родительский объект неизменяем.

10. В разделе **Исключения** настройте следующие параметры:

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет все объекты.

  По умолчанию флажок снят.

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

  Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

11. В разделе **Дополнительные параметры** настройте следующие параметры:

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

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

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

  Если флажок снят, продолжительность проверки не ограничена.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

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

  Исключение из проверки объектов больше указанного размера.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при антивирусной проверке составные объекты, размер которых превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы и проверяет только новые файлы и файлы, которые были изменены с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

12. В разделе **Действия над автономными файлами** выберите одно из следующих действий над файлами:
    - **Не проверять**
    - **Проверять только резидентную часть файла**
    - **Проверять файл полностью**

      Если выбрано это действие, доступны следующие параметры проверки:
      - Снимите или установите флажок **Только если к файлу производилось обращение в указанный период (сут)** и укажите количество дней.
      - Снимите или установите флажок **Не копировать файл на локальный жесткий диск, если возможно**.
13. Нажмите на кнопку **OK**.

## Настройка параметров задачи

► *Чтобы настроить параметры задачи проверки по требованию, выполните следующие действия:*

1. Перейдите к свойствам задачи проверки по требованию (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. 610).
2. Выберите раздел **Параметры**.
3. 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.
4. При необходимости в раскрывающемся списке **Уровень эвристического анализа** выберите уровень анализа.

   Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни чувствительности проверки:

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

     Этот уровень выбран по умолчанию.

- **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.

5. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

- Установите флажок **Применять доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону.

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

  По умолчанию флажок установлен.

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

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

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

  Если флажок снят, задача проверки по требованию не использует службы KSN.

  По умолчанию флажок установлен.

- Чтобы присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*, установите флажок **Выполнять задачу в фоновом режиме**.

  Флажок изменяет приоритет задачи.

  Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему защищаемого устройства со стороны других задач Kaspersky Embedded Systems Security для Windows и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

  Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security для Windows и другие программы. В этом случае скорость выполнения задачи увеличивается.

  По умолчанию флажок снят.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security для Windows, имеют приоритет *Средний*.

- Чтобы использовать создаваемую задачу в качестве задачи Проверка важных областей, установите флажок **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Проверка важных областей* и обновление статуса защиты устройства. Kaspersky Security Center оценивает безопасность защищаемых устройств по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security для Windows. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты устройства по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок снят для пользовательских задач проверки по требованию.

# Доверенная зона

Этот раздел содержит информацию о доверенной зоне Kaspersky Embedded Systems Security для Windows, а также инструкции по добавлению объектов в доверенную зону при выполнении задач.

## В этом разделе


О доверенной зоне ..... 619

Управление доверенной зоной с помощью Плагина управления ..... 620

Управление доверенной зоной с помощью Консоли программы ..... 627

Управление доверенной зоной с помощью Веб-плагина ..... 635


# О доверенной зоне

Доверенная зона - это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах проверки по требованию и в задаче Постоянная защита файлов, в недавно созданных пользовательских задачах проверки по требованию, всех системных задачах проверки по требованию, за исключением задачи Проверка объектов на карантине.

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный XML-файл, чтобы затем импортировать его в Kaspersky Embedded Systems Security для Windows на другом защищаемом устройстве.

**Доверенные процессы**

Применяется в задачах постоянной защиты файлов.

Некоторые программы на защищаемом устройстве могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Embedded Systems Security для Windows. К таким программам относятся, например, системные программы домен-контроллеров.

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

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Названия некоторых из них приведены на веб-сайте Microsoft https://www.microsoft.com/ru-ru (код статьи: KB822158).

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

Если исполняемый файл изменяется, например, в результате обновления, Kaspersky Embedded Systems Security для Windows исключает его из списка доверенных процессов.

Программа не использует путь к файлу на защищаемом устройстве для идентификации процесса как доверенного. Путь к файлу на локальном компьютере применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

**Операции резервного копирования**

Применяется в задачах постоянной защиты компьютера.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства можно выключить защиту объектов, доступ к которым осуществляется при операциях резервного копирования. Kaspersky Embedded Systems Security для Windows будет проверять объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

**Исключения**

- Применяется в задачах постоянной защиты файлов;
- все объекты, обнаруживаемые в указанных областях защищаемого устройства;
- указанные объекты, обнаруживаемые по имени или маске имени во всей области защиты или проверки.

# Управление доверенной зоной с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка доверенной зоны для одного или всех защищаемых устройств в сети.

## В этом разделе


Навигация ..... 620

Настройка параметров доверенной зоны с помощью Плагина управления ..... 622


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам политики для доверенной зоны ..... 621

Переход к окну параметров доверенной зоны ..... 621

## Переход к параметрам политики для доверенной зоны

► *Чтобы перейти к доверенной зоне в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
6. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

## Переход к окну параметров доверенной зоны

► *Чтобы настроить доверенную зону в окне свойств программы, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security 3.3 для Windows**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Embedded Systems Security 3.3 для Windows**.
7. Выберите раздел **Дополнительные возможности**.
8. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

kaspersky

# Настройка параметров доверенной зоны с помощью Плагина управления

► *Чтобы настроить параметры доверенной зоны:*

1. На вкладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security для Windows пропускает (см. раздел "Добавление исключений" на стр. 622) при выполнении задачи.
2. На вкладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security для Windows пропускает (см. раздел "Добавление доверенных процессов с помощью Плагина управления" на стр. 624) при выполнении задачи.
3. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 627).

## В этом разделе


Добавление исключений ..... 622

Добавление доверенных процессов с помощью Плагина управления ..... 624

Использование маски not-a-virus ..... 627


## Добавление исключений

► *Чтобы добавить исключение в доверенную зону в политике Kaspersky Security Center:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 621).
2. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security для Windows пропускает при проверке и защите:
   - Чтобы создать рекомендуемые исключения, нажмите на кнопку **Добавить рекомендуемые исключения**.

     При нажатии на эту кнопку в список исключений добавляются исключения, рекомендованные корпорацией Microsoft и "Лабораторией Касперского".
   - Чтобы импортировать предварительно настроенные исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Исключения из файла XML будут добавлены в список исключений.
   - Чтобы вручную указать условия, при выполнении которых объект считается доверенным, нажмите на кнопку **Добавить** и перейдите к следующим шагам.

     Откроется окно **Параметры правила исключения**.

3. Если вы нажали на кнопку **Добавить** в разделе **Не проверять объект при выполнении следующих условий**, укажите объекты, которые требуется исключить из области защиты или проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

   - Чтобы исключить объект из области защиты или проверки:

     a. Установите флажок **Объект, исключенный из проверки**.

     Добавляет файл, папку, диск или файл скрипта в исключения.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Embedded Systems Security для Windows, выбранных в разделе **Область применения правила**.

     По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Объект для исключения из проверки**.

     c. Выберите объект, который вы хотите исключить из области проверки.

     > При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security для Windows при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security для Windows обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

     d. Нажмите на кнопку **OK**.

     e. Установите флажок **Применять к подпапкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

   - Чтобы указать имя обнаруживаемого объекта:

     a. Установите флажок **Объекты, исключенные из обнаружения**.

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Объекты для исключения из обнаружения**.

     c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

d. Нажмите на кнопку **Добавить**.

e. Нажмите на кнопку **OK**.

4. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.
5. Нажмите на кнопку **OK**.

Исключение отображается в списке на вкладке **Исключения** окна **Доверенная зона**.

## Добавление доверенных процессов с помощью Плагина управления

► *Чтобы добавить один или несколько процессов в список доверенных с помощью Плагина управления:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 621).
2. Выберите вкладку **Доверенные процессы**.
3. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

   Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом устройстве.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

   По умолчанию флажок установлен.
4. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.
5. Чтобы добавить процесс в список доверенных процессов, выполните одно из следующих действий:
   - Чтобы импортировать предварительно настроенные доверенные процессы, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Процессы из файла XML будут добавлены в список доверенных процессов.
   - Чтобы указать процессы вручную, нажмите на кнопку **Добавить** и перейдите к следующим шагам.

6. Если вы нажали на кнопку **Добавить**, в контекстном меню кнопки выберите один из следующих вариантов:

   - **Несколько процессов**.

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

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

        Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

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

        Если флажок установлен, Kaspersky Embedded Systems Security для Windows использует хеш выбранного файла для определения, является ли процесс доверенным.

        Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

        По умолчанию флажок установлен.

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

     d. Выберите исполняемый файл в открывшемся окне.

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

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

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

     g. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

     h. Нажмите на кнопку **OK**.

        Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Embedded Systems Security для Windows, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

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

     В открывшемся окне **Добавление процесса** выполните следующие действия:

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

При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security для Windows при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security для Windows обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

b. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

c. Нажмите на кнопку **OK**.

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

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

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

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

     Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows использует хеш выбранного файла для определения, является ли процесс доверенным.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  e. Нажмите на кнопку **OK**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

Если вы сделали процесс доверенным для задачи Контроль запуска программ и в параметрах задачи создали доверенный пакет установки на основе исполняемого файла этого процесса, параметры Доверенной зоны имеют больший приоритет. Kaspersky Embedded Systems Security для Windows считает процесс доверенным, но запрещает запуск исполняемого файла этого процесса.

7. В окне **Доверенная зона** нажмите на кнопку **OK**.

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

### Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security для Windows выполнит действия, указанные в параметрах задачи, для программ, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел "**Переход к параметрам политики для доверенной зоны**" на стр. 621).
2. На закладке **Исключения** в графе **Обнаруживаемые объекты** прокрутите список и выберите строку со значением *not-a-virus:**, если флажок снят.
3. Нажмите на кнопку **OK**.

Новые параметры будут применены.

# Управление доверенной зоной с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка доверенной зоны для защищаемого устройства.

## В этом разделе

Использование доверенной зоны для задач в Консоли программы ..... 627
Настройка параметров доверенной зоны в Консоли программы ..... 628

## Использование доверенной зоны для задач в Консоли программы

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

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

► *Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Embedded Systems Security для Windows, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить использование доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** выполните одно из следующих действий:
   - Чтобы применить доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Чтобы выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Чтобы настроить параметры доверенной зоны, перейдите по ссылке в названии флажка **Применять доверенную зону**.

   Откроется окно **Доверенная зона**.

   В окне **Доверенная зона** настройте исключения (см. раздел "Добавление исключений в доверенную зону" на стр. 629) и доверенные процессы (см. раздел "Добавление доверенных процессов с помощью Консоли программы" на стр. 631) и нажмите на кнопку **OK**.
5. Нажмите на кнопку **OK** в окне **Параметры задачи**, чтобы сохранить изменения.

## Настройка параметров доверенной зоны в Консоли программы

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security для Windows пропускает (см. раздел "Добавление исключений в доверенную зону" на стр. 629) при выполнении задачи.
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security для Windows пропускает (см. раздел "Добавление доверенных процессов с помощью Консоли программы" на стр. 631) при выполнении задачи.
3. Примените доверенную зону для задач программы (см. раздел "Использование доверенной зоны для задач в Консоли программы" на стр. 627).
4. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 634).

kaspersky

## В этом разделе

Добавление исключений в доверенную зону ..... 629
Добавление доверенных процессов с помощью Консоли программы ..... 631
Использование маски not-a-virus ..... 634

## Добавление исключений в доверенную зону

► *Чтобы вручную добавить исключение в доверенную зону в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Укажите объекты, которые Kaspersky Embedded Systems Security для Windows пропускает при проверке и защите:
   - Чтобы импортировать предварительно настроенные исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Исключения из файла XML будут добавлены в список исключений.
   - Чтобы вручную указать условия, при выполнении которых объект считается доверенным, нажмите на кнопку **Добавить** и перейдите к следующим шагам.

     Откроется окно **Параметры правила исключения**.
5. Если вы нажали на кнопку **Добавить** в разделе **Не проверять объект при выполнении следующих условий**, укажите объекты, которые требуется исключить из области защиты или проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:
   - Чтобы исключить объект из области защиты или проверки:
     a. Установите флажок **Объект, исключенный из проверки**.

        Добавляет файл, папку, диск или файл скрипта в исключения.

        Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает указанную стандартную область, файл, папку, диск или скрипт при запуске проверки с использованием компонентов Kaspersky Embedded Systems Security для Windows, выбранных в разделе **Область применения правила**.

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Объект для исключения из проверки**.

     c. Выберите объект, который вы хотите исключить из области проверки.

> При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security для Windows при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security для Windows обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

d. Нажмите на кнопку **OK**.

e. Установите флажок **Применять к подпапкам**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Чтобы указать имя обнаруживаемого объекта:

  a. Установите флажок **Объекты, исключенные из обнаружения**.

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

  b. Нажмите на кнопку **Изменить**.

     Откроется окно **Объекты для исключения из обнаружения**.

  c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

  d. Нажмите на кнопку **Добавить**.

  e. Нажмите на кнопку **OK**.

6. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

7. Нажмите на кнопку **OK**.

Исключение отображается в списке на вкладке **Исключения** окна **Доверенная зона**.

## Добавление доверенных процессов с помощью Консоли программы

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

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

Если исполняемый файл процесса изменится, Kaspersky Embedded Systems Security для Windows исключит этот процесс из списка доверенных процессов.

► *Чтобы добавить один или несколько процессов в список доверенных с помощью Консоли программы:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите вкладку **Доверенные процессы**.
4. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

   Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются средствами резервного копирования, установленными на защищаемом устройстве.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет операции чтения файлов, выполняемые средствами резервного копирования, установленными на защищаемом устройстве.

   По умолчанию флажок установлен.
5. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Embedded Systems Security для Windows пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Embedded Systems Security для Windows проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.

6. Чтобы добавить процесс в список доверенных процессов, выполните одно из следующих действий:
   - Чтобы импортировать предварительно настроенные доверенные процессы, нажмите на кнопку **Импорт** и в открывшемся окне выберите файл конфигурации в формате XML, хранящийся на устройстве.

     Процессы из файла XML будут добавлены в список доверенных процессов.
   - Чтобы указать процессы вручную, нажмите на кнопку **Добавить** и перейдите к следующим шагам.
7. Если вы нажали на кнопку **Добавить**, в контекстном меню кнопки выберите один из следующих вариантов:
   - **Несколько процессов**.

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

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

        Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

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

        Если флажок установлен, Kaspersky Embedded Systems Security для Windows использует хеш выбранного файла для определения, является ли процесс доверенным.

        Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

        По умолчанию флажок установлен.

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

     d. Выберите исполняемый файл в открывшемся окне.

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

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

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

     g. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

     h. Нажмите на кнопку **OK**.

> Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Embedded Systems Security для Windows, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

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

  В открывшемся окне **Добавление процесса** выполните следующие действия:

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

  > При указании объектов можно использовать маски имен (с помощью символов ? и *) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security для Windows при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security для Windows обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

  b. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  c. Нажмите на кнопку **OK**.

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

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

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

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

     Если выбран этот вариант, Kaspersky Embedded Systems Security для Windows использует полный путь к файлу для определения, является ли процесс доверенным.

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

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows использует хеш выбранного файла для определения, является ли процесс доверенным.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. В блоке **Область применения исключения** установите флажки рядом с названиями задач, к которым требуется применить исключения.

  e. Нажмите на кнопку **OK**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

Если вы сделали процесс доверенным для задачи Контроль запуска программ и в параметрах задачи создали доверенный пакет установки на основе исполняемого файла этого процесса, параметры Доверенной зоны имеют больший приоритет. Kaspersky Embedded Systems Security для Windows считает процесс доверенным, но запрещает запуск исполняемого файла этого процесса.

8. В окне **Доверенная зона** нажмите на кнопку **OK**.

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

## Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security для Windows выполнит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security для Windows**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Прокрутите список до элемента *not-a-virus:**.
5. Установите соответствующий флажок, если он снят.
6. Нажмите на кнопку **OK**.

Новые параметры будут применены.

# Управление доверенной зоной с помощью Веб-плагина

Чтобы настроить доверенную зону с помощью Веб-плагина, выполните следующие действия:

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.
6. Настройте доверенную зону (см. раздел "Настройка параметров доверенной зоны с помощью Плагина управления" на стр. 622) в соответствии с вашими требованиями.

kaspersky

# Защита от эксплойтов

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

## В этом разделе


О защите от эксплойтов ..... 636

Управление защитой от эксплойтов с помощью Плагина управления ..... 638

Управление защитой от эксплойтов с помощью Консоли программы ..... 642

Управление защитой от эксплойтов с помощью Веб-плагина ..... 646

Техники защиты от эксплойтов ..... 648


# О защите от эксплойтов

Kaspersky Embedded Systems Security для Windows предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

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

Агент защиты процессов – это динамически загружаемый модуль Kaspersky Embedded Systems Security для Windows, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, вам нужно завершить данный процесс. Может потребоваться перезагрузка защищаемого устройства (например, при защите системного процесса).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Embedded Systems Security для Windows 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 устройстве. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемое устройство создается и запускается процесс kavfswh. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

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

Если на устройстве установлена операционная система Windows 10 или более поздних версий, программа не будет продолжать защищать процессы и память процессов после остановки службы Kaspersky Security Exploit Prevention.

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

**Режимы защиты от эксплойтов**

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

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

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Embedded Systems Security для Windows не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

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

  В этом режиме Kaspersky Embedded Systems Security для Windows регистрирует все попытки эксплуатации уязвимостей посредством создания событий. Выбран по умолчанию.

kaspersky

# Управление защитой от эксплойтов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров компонента для защищаемых устройств в сети.

## В этом разделе


Навигация ..... 638

Настройка защиты памяти процессов ..... 639

Добавление процесса в область защиты ..... 641


## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе


Переход к параметрам политики для защиты от эксплойтов ..... 638

Переход к окну параметров защиты от эксплойтов ..... 639


### Переход к параметрам политики для защиты от эксплойтов

► *Чтобы перейти к параметрам защиты от эксплойтов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

### Переход к окну параметров защиты от эксплойтов

► *Чтобы перейти к окну свойства для защиты от эксплойтов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security 3.3 для Windows**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Embedded Systems Security 3.3 для Windows**.
7. Перейдите в раздел **Постоянная защита компьютера**.
8. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

## Настройка защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 638).
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы устройства от эксплуатации уязвимостей.

     По умолчанию флажок снят.
   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Embedded Systems Security для Windows завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

- **Только сообщать**.

  Если выбран данный режим, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.

3. В разделе **Действия по защите** настройте следующие параметры:

- **Сообщать о скомпрометированных процессах посредством службы терминалов**.

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention.

  По умолчанию флажок снят.

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

  Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security для Windows не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

  Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

  По умолчанию флажок снят.

4. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Можно исключить процессы из области защиты, сняв соответствующие флажки в списке процессов.

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

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 638).
2. На закладке **Защищаемые процессы** нажмите на кнопку **Обзор**.

   Откроется окно проводника Windows.
3. Выберите процесс, который вы хотите добавить в список.
4. Нажмите на кнопку **Открыть**.

   Имя процесса будет отображено в строке.
5. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.
6. Выберите добавленный процесс.
7. Нажмите на кнопку **Указать техники защиты от эксплойта**.

   Откроется окно **Техники защиты от эксплойта**.
8. Выберите один из следующих вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**.

     Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
   - **Применять указанные техники защиты от эксплойта**

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

     b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.
9. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
   - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
     - **Интернет**
     - **Интранет**
     - **Доверенные сайты**
     - **Сайты с ограниченным доступом**
     - **Компьютер**

Данные параметры применимы только для Internet Explorer®.

10. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

# Управление защитой от эксплойтов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров компонента на защищаемом устройстве.

## В этом разделе

Навигация ..... 642
Настройка защиты памяти процессов ..... 643
Добавление процесса в область защиты ..... 644

## Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью выбранного интерфейса.

## В этом разделе

Переход к основным параметрам защиты от эксплойтов ..... 642
Переход к параметрам защиты процессов при защите от эксплойтов ..... 643

### Переход к основным параметрам защиты от эксплойтов

► *Чтобы перейти к окну **Параметры защиты от эксплуатации уязвимостей**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита файлов**.
2. Выберите узел **Защита от эксплойтов**.
3. В разделе **Параметры защиты процессов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.

Настройте общие параметры защиты от эксплойтов в соответствии с вашими требованиями.

### Переход к параметрам защиты процессов при защите от эксплойтов

► *Чтобы перейти к окну **Параметры защиты процессов**, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита файлов**.
2. Выберите узел **Защита от эксплойтов**.
3. В разделе **Параметры защиты процессов** перейдите по ссылке **Параметры защиты процессов**.

   Откроется окно **Параметры защиты процессов**.
4. Настройте параметры защиты процессов для защиты от эксплойтов в соответствии с вашими требованиями.

## Настройка защиты памяти процессов

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

1. Откройте окно **Параметры защиты от эксплуатации уязвимостей**.
2. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы устройства от эксплуатации уязвимостей.

     По умолчанию флажок снят.
   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Embedded Systems Security для Windows завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.
   - **Только сообщать**.

     Если выбран данный режим, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows обнаружит факт эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.

3. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention.

     По умолчанию флажок снят.
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security Service**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security для Windows не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

     По умолчанию флажок снят.
4. В окне **Параметры защиты от эксплуатации уязвимостей** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

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

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

1. Откройте окно **Параметры защиты процессов**.
2. Чтобы защитить процесс от компрометации и снизить возможное влияние эксплуатации уязвимостей, выполните следующие действия:
   a. Нажмите на кнопку **Обзор**.

      Откроется стандартное окно Microsoft Windows **Открыть**.

   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.

   c. Нажмите на кнопку **Открыть**.

d. Нажмите на кнопку **Добавить**.

Указанный процесс добавится в список защищаемых процессов.

3. Выберите добавленный процесс в списке.
4. Текущая конфигурация отображается на **Параметры защиты процессов** закладке:
   - **Имя процесса**.
   - **Выполняется сейчас**.
   - **Применяемые техники защиты**.
   - **Снижение области действия процесса (параметры техники Attack Surface Reduction)**.
5. Чтобы изменить применяемые к процессу техники защиты от эксплойтов, выберите закладку **Запрет загрузки модулей**.
6. Выберите один из следующих вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**.

     Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
   - **Применять указанные техники защиты от эксплойта**.

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
7. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
   - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей**.
   - В разделе **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
     - **Интернет**
     - **Интранет**
     - **Доверенные сайты**
     - **Сайты с ограниченным доступом**
     - **Компьютер**

     Данные параметры применимы только для Internet Explorer®.
8. Нажмите на кнопку **Сохранение**.

Процесс будет добавлен в область защиты задачи.

kaspersky

# Управление защитой от эксплойтов с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров компонента на защищаемом устройстве.

## В этом разделе


Настройка защиты памяти процессов ..... 646

Добавление процесса в область защиты ..... 647


## Настройка защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.
6. Откройте закладку **Параметры защиты от эксплойтов**.
7. В разделе **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы устройства от эксплуатации уязвимостей.

     По умолчанию флажок снят.
   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Embedded Systems Security для Windows завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.
   - **Только статистика**.

     Если выбран данный режим, Kaspersky Embedded Systems Security для Windows 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 Embedded Systems Security для Windows обнаружит факт

эксплуатации уязвимости критического процесса, компонент переходит в режим **Только статистика**.

8. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows отображает терминальное окно с описанием причины срабатывания защиты и указанием процесса, в котором была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention.

     По умолчанию флажок снят.
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security Service**.

     Если флажок установлен, Kaspersky Embedded Systems Security для Windows снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security для Windows не защищает процессы, добавленные после остановки службы Kaspersky Security. В случае перезапуска службы снижение рисков эксплуатации уязвимостей будет остановлено для всех процессов.

     Если флажок снят, Kaspersky Embedded Systems Security для Windows не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

     По умолчанию флажок снят.
9. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security для Windows сохранит и применит настроенные параметры защиты памяти процессов.

## Добавление процесса в область защиты

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. В главном окне Веб-консоли Kaspersky Security Center выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.
6. Перейдите на закладку **Защищаемые процессы**.
7. Нажмите на кнопку **Добавить**.
8. Откроется окно **Техники защиты от эксплойтов**.

9. Укажите название процесса.
10. Выберите один из следующих вариантов применения техник снижения рисков:
    - **Применять все доступные техники защиты от эксплойтов**.

      Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.
    - **Применять указанные техники защиты от эксплойтов**

      Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

      a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

      b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.
11. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
    - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
    - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
      - **Интернет**
      - **Интранет**
      - **Доверенные сайты**
      - **Сайты с ограниченным доступом**
      - **Компьютер**

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

Процесс будет добавлен в область защиты задачи.

# Техники защиты от эксплойтов

*Таблица 83. Техники защиты от эксплойтов*

| Техника защиты от эксплойтов | Описание |
|---|---|
| Data Execution Prevention (DEP) | Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти. |
| Address Space Layout Randomization (ASLR) | Изменение расположения структур данных в адресном пространстве процесса. |
| Structured Exception Handler Overwrite Protection (SEHOP) | Подмена записи в структуре исключений или подмена обработчика исключений. |
| Null Page Allocation | Предотвращение переориентации нулевого указателя. |

| Техника защиты от эксплойтов | Описание |
|---|---|
| LoadLibrary Network Call Check (Anti ROP) | Защита от загрузки динамических библиотек с сетевых путей. |
| Executable Stack (Anti ROP) | Запрет на несанкционированное исполнение областей стека. |
| Anti RET Check (Anti ROP) | Проверка безопасного вызова функции через CALL инструкцию. |
| Anti Stack Pivoting (Anti ROP) | Защита от перемещения указателя стека ESP на эксплуатируемый адрес. |
| Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register) | Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll. |
| Heap Spray Allocation (Heapspray) | Защита от выделения памяти под исполнение вредоносного кода. |
| Execution Flow Simulation (Anti Return Oriented Programming) | Обнаружение потенциально опасных цепочек инструкций (возможный ROP-гаджет) в компоненте Windows API. |
| IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP)) | Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile). |
| Attack Surface Reduction (ASR) | Блокирование запуска уязвимых модулей через защищаемый процесс. |
| Anti Process Hollowing (Hollowing) | Защита от создания и запуска вредоносных копий доверенных процессов. |
| Anti AtomBombing (APC) | Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC). |
| Anti CreateLocalThread (RThreadRemote) | Сторонний процесс создал поток в защищаемом процессе. |
| Anti CreateRemoteThread (RThreadRemote) | Защита внедрения потока защищаемого процесса в другой процесс. |

kaspersky

# Интеграция со сторонними системами

Этот раздел содержит описание интеграции Kaspersky Embedded Systems Security для Windows с функциями и технологиями сторонних производителей.

## В этом разделе


Счетчики производительности для программы Системный монитор ..... 650

SNMP-счетчики и ловушки в Kaspersky Embedded Systems Security для Windows ..... 658

Интеграция с WMI ..... 668


# Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы "Системный монитор" Microsoft Windows, которые регистрирует Kaspersky Embedded Systems Security для Windows во время установки.

## В этом разделе


О счетчиках производительности Kaspersky Embedded Systems Security для Windows ..... 651

Общее количество отвергнутых запросов ..... 651

Общее количество пропущенных запросов ..... 652

Количество запросов, не обработанных из-за нехватки системных ресурсов ..... 653

Количество запросов, отправленных на обработку ..... 654

Среднее количество потоков диспетчера файловых перехватов ..... 654

Максимальное количество потоков диспетчера файловых перехватов ..... 655

Количество элементов в очереди зараженных объектов ..... 656

Количество объектов, обрабатываемых за секунду ..... 657

# О счетчиках производительности Kaspersky Embedded Systems Security для Windows

Счетчики производительности – компонент Kaspersky Embedded Systems Security для Windows, с помощью которого вы можете контролировать производительность программы во время выполнения задач постоянной защиты компьютера. Вы можете обнаружить узкие места и недостаточность ресурсов при совместной работе с другими программами. Вы можете диагностировать сбои в работе и неоптимальную настройку Kaspersky Embedded Systems Security для Windows.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security для Windows, открыв консоль **Производительность** Панели управления Windows в разделе **Администрирование**.

В следующих разделах приведены определения счетчиков, рекомендованные интервалы считывания показаний, пороговые значения и рекомендованные значения параметров Kaspersky Embedded Systems Security для Windows для случаев, когда значения счетчиков превышают пороговые значения.

## Общее количество отвергнутых запросов

*Таблица 84. Общее количество отвергнутых запросов*

| | |
|---|---|
| **Название** | Общее количество отвергнутых запросов |
| **Определение** | Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты процессами программы; рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security для Windows.<br>Программа пропускает объекты, запросы на обработку которых отвергаются процессами Kaspersky Embedded Systems Security для Windows. |
| **Назначение** | Счетчик позволяет обнаруживать следующие ситуации:<br>• снижение эффективности постоянной защиты компьютера из-за повышенной нагрузки на процессы Kaspersky Embedded Systems Security для Windows;<br>• прерывание постоянной защиты компьютера из-за отказа диспетчера файловых перехватов. |
| **Нормальное / пороговое значение** | 0 / 1 |
| **Рекомендуемый интервал считывания показаний** | 1 час |

| | |
|---|---|
| **Рекомендации по настройке, если значение превышает пороговое** | Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов.<br>Возможны следующие ситуации в зависимости от поведения счетчика:<br>• Счетчик показывает несколько запросов, отвергнутых в течение длительного времени: все процессы Kaspersky Embedded Systems Security для Windows были полностью загружены, поэтому программа Kaspersky Embedded Systems Security для Windows не смогла проверить объекты.<br>Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты компьютера. Можно использовать такой параметр Kaspersky Embedded Systems Security для Windows, как **Количество процессов для постоянной защиты**.<br>• Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Embedded Systems Security для Windows не проверяет объекты при обращении к ним.<br>Перезапустите Kaspersky Embedded Systems Security для Windows. |

## Общее количество пропущенных запросов

*Таблица 85. Общее количество пропущенных запросов*

| | |
|---|---|
| **Название** | Общее количество пропущенных запросов |
| **Определение** | Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Embedded Systems Security для Windows, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы.<br>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 Embedded Systems Security для Windows пропускает такой объект и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. |
| **Назначение** | Счетчик позволяет обнаруживать снижение производительности из-за сбоев диспетчера файловых перехватов. |
| **Нормальное / пороговое значение** | 0 / 1 |
| **Рекомендуемый интервал считывания показаний** | 1 час |

| | |
|---|---|
| **Рекомендации по настройке, если значение превышает пороговое** | Если значение счетчика отличается от нуля, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент.<br>Если скорость проверки не удовлетворительна, перезапустите Kaspersky Embedded Systems Security для Windows, чтобы восстановить простаивающие потоки. |

## Количество запросов, не обработанных из-за нехватки системных ресурсов

*Таблица 86. 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 Embedded Systems Security для Windows.<br>Kaspersky Embedded Systems Security для Windows пропускает запросы на обработку объектов, которые не обрабатываются драйвером файловых перехватов. |
| **Назначение** | Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты компьютера, возникающее из-за недостаточности системных ресурсов. |
| **Нормальное / пороговое значение** | 0 / 1 |
| **Рекомендуемый интервал считывания показаний** | 1 час |
| **Рекомендации по настройке, если значение превышает пороговое** | Если значение счетчика отличается от нуля, рабочим процессам Kaspersky Embedded Systems Security для Windows требуется больший объем оперативной памяти для обработки запросов.<br>Возможно, активные процессы других программ используют всю доступную оперативную память. |

## Количество запросов, отправленных на обработку

*Таблица 87. Количество запросов, отправленных на обработку*

| | |
|---|---|
| **Название** | Количество запросов, отправленных на обработку. |
| **Определение** | Количество объектов, ожидающих обработки рабочими процессами. |
| **Назначение** | Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Embedded Systems Security для Windows и общий уровень файловой активности на защищаемом устройстве. |
| **Нормальное / пороговое значение** | Значение счетчика может изменяться в зависимости от уровня файловой активности на защищаемом устройстве. |
| **Рекомендуемый интервал считывания показаний** | 1 мин. |
| **Рекомендации по настройке, если значение превышает пороговое** | Недоступно |

## Среднее количество потоков диспетчера файловых перехватов

*Таблица 88. Среднее количество потоков диспетчера файловых перехватов*

| | |
|---|---|
| **Название** | Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams) |
| **Определение** | Количество потоков диспетчера файловых перехватов в одном процессе и среднее по всем процессам, участвующим в задачах постоянной защиты компьютера. |
| **Назначение** | Счетчик позволяет обнаруживать и устранять возможное снижение уровня постоянной защиты компьютера из-за полной загрузки процессов Kaspersky Embedded Systems Security для Windows. |
| **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 Embedded Systems Security для Windows пропустит объект.<br>Увеличьте количество процессов Kaspersky Embedded Systems Security для Windows для задач постоянной защиты компьютера. Можно использовать такой параметр Kaspersky Embedded Systems Security для Windows, как **Количество процессов для постоянной защиты**. |

## Максимальное количество потоков диспетчера файловых перехватов

*Таблица 89. Максимальное количество потоков диспетчера файловых перехватов*

| | |
|---|---|
| **Название** | Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams). |
| **Определение** | Количество потоков диспетчера файловых перехватов в одном процессе и максимальное по всем процессам, участвующим в задачах постоянной защиты компьютера. |
| **Назначение** | Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах. |
| **Нормальное / пороговое значение** | Варьируется / 40. |
| **Рекомендуемый интервал считывания показаний** | 1 мин. |
| **Рекомендации по настройке, если значение превышает пороговое** | Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Kaspersky Embedded Systems Security для Windows неравномерно распределяет нагрузку на выполняющиеся процессы.<br>Перезапустите Kaspersky Embedded Systems Security для Windows. |

## Количество элементов в очереди зараженных объектов

*Таблица 90. Количество элементов в очереди зараженных объектов*

| | |
|---|---|
| **Название** | Количество элементов в очереди зараженных объектов. |
| **Определение** | Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент. |
| **Назначение** | Счетчик позволяет обнаруживать следующие ситуации:<br>• прерывание постоянной защиты компьютера из-за возможного отказа диспетчера файловых перехватов;<br>• перегруженность процессов из-за неравномерного распределения процессорного времени между рабочими процессами и Kaspersky Embedded Systems Security для Windows;<br>• вирусную эпидемию. |
| **Нормальное / пороговое значение** | Значение счетчика может быть отличным от нуля, пока Kaspersky Embedded Systems Security для Windows обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время. |
| **Рекомендуемый интервал считывания показаний** | 1 мин. |
| **Рекомендации по настройке, если значение превышает пороговое** | Если значение счетчика остается ненулевым длительное время:<br>• Kaspersky Embedded Systems Security для Windows не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов).<br>Перезапустите Kaspersky Embedded Systems Security для Windows.<br>• Не хватает процессорного времени для обработки объектов.<br>Обеспечьте выделение Kaspersky Embedded Systems Security для Windows дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ.<br>• Возникла вирусная эпидемия.<br>О возникновении вирусной эпидемии свидетельствует большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи. |

## Количество объектов, обрабатываемых за секунду

*Таблица 91. Количество объектов, обрабатываемых за секунду*

| | |
|---|---|
| **Название** | Количество объектов, обрабатываемых за секунду (Number of objects processed per second) |
| **Определение** | Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени. |
| **Назначение** | Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности защищаемого устройства, возникшее из-за недостаточности процессорного времени, выделяемого рабочим процессам Kaspersky Embedded Systems Security для Windows, или из-за сбоев в работе Kaspersky Embedded Systems Security для Windows. |
| **Нормальное / пороговое значение** | Варьируется / Нет. |
| **Рекомендуемый интервал считывания показаний** | 1 мин. |
| **Рекомендации по настройке, если значение превышает пороговое** | Значения счетчика зависят от установленных значений параметров Kaspersky Embedded Systems Security для Windows и от загрузки защищаемого устройства процессами других программ.<br>Отслеживайте среднее значение показаний счетчика в течение продолжительного времени. Если среднее значение показаний счетчика снизилось, то могла возникнуть одна из следующих ситуаций:<br>• Рабочим процессам Kaspersky Embedded Systems Security для Windows не хватает процессорного времени для обработки объектов.<br>Обеспечьте выделение Kaspersky Embedded Systems Security для Windows дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ.<br>• Возник сбой в работе Kaspersky Embedded Systems Security для Windows (простаивает несколько потоков).<br>Перезапустите Kaspersky Embedded Systems Security для Windows. |

# SNMP-счетчики и ловушки в Kaspersky Embedded Systems Security для Windows

Этот раздел содержит информацию о счетчиках и ловушках Kaspersky Embedded Systems Security для Windows.

## В этом разделе


О SNMP-счетчиках и ловушках Kaspersky Embedded Systems Security для Windows ..... 658

SNMP-счетчики Kaspersky Embedded Systems Security для Windows ..... 658

SNMP-ловушки Kaspersky Embedded Systems Security для Windows и их параметры ..... 662

Описания и возможные значения параметров SNMP-ловушек Kaspersky Embedded Systems Security для Windows ..... 666


## О SNMP-счетчиках и ловушках Kaspersky Embedded Systems Security для Windows

Если вы включили компонент Счетчики и ловушки SNMP в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Embedded Systems Security для Windows по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Embedded Systems Security для Windows на компьютере-рабочем месте администратора, запустите на защищаемом устройстве Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

## SNMP-счетчики Kaspersky Embedded Systems Security для Windows

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Embedded Systems Security для Windows.

## В этом разделе


Счетчики производительности ..... 659

Счетчики карантина ..... 659

Счетчик резервного хранилища ..... 659

Общие счетчики ..... 660

Счетчик обновлений ..... 660

Счетчики постоянной защиты файлов ..... 660

## Счетчики производительности

*Таблица 92. Счетчики производительности*

| Счетчик | Определение |
|---|---|
| currentRequestsAmount | Количество запросов, отправленных на обработку (на стр. 654) |
| currentInfectedQueueLength | Количество элементов в очереди зараженных объектов (на стр. 656) |
| currentObjectProcessingRate | Количество объектов, обрабатываемых за секунду (на стр. 657) |
| currentWorkProcessesNumber | Количество рабочих процессов Kaspersky Embedded Systems Security для Windows в текущий момент |

## Счетчики карантина

*Таблица 93. Счетчики карантина*

| Счетчик | Определение |
|---|---|
| totalObjects | Количество объектов в папке карантина в текущий момент |
| totalSuspiciousObjects | Количество возможно зараженных объектов в папке карантина в текущий момент |
| currentStorageSize | Общий объем данных в папке карантина (МБ) |

## Счетчик резервного хранилища

*Таблица 94. Счетчик резервного хранилища*

| Счетчик | Определение |
|---|---|
| currentBackupStorageSize | Общий объем данных в папке резервного хранилища (МБ) |

## Общие счетчики

*Таблица 95. Общие счетчики*

| Счетчик | Определение |
|---|---|
| lastCriticalAreasScanAge | Период с момента проведения последней полной проверки важных областей защищаемого устройства (промежуток времени в секундах с момента завершения задачи Проверка важных областей). |
| licenseExpirationDate | Дата окончания срока действия лицензии. Если добавлен активный и дополнительный ключ, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом. |
| currentApplicationUptime | Время работы Kaspersky Embedded Systems Security для Windows с момента его последнего запуска, в сотых долях секунды. |

## Счетчик обновлений

*Таблица 96. Счетчик обновлений*

| Счетчик | Определение |
|---|---|
| avBasesAge | "Возраст" баз (промежуток времени в сотых долях секунды с момента создания последних установленных обновлений баз) |

## Счетчики постоянной защиты файлов

*Таблица 97. Счетчики постоянной защиты файлов*

| Счетчик | Определение |
|---|---|
| totalObjectsProcessed | Общее количество проверенных объектов с момента последнего запуска задачи Постоянная защита файлов |
| totalInfectedObjectsFound | Общее количество обнаруженных зараженных и других объектов с момента последнего запуска задачи Постоянная защита файлов |
| totalSuspiciousObjectsFound | Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска задачи Постоянная защита файлов |
| totalVirusesFound | Общее количество обнаруженных объектов с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsQuarantined | Общее количество зараженных, возможно зараженных и прочих объектов, которые программа Kaspersky Embedded Systems Security для Windows поместила на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotQuarantined | Общее количество зараженных или возможно зараженных объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось поместить на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |

| Счетчик | Определение |
| --- | --- |
| totalObjectsDisinfected | Общее количество зараженных объектов, которые вылечила программа Kaspersky Embedded Systems Security для Windows; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotDisinfected | Общее количество зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось вылечить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsDeleted | Общее количество зараженных, возможно зараженных и прочих объектов, которые удалила программа Kaspersky Embedded Systems Security для Windows; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotDeleted | Общее количество зараженных, возможно зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось удалить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsBackedUp | Общее количество зараженных и прочих объектов, которые программа Kaspersky Embedded Systems Security для Windows поместила в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotBackedUp | Общее количество зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security для Windows не удалось поместить в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |

# SNMP-ловушки Kaspersky Embedded Systems Security для Windows и их параметры

В Kaspersky Embedded Systems Security для Windows предусмотрены следующие параметры SNMP-ловушек:

- eventThreatDetected: Обнаружен объект.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в резервном хранилище превысил значение, заданное параметром **Максимальный размер резервного хранилища (МБ)**. Kaspersky Embedded Systems Security для Windows продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: Достигнут порог свободного места в резервном хранилище. Объем свободного места в резервном хранилище меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Embedded Systems Security для Windows продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventQuarantineStorageSizeExceeds: Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, заданное параметром **Максимальный размер карантина (МБ)**. Kaspersky Embedded Systems Security для Windows продолжает помещать возможно зараженные объекты на карантин.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds: Достигнут порог свободного места в карантине. Объем свободного места в папке карантина меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Embedded Systems Security для Windows продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined: Ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason
- eventObjectNotBackuped: Ошибка сохранения копии объекта в резервное хранилище.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError: Внутренняя ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: Ошибка резервного хранилища.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: Базы программы устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated: Базы программы сильно устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted: программа Kaspersky Embedded Systems Security для Windows запущена.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown: программа Kaspersky Embedded Systems Security для Windows остановлена.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей давно не выполнялась. Количество дней с момента последнего завершения задачи Проверка важных областей.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: Срок действия лицензии истек.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: Ошибка выполнения задачи.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName
- eventUpdateError: Ошибка при выполнении задачи обновления.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

# Описания и возможные значения параметров SNMP-ловушек Kaspersky Embedded Systems Security для Windows

Ниже приведено описание и допустимые значения параметров ловушек:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.

  Параметр может принимать следующие значения:

  - critical (1) – критический;
  - warning (2) – предупреждение;
  - info (3) – информационный.
- userName: имя пользователя (например, имя пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя защищаемого устройства (например, имя защищаемого устройства, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

  Параметр может принимать следующие значения:

  - unknown (0) – функциональный компонент не определен;
  - quarantine (1) – Карантин;
  - backup (2) – Резервное хранилище;
  - reporting (3) – Журналы выполнения задач;
  - updates (4)– Обновление;
  - realTimeProtection (5) – Постоянная защита файлов;
  - onDemandScanning (6) – Проверка по требованию;
  - product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Embedded Systems Security для Windows в целом;
  - systemAudit (8) – Журнал системного аудита.
- eventReason: причина возникновения события.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Embedded Systems Security для Windows будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.
- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).
- threatName: имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название объекта, которое Kaspersky Embedded Systems Security для Windows возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.

- detectType: тип обнаруженного объекта.

  Параметр может принимать следующие значения:

  - undefined (0) – не определен;
  - virware – классические вирусы и сетевые черви;
  - trojware – троянские программы;
  - malware – прочие вредоносные программы;
  - adware – рекламные программы;
  - pornware – порнографические программы;
  - riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройству или личным данным.
- detectCertainty: степень уверенности обнаружения угрозы.

  Параметр может принимать следующие значения:

  - Suspicion (возможно зараженный) – программа Kaspersky Embedded Systems Security для Windows обнаружила частичное совпадение участка кода объекта с известным участком вредоносного кода.
  - Sure (зараженный) – программа Kaspersky Embedded Systems Security для Windows обнаружила полное совпадение участка кода объекта с известным участком вредоносного кода.
- days: количество дней (например, количество дней до окончания срока действия лицензии).
- errorCode: код ошибки.
- knowledgeBaseId: адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
- taskName: название задачи.
- updaterErrorEventReason: причина ошибки обновления.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonAccessDenied – доступ запрещен;
  - reasonUrlsExhausted – список источников обновлений исчерпан;
  - reasonInvalidConfig – неправильный файл конфигурации;
  - reasonInvalidSignature – неверная подпись;
  - reasonCantCreateFolder – невозможно создать папку;
  - reasonFileOperError – файловая ошибка;
  - reasonDataCorrupted – объект поврежден;
  - reasonConnectionReset – сброс соединения;
  - reasonTimeOut – истекло время ожидания при соединении;
  - reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;
  - reasonServerAuthError – ошибка проверки подлинности на сервере;

- reasonHostNotFound – устройство не найдено;
- reasonServerBusy – сервер недоступен;
- reasonConnectionError – ошибка соединения;
- reasonModuleNotFound – объект не найден;
- reasonBlstCheckFailed(16) – ошибка проверки списка запрещенных ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.

- storageObjectNotAddedEventReason: причина, по которой объект не был помещен в резервное хранилище или на карантин.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonStorageInternalError – ошибка базы данных; необходимо восстановление Kaspersky Embedded Systems Security для Windows.
  - reasonStorageReadOnly – база данных доступна только для чтения; необходимо восстановление Kaspersky Embedded Systems Security для Windows.
  - reasonStorageIOError – ошибка ввода-вывода: а) программа Kaspersky Embedded Systems Security для Windows повреждена и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Embedded Systems Security для Windows, поврежден.
  - reasonStorageCorrupted – хранилище повреждено; необходимо восстановление Kaspersky Embedded Systems Security для Windows.
  - reasonStorageFull – база данных заполнена; требуется свободное место на диске.
  - reasonStorageOpenError – не удается открыть файл базы данных; необходимо восстановление Kaspersky Embedded Systems Security для Windows.
  - reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Embedded Systems Security для Windows.
  - reasonObjectNotFound – помещаемый на карантин объект отсутствует на диске.
  - reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
  - reasonDiskOutOfSpace – недостаточно места на диске.

# Интеграция с WMI

Kaspersky Embedded Systems Security для Windows поддерживает интеграцию с инструментарием управления Windows (Windows Management Instrumentation, WMI): вы можете использовать клиентские системы, которые получают с помощью WMI данные по стандарту Web-Based Enterprise Management (WBEM), для получения данных о статусе программы Kaspersky Embedded Systems Security для Windows и ее компонентов.

В момент установки Kaspersky Embedded Systems Security для Windows регистрирует в системе собственный модуль для создания пространства имен Kaspersky Embedded Systems Security для Windows на защищаемом устройстве. Пространство имен Kaspersky Embedded Systems Security для Windows позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Embedded Systems Security для Windows.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

*Непериодические задачи* – это задачи программы, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения. Результаты выполнения таких задач фиксируются непрерывно в ходе выполнения и представляют собой отдельные события (например, обнаружение зараженного объекта одной из задач постоянной защиты компьютера). Задачами такого типа можно управлять с помощью политик Kaspersky Security Center.

*Периодические задачи* – это задачи программы, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде количества процентов. Результаты выполнения таких задач фиксируются по завершении задачи и представляют собой отдельный элемент или факт изменения состояния программы (например, завершение Обновления баз программы, сформированные конфигурационные файлы для задач автоматического формирования правил). На одном защищаемом устройстве одновременно может быть запущено несколько периодических задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять периодическими задачами с помощью групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из него динамические данные, вы сможете получить следующие данные о текущем состоянии программы.

*Таблица 98. Данные о состоянии программы*

| Свойство экземпляра класса | Описание | Значения |
|---|---|---|
| ProductName | Название установленной программы. | Полное название программы без номера версии. |
| ProductVersion | Полный номер версии установленной программы. | Полный номер версии программы, включая номер сборки. |
| InstalledPatches | Набор отображаемых имен установленных патчей. | Перечень критических исправлений, установленных для программы. |
| IsLicenseInstalled | Статус активации программы. | Статус ключа, с помощью которого активирована программа.<br>Возможные значения:<br>• False – В программе не добавлен лицензионный ключ.<br>• True - В программе добавлен лицензионный ключ. |
| LicenseDaysLeft | Количество дней до истечения срока действия текущей лицензии. | Количество дней, оставшихся до истечения срока действия текущей лицензии.<br>Возможные неположительные значения:<br>• 0 - Срок действия лицензии истек.<br>• -1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по причине нахождения в списке запрещенных ключей). |

| Свойство экземпляра класса | Описание | Значения |
|---|---|---|
| AVBasesDatetime | Временная отметка для текущей версии антивирусных баз. | Дата и время формирования антивирусных баз, используемых в текущий момент.<br>Если установленная программа не использует антивирусные базы, поле содержит значение Not installed. |
| IsExploitPreventionEnabled | Статус компонента Защита от эксплойтов. | Статус компонента Защита от эксплойтов.<br>Возможные значения:<br>• True - Компонент Защита от эксплойтов включен и выполняет функции защиты.<br>• False - Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение. |
| ProtectionTasksRunning | Набор запущенных задач защиты. | Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные непериодические задачи.<br>Если не запущена ни одна из непериодических задач, поле содержит значение "Нет". |
| IsAppControlRunning | Статус выполнения задачи Контроль запуска программ. | Статус выполнения задачи Контроль запуска программ.<br>• True - Задача Контроль запуска программ выполняется в текущий момент.<br>• False - Задача Контроль запуска программ не выполняется в текущий момент или компонент Контроль запуска программ не установлен. |
| AppControlMode | Режим работы задачи Контроль запуска программ. | Описание текущего состояния компонента Контроль запуска программ, а также выбранного режима соответствующей задачи.<br>Возможные значения:<br>• Active - в параметрах задачи указан режим **Активный**.<br>• Statistics Only - в параметрах задачи указан режим **Только статистика**.<br>• Not installed - Компонент Контроль запуска программ не установлен. |

| Свойство экземпляра класса | Описание | Значения |
|---|---|---|
| AppControlRulesNumber | Общее количество правил контроля запуска программ. | Количество правил, заданных в параметрах задачи Контроль запуска программ в текущий момент. |
| AppControlLastBlocking | Временная отметка последней блокировки запуска программы, выполненной задачей Контроль запуска программ в любом режиме. | Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима выполнения задачи.<br>Если на момент выполнения запроса WMI не зарегистрировано ни одного случая блокировки запуска программы, в поле отображается значение "Нет". |
| PeriodicTasksRunning | Набор запущенных периодических задач. | Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны отображаться все запущенные периодические задачи.<br>Если не запущена ни одна из периодических задач, поле содержит значение "Нет". |
| ConnectionState | Состояние соединения между компонентом Поставщик WMI и службой Kaspersky Security (KAVFS). | Информация о статусе соединения между компонентом Поставщик WMI и службой Kaspersky Security.<br>Возможные значения:<br>• Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы.<br>• Failed. Error Code: <code> - Соединение не удалось установить из-за ошибки с указанным кодом. |

Указанные данные являются свойствами экземпляра класса KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security для Windows, где:

- KasperskySecurity_ProductInfo – имя класса Kaspersky Embedded Systems Security для Windows;
- .ProductName=Kaspersky Embedded Systems Security для Windows – ключевые свойства Kaspersky Embedded Systems Security для Windows.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

kaspersky

# Работа с Kaspersky Embedded Systems Security для Windows из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security для Windows из командной строки.

## В этом разделе


Команды ..... 672

Коды возврата команд ..... 704


## Команды

Вы можете выполнять основные команды управления Kaspersky Embedded Systems Security для Windows из командной строки защищаемого устройства с помощью компонента Утилита командной строки, входящего в группу программных компонентов Kaspersky Embedded Systems Security для Windows.

С помощью командной строки можно управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Embedded Systems Security для Windows.

Некоторые из команд Kaspersky Embedded Systems Security для Windows выполняются в следующих режимах:

- Синхронный режим: управление возвращается на Консоль только после завершения выполнения команды.
- Асинхронный режим: управление возвращается на Консоль сразу после запуска команды.

► *Чтобы прервать выполнение команды в синхронном режиме,*

нажмите комбинацию клавиш **CTRL+C**.

При вводе команд Kaspersky Embedded Systems Security для Windows применяйте следующие правила:

- Вводите ключи и команды символами верхнего или нижнего регистра.
- Разделяйте ключи символом пробела.
- Если имя файла или папки содержит пробел, заключите путь к файлу или папке в кавычки, например: `"C:\TEST\test cpp.exe"`.
- При необходимости можно использовать подстановочные символы в масках имен файлов или путей, например: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

С помощью командной строки можно выполнять все операции по управлению и администрированию Kaspersky Embedded Systems Security для Windows (см. таблицу ниже).

*Таблица 99. Команды Kaspersky Embedded Systems Security для Windows*

| Команда | Описание |
|---|---|
| KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL" на стр. 687) | Обновляет список правил в соответствии с выбранным правилом импорта. |
| KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачей Контроль запуска программ: KAVSHELL APPCONTROL /CONFIG" на стр. 684) | Задает режим работы задачи Контроль запуска программ. |
| KAVSHELL APPCONTROL /GENERATE (см. раздел "Формирование правил контроля запуска программ: KAVSHELL APPCONTROL /GENERATE" на стр. 685) | Запускает задачу Формирование правил контроля запуска программ. |
| KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала Kaspersky Embedded Systems Security для Windows. KAVSHELL VACUUM" на стр. 697) | Дефрагментирует файлы журналов Kaspersky Embedded Systems Security для Windows. |
| KAVSHELL PASSWORD | Управляет параметрами защиты паролем. |
| KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Embedded Systems Security для Windows. KAVSHELL HELP" на стр. 675) | Отображает справку о командах Kaspersky Embedded Systems Security для Windows. |
| KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP" на стр. 675) | Запускает службу Kaspersky Security. |
| KAVSHELL STOP (см. раздел "Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP" на стр. 675) | Останавливает службу Kaspersky Security. |
| KAVSHELL SCAN (см. раздел "Проверка указанной области: KAVSHELL SCAN" на стр. 676) | Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами командной строки. |

| Команда | Описание |
| --- | --- |
| KAVSHELL SCANCRITICAL (см. раздел "Запуск задачи Проверка важных областей: KAVSHELL SCANCRITICAL" на стр. 680) | Запускает локальную системную задачу Проверка важных областей. |
| KAVSHELL TASK (см. раздел "Управление задачей в асинхронном режиме: KAVSHELL TASK" на стр. 681) | Запускает, приостанавливает, возобновляет, останавливает указанную задачу в асинхронном режиме. Возвращает текущее состояние задачи / статистику задачи. |
| KAVSHELL RTP (см. раздел "Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP" на стр. 683) | Запускает или останавливает все задачи постоянной защиты компьютера. |
| KAVSHELL UPDATE (см. раздел "Запуск задачи Обновление баз программы: KAVSHELL UPDATE" на стр. 689) | Запускает задачу Обновление баз программы с параметрами, заданными ключами командной строки. |
| KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Embedded Systems Security для Windows: KAVSHELL ROLLBACK" на стр. 692) | Откатывает базы программы до предыдущей версии. |
| KAVSHELL LICENSE (см. раздел "Активация программы. KAVSHELL LICENSE" на стр. 693) | Добавляет или удаляет ключи. Отображает информацию о добавленных ключах. |
| KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE" на стр. 694) | Включает или выключает трассировку. Управляет параметрами трассировки. |
| KAVSHELL DUMP (см. раздел "Включение и выключение создания файла дампа. KAVSHELL DUMP" на стр. 698) | Включает и выключает создание файлов дампов процессов Kaspersky Embedded Systems Security для Windows при их аварийном завершении. |
| KAVSHELL IMPORT (см. раздел "Импорт параметров. KAVSHELL IMPORT" на стр. 699) | Импортирует общие параметры Kaspersky Embedded Systems Security для Windows, а также параметры функций и задач из конфигурационного файла. |
| KAVSHELL EXPORT (см. раздел "Экспорт параметров. KAVSHELL EXPORT" на стр. 700) | Экспортирует все параметры Kaspersky Embedded Systems Security для Windows и существующих задач в конфигурационный файл. |

| Команда | Описание |
| --- | --- |
| KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL" на стр. 688) | Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления. |

## Вызов справки о командах Kaspersky Embedded Systems Security для Windows. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Embedded Systems Security для Windows, выполните одну из следующих команд:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Чтобы получить описание команды и ее синтаксис, выполните одну из следующих команд:

```
KAVSHELL HELP <команда>

KAVSHELL <команда> /?
```

**Примеры команды KAVSHELL HELP**

Чтобы просмотреть подробную информацию о команде KAVSHELL SCAN, выполните следующую команду:

```
KAVSHELL HELP SCAN
```

## Запуск и остановка службы Kaspersky Security KAVSHELL START: KAVSHELL STOP

Чтобы запустить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускается Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

## Проверка указанной области: KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого устройства, используйте команду KAVSHELL SCAN. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная с помощью команды KAVSHELL SCAN, является временной. Она отображается в Консоли программы только во время выполнения (в Консоли программы не отображаются ее параметры). Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи.

При указании путей в задачах проверки отдельных областей можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду KAVSHELL SCAN с правами этого пользователя.

Команда KAVSHELL SCAN выполняется в синхронном режиме.

Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду KAVSHELL TASK (см. раздел "Управление задачей в асинхронном режиме: KAVSHELL TASK" на стр. 681).

### Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<путь к файлу со
списком областей проверки>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"маски">] [/ES:<размер>] [/ET:<количество секунд>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<дни>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<путь к файлу
журнала выполнения задачи>] [/ANSI] [/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL SCAN есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

### Пример команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

*Таблица 100. Ключи / параметры команды KAVSHELL SCAN*

| Ключ / параметр | Описание |
|---|---|
| **Область проверки**. Обязательный параметр. | |
| <файлы><br><папки><br><сетевой путь> | Область проверки – список файлов, папок, сетевых путей и стандартных областей.<br>Указывайте сетевые пути к формате UNC (Universal Naming Convention).<br>В следующем примере папка Folder4 указана без пути к ней. Это значит, что она находится в папке, из которой вы запускаете команду KAVSHELL.<br>KAVSHELL SCAN Folder4<br>Если имя объекта, который вы хотите проверить, содержит пробелы, заключайте его в кавычки.<br>Kaspersky Embedded Systems Security для Windows проверит также все вложенные папки в выбранной папке.<br>Для проверки группы файлов вы можете использовать символы * или ?. |
| /MEMORY | Проверять объекты в оперативной памяти. |
| /SHARED | Проверять папки общего доступа на защищаемом устройстве. |
| /STARTUP | Проверять объекты автозапуска. |
| /REMDRIVES | Проверять съемные диски. |
| /FIXDRIVES | Проверять жесткие диски. |
| /MYCOMP | Проверять все области защищаемого устройства. |
| /L: <путь к файлу со списком областей проверки> | Полный путь к файлу со списком областей проверки.<br>Разделяйте области проверки в файле символом перевода строки. Вы можете указывать стандартные области проверки, как показано в следующем примере файла со списком областей проверки:<br>C:\<br>D:\Docs*.doc<br>E:\My Documents<br>/STARTUP<br>/SHARED |
| **Проверка объектов** (типы файлов). Если вы не укажете этот ключ, Kaspersky Embedded Systems Security для Windows будет проверять объекты по формату. | |
| /FA | Проверять все объекты |
| /FC | Проверять объекты по формату (по умолчанию). Kaspersky Embedded Systems Security для Windows проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам. |
| /FE | Проверять объекты по расширению. Kaspersky Embedded Systems Security для Windows проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам. |
| /NEWONLY | Проверять только новые и измененные файлы.<br>Если вы не укажете этот ключ, Kaspersky Embedded Systems Security для Windows будет проверять все объекты. |

| Ключ / параметр | Описание |
|---|---|
| **Действия над зараженными и другими обнаруженными объектами**. Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security для Windows будет выполнять действие **Пропускать**. | |
| DISINFECT | Лечить; если лечение невозможно, пропускать<br>Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для Windows для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Embedded Systems Security для Windows не будет обрабатывать возможно зараженные объекты. |
| DISINFDEL | Лечить; если лечение невозможно, удалять |
| DELETE | Удалять<br>Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для Windows для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Embedded Systems Security для Windows не будет обрабатывать возможно зараженные объекты. |
| REPORT | Отсылать отчет (по умолчанию) |
| AUTO | Выполнять рекомендованное действие |
| /AS: **Действия над возможно зараженными объектами** Если вы не укажете этот параметр, Kaspersky Embedded Systems Security для Windows будет выполнять действие **Пропускать**. | |
| QUARANTINE | Карантин |
| DELETE | Удалять |
| REPORT | Отсылать отчет (по умолчанию) |
| AUTO | Выполнять рекомендованное действие |
| **Исключения** | |
| /E:ABMSPO | Исключать составные объекты следующих типов:<br>A – SFX-архивы;<br>B – почтовые базы;<br>M – файлы почтовых форматов;<br>S – архивы (включая SFX-архивы);<br>P – упакованные объекты;<br>O – вложенные OLE-объекты. |
| /EM:<"`маски`"> | Исключать файлы по маске<br>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.<br>По умолчанию ограничений продолжительности нет. |

| Ключ / параметр | Описание |
|---|---|
| /ES:<размер> | Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанное значение.<br>По умолчанию Kaspersky Embedded Systems Security для Windows проверяет объекты любого размера. |
| /TZOFF | Отменить исключения доверенной зоны. |
| **Дополнительные параметры** (опции) | |
| /NOICHECKER | Выключить использование технологии iChecker (по умолчанию включено). |
| /NOISWIFT | Выключить использование технологии iSwift (по умолчанию включено). |
| /ANALYZERLEVEL:<уровень эвристического анализа> | Включить использование эвристического анализатора, настроить уровень анализа.<br>Доступны следующие уровни эвристического анализа:<br>1 – поверхностный;<br>2 – средний;<br>3 – глубокий.<br>Если вы опустите этот параметр, Kaspersky Embedded Systems Security для Windows не будет использовать эвристический анализатор. |
| /ALIAS:<альтернативное название задачи> | Присваивает задаче проверки по требованию временное название, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Embedded Systems Security для Windows.<br>Если этот параметр не задан, задаче присваивается временное название вида scan_<kavshell_pid>, например, scan_1234. В Консоли программы задаче присваивается название "Проверка объектов <дата и время>", например, "Проверка объектов 16.08.2007 17:13:14". |
| Параметры журнала выполнения задачи | |

| Ключ / параметр | Описание |
|---|---|
| /W:<имя файла журнала выполнения задачи> | Если указан этот параметр, Kaspersky Embedded Systems Security для Windows сохранит файл журнала выполнения задачи с именем, заданным значением параметра.<br>Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.<br>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий".<br>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле Журналы выполнения задач Консоли программы.<br>Если Kaspersky Embedded Systems Security для Windows не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке. |
| /ANSI | Этот параметр позволяет записывать события в журнал выполнения задачи в кодировке ANSI.<br>Параметр ANSI не будет применяться, если не задан параметр W.<br>Если параметр ANSI не указан, то журнал выполнения задачи формируется в кодировке UNICODE. |

## Запуск задачи Проверка важных областей: KAVSHELL SCANCRITICAL

Используйте команду `KAVSHELL SCANCRITICAL`, чтобы запустить задачу Проверка важных областей с параметрами, заданными в Консоли программы.

### Синтаксис команды KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<имя файла журнала выполнения задачи>]
```

### Примеры команды KAVSHELL SCANCRITICAL

Чтобы запустить задачу Проверка важных областей и сохранить журнал выполнения задачи в файле с именем scancritical.log в текущей папке, выполните следующую команду:

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

С помощью параметра /W можно настроить местоположение файла журнала выполнения задачи (см. таблицу ниже).

*Таблица 101. Синтаксис параметра /W команды KAVSHELL SCANCRITICAL*

| Ключ / параметр | Описание |
|---|---|
| /W:<имя файла журнала выполнения задачи> | Если указан этот параметр, Kaspersky Embedded Systems Security для Windows сохранит файл журнала выполнения задачи с именем, заданным значением параметра.<br>Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.<br>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий".<br>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле **Журналы выполнения задач** в Консоли программы.<br>Если Kaspersky Embedded Systems Security для Windows не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке. |

## Управление задачей в асинхронном режиме: KAVSHELL TASK

Команда KAVSHELL TASK позволяет управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

### Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное название задачи> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS>]
```

### Пример команды KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

```
KAVSHELL TASK network-attack-blocker /START
```

Команда `KAVSHELL TASK` может быть выполнена как без ключей/параметров, так и с использованием одного либо нескольких ключей/параметров (см. таблицу ниже).

*Таблица 102. Ключи / параметры команды KAVSHELL TASK*

| Ключ / параметр | Описание |
|---|---|
| Без параметров | Возвращает список всех существующих задач Kaspersky Embedded Systems Security для Windows. Список содержит следующие поля: альтернативное название задачи, категория задачи (системная или пользовательская) и текущий статус задачи. |
| <альтернативное название задачи> | Вместо названия задачи в команде SCAN TASK используйте ее альтернативное название – дополнительное сокращенное название, которое Kaspersky Embedded Systems Security для Windows присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Embedded Systems Security для Windows, введите команду KAVSHELL TASK без параметров. |
| /START | Запустить указанную задачу в асинхронном режиме |
| /STOP | Остановить указанную задачу |
| /PAUSE | Приостановить указанную задачу |
| /RESUME | Возобновить указанную задачу в асинхронном режиме |
| /STATE | Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*). |
| /STATISTICS | Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи |

Обратите внимание, что не все задачи Kaspersky Embedded Systems Security для Windows поддерживают ключи /PAUSE, /RESUME и /STATE.

Коды возврата команды KAVSHELL TASK (на стр. 706).

## Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG

Команда `KAVSHELL CONFIG` позволяет удалить атрибут защищенного процесса (Protected Process Light) у службы Kaspersky Security с помощью драйвера ELAM, установленного во время установки программы.

### Синтаксис команды KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

*Таблица 103. Ключи / параметры команды KAVSHELL CONFIG*

| Ключ / параметр | Описание |
|---|---|
| /PPL:OFF | Снять атрибут PPL со службы Kaspersky Security. |

## Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP

Команда `KAVSHELL RTP` позволяет запустить или остановить все задачи постоянной защиты компьютера.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

### Синтаксис команды KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

### Пример команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты компьютера, выполните следующую команду:

```
KAVSHELL RTP /START
```

Команда `KAVSHELL RTP` должна включать один из двух параметров (см. таблицу ниже).

*Таблица 104. Параметры команды KAVSHELL RTP*

| Ключ / параметр | Описание |
|---|---|
| /START | Запустить все задачи постоянной защиты компьютера: Постоянная защита файлов и Использование KSN. |
| /STOP | Остановить все задачи постоянной защиты компьютера. |

# Управление задачей Контроль запуска программ: KAVSHELL APPCONTROL /CONFIG

Команда `KAVSHELL APPCONTROL /CONFIG` позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

### Синтаксис команды KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<полный путь к XML файлу>
```

### Примеры команды KAVSHELL APPCONTROL /CONFIG

► *Чтобы запустить задачу Контроль запуска программ в режиме **Активный** без контроля загрузки DLL-модулей и сохранить параметры задачи по завершении, выполните следующую команду:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

*Таблица 105. `KAVSHELL APPCONTROL /CONFIG` command-line parameters/options*

| Ключ / параметр | Описание |
|---|---|
| `/mode:<applyrules\|statistics>` | Режим работы задачи Контроль запуска программ.<br>Вы можете выбрать один из следующих режимов работы задачи:<br>• active - применяются правила контроля запуска программ;<br>• statistics - только формировать статистику. |
| `/dll:<no\|yes>` | Выключить или включить контроль загрузки DLL-модулей. |
| `/savetofile: <полный путь к XML файлу>` | Экспортировать заданные правила в указанный файл в формате XML. |
| `/savetofile: <полное имя xml-файла>` | Сохранить список правил в файл. |
| `/savetofile: <полное имя xml-файла> /sdc` | Сохранить список правил контроля распространения программного обеспечения в файл. |
| `/clearsdc` | Удалить все правила контроля распространения программного обеспечения. |

# Формирование правил контроля запуска программ: KAVSHELL APPCONTROL /GENERATE

Команда `KAVSHELL APPCONTROL /GENERATE` позволяет формировать списки правил контроля запуска программ.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

### Синтаксис команды KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <путь к папке> | /source:<путь к файлу со списком папок> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<пользователь или группа пользователей>] [/export:<полный путь к XML файлу>] [/import:<a|r|m>] [/prefix:<префикс для названий правил>] [/unique]
```

### Примеры команды KAVSHELL APPCONTROL /GENERATE

► *Чтобы сформировать правила для файлов из указанных папок, выполните команду:*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

► *Чтобы сформировать правила для исполняемых файлов с любыми расширениями, хранящихся в указанной папке, и по завершении задачи сохранить сформированные правила в указанный XML-файл, выполните следующую команду:*

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c\rules\appctrlrules.xml
```

Вы можете использовать ключи/параметры для настройки автоматического формирования правил задачи Контроль запуска программ (см. таблицу ниже).

*Таблица 106. Ключи / параметры команды `KAVSHELL APPCONTROL /GENERATE`*

| Ключ / параметр | Описание |
|---|---|
| **Область применения разрешающих правил** | |
| <путь к папке> | Указать путь к папке с исполняемыми файлами, для которых будут автоматически формироваться разрешающие правила. |
| /source: <путь к файлу со списком папок> | Указать путь к TXT-файлу со списком папок, содержащих исполняемые файлы, для которых будут автоматически формироваться разрешающие правила. |

| | |
|---|---|
| /masks: <edms> | Указать расширения исполняемых файлов, для которых будут автоматически формироваться разрешающие правила.<br>В область применения правил можно включить файлы со следующими расширениями:<br>• e - файлы с расширением exe;<br>• d - файлы с расширением dll;<br>• m - файлы с расширением msi;<br>• s - скрипты. |
| /runapp | Учитывать при формировании разрешающих правил программы, запущенные на защищаемом устройстве в текущий момент. |
| **Действия при автоматическом формировании разрешающих правил** | |
| /rules: <ch\|cp\|h> | Указать действия при формировании разрешающих правил для задачи Контроль запуска программ:<br>• ch – использовать цифровой сертификат. Если сертификат отсутствует, использовать SHA256-хеш.<br>• cp — использовать цифровой сертификат. Если сертификат отсутствует, использовать путь к исполняемому файлу.<br>• h – использовать SHA256-хеш. |
| /strong | Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании разрешающих правил для задачи Контроль запуска программ. Команда выполняется, если задано значение ключа /rules: <ch\|cp>. |
| /user: <пользователь или группа пользователей> | Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или группой. |
| **Действия по завершении выполнения задачи Формирование правил контроля запуска программ** | |
| /export: <полный путь к XML файлу> | Сохранить сформированные правила в XML-файл. |
| /unique | Добавлять информацию о защищаемом устройстве, по программам которого формируются разрешающие правила контроля запуска программ. |
| /prefix: <префикс для названий правил> | Указать префикс названий разрешающих правил контроля запуска программ. |

| | |
|---|---|
| /import: <a\|r\|m> | Импортировать сформированные правила в указанный список правил контроля запуска программ в соответствии с выбранным принципом добавления новых правил:<br>• a – **Добавить правила к существующим** (одинаковые правила дублируются);<br>• r – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален);<br>• m – **Объединить правила с существующими** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален). |

## Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL

Команда `KAVSHELL APPCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль запуска программ в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

### Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

### Пример команды KAVSHELL APPCONTROL

► *Чтобы добавить к имеющимся правилам контроля запуска программ правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля запуска программ (см. таблицу ниже).

*Таблица 107. Ключи / параметры команды KAVSHELL APPCONTROL*

| Ключ / параметр | Описание |
|---|---|
| /append <полный путь к XML файлу> | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются). |
| /replace <полный путь к XML файлу> | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален). |
| /merge <полный путь к XML файлу> | Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила). |
| /clear | Очистить список правил контроля запуска программ. |

## Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL

Команда `KAVSHELL DEVCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль устройств в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

### Синтаксис команды KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

### Пример команды KAVSHELL DEVCONTROL

► *Чтобы добавить к имеющимся правилам контроля устройств правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля устройств (см. таблицу ниже).

*Таблица 108. Ключи / параметры команды KAVSHELL DEVCONTROL*

| Ключ | Описание |
|---|---|
| /append <полный путь к XML файлу> | Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются). |
| /replace <полный путь к XML файлу> | Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален). |
| /merge <полный путь к XML файлу> | Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила). |
| /clear | Очистить список правил контроля устройств. |

## Запуск задачи Обновление баз программы: KAVSHELL UPDATE

Команда KAVSHELL UPDATE позволяет запускать задачу обновления баз Kaspersky Embedded Systems Security для Windows в синхронном режиме.

Задача Обновление баз программы, запущенная с помощью команды KAVSHELL UPDATE, является временной. Она отображается в Консоли программы только во время ее выполнения. Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, и к задачам обновления, созданным в Консоли программы, могут применяться политики Kaspersky Security Center. Сведения об использовании Kaspersky Security Center для управления Kaspersky Embedded Systems Security для Windows на защищаемых устройствах приведены в разделе "Управление Kaspersky Embedded Systems Security для Windows с помощью Kaspersky Security Center".

Чтобы указать путь к источнику обновлений в этой задаче, можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду KAVSHELL UPDATE с правами этого пользователя.

### Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE < Путь к источнику обновления | /AK | /KL > [/NOUSEKL]
[/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>]
[/PROXYPWD:<пароль>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
[/REG:<код iso3166>] [/W:<имя файла журнала выполнения задачи>]
[/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL UPDATE есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

**Пример команды KAVSHELL UPDATE**

► *Чтобы запустить пользовательскую задачу Обновление баз программы, выполните следующую команду:*

```
KAVSHELL UPDATE
```

► *Чтобы запустить задачу Обновление баз программы, файлы обновлений для которой хранятся в сетевой папке \\server\databases, выполните следующую команду:*

```
KAVSHELL UPDATE \\server\bases
```

► *Чтобы запустить задачу Обновление баз программы с FTP-сервера ftp://dnl-ru1.kaspersky-labs.com/ и записать все события задачи в файл c:\update_report.log, выполните следующую команду:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *Чтобы загрузить обновления баз Kaspersky Embedded Systems Security для Windows с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений с помощью прокси-сервера (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к защищаемому устройству с помощью встроенной в Windows проверки подлинности NTLM с именем пользователя netuser и паролем 123456, выполните следующую команду:*

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

*Таблица 109. Ключи / параметры команды KAVSHELL UPDATE*

| Ключ / параметр | Описание |
|---|---|
| **Источник обновлений** (обязательный параметр). Укажите один или несколько источников. Kaspersky Embedded Systems Security для Windows будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела. | |
| <путь в формате UNC> | Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC. |
| <URL> | Пользовательские источники обновления. Адрес HTTP- или FTP-сервера, на котором располагается папка с обновлениями. |
| <Локальная папка> | Пользовательские источники обновления. Папка на защищаемом устройстве. |
| /AK | Использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений. |
| /KL | Использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. |
| /NOUSEKL | Не использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны (по умолчанию). |
| **Параметры прокси-сервера** | |

| Ключ / параметр | Описание |
|---|---|
| /PROXY:<адрес>:<порт> | Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот параметр, Kaspersky Embedded Systems Security для Windows будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети. |
| /AUTHTYPE:<0-2> | Этот параметр задает метод аутентификации для доступа к прокси-серверу. Он может принимать следующие значения:<br>**0** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Embedded Systems Security обращается к прокси-серверу с использованием учетной записи **Локальная система** (**SYSTEM**).<br>**1** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Embedded Systems Security обращается к прокси-серверу с использованием учетной записи, имя пользователя и пароль которой заданы параметрами /PROXYUSER и /PROXYPWD.<br>**2** – обычная проверка подлинности по имени пользователя и паролю, заданным параметрами /PROXYUSER и /PROXYPWD.<br>Если для доступа к прокси-серверу не требуется аутентификация, можно не указывать этот параметр. |
| /PROXYUSER:<имя пользователя> | Имя пользователя, используемое для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. |
| /PROXYPWD:<пароль> | Пароль пользователя, используемый для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если указан параметр /PROXYUSER, но не указан параметр /PROXYPWD, считается, что задан пустой пароль. |
| /NOPROXYFORKL | Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию). |
| /USEPROXYFORCUSTOM | Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используется). |
| /USEPROXYFORLOCAL | Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать прокси-сервер для локальных адресов**. |
| **Общие параметры FTP- и HTTP-сервера** | |
| /NOFTPPASSIVE | Если указан этот ключ, Kaspersky Embedded Systems Security для Windows использует активный режим FTP-сервера для соединения с защищаемым устройством. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security для Windows использует пассивный режим FTP-сервера, при возможности. |
| /TIMEOUT:<количество секунд> | Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот параметр, Kaspersky Embedded Systems Security для Windows использует значение по умолчанию: 10 секунд. Значение параметра должно быть целым числом. |

| Ключ / параметр | Описание |
|---|---|
| /REG:<код iso3166> | Региональные параметры. Этот параметр используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Embedded Systems Security для Windows минимизирует нагрузку на защищаемое устройство, выбирая ближайший к нему сервер обновлений.<br>Значение этого параметра должно быть двухбуквенным кодом страны, в которой расположено защищаемое устройство, в стандарте ISO 3166-1, например: /REG: gr или /REG:US. Если ключ не указан или указан недопустимый код страны, Kaspersky Embedded Systems Security для Windows распознает местоположение защищаемого устройства в соответствии с региональными параметрами защищаемого устройства, на котором установлена Консоль программы. |
| /ALIAS:<альтернативное название задачи> | Этот параметр позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Embedded Systems Security для Windows.<br>Если этот ключ не задан, задаче присваивается временное название вида update_<kavshell_pid>, например, update_1234. В Консоли программы задаче присваивается название "Обновление баз программы <дата и время>", например: "Обновление баз программы 16.08.2007 17:41:02". |
| /W:<имя файла журнала выполнения задачи> | Если указан этот параметр, Kaspersky Embedded Systems Security для Windows сохранит файл журнала выполнения задачи с именем, заданным значением параметра.<br>Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи.<br>В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security для Windows в оснастке "Просмотр событий".<br>Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле **Журналы выполнения задач** в Консоли программы.<br>Если Kaspersky Embedded Systems Security для Windows не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке. |

Коды возврата команды KAVSHELL UPDATE (на стр. 707).

## Откат обновления баз Kaspersky Embedded Systems Security для Windows: KAVSHELL ROLLBACK

Команда `KAVSHELL ROLLBACK` позволяет выполнить локальную системную задачу Откат обновления баз программы – откатить базы Kaspersky Embedded Systems Security для Windows до предыдущей установленной версии. Команда выполняется синхронно.

**Синтаксис команды**

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK (на стр. 707).

## Управление анализом журналов: KAVSHELL TASK LOG-INSPECTOR

Команда `KAVSHELL TASK LOG-INSPECTOR` позволяет осуществлять контроль целостности среды, основываясь на анализе журнала событий Windows.

**Синтаксис команды**

```
KAVSHELL TASK LOG-INSPECTOR
```

**Пример команды**

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

*Таблица 110. Ключи / параметры команды KAVSHELL TASK LOG-INSPECTOR*

| Ключ / параметр | Описание |
|---|---|
| /START | Запустить указанную задачу в асинхронном режиме |
| /STOP | Остановить указанную задачу |
| /STATE | Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*) |
| /STATISTICS | Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи. |

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR (на стр. 705).

## Активация программы. KAVSHELL LICENSE

Команда `KAVSHELL LICENSE` позволяет управлять ключами и кодами активации Kaspersky Embedded Systems Security для Windows.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

**Синтаксис команды KAVSHELL LICENSE**

```
KAVSHELL LICENSE [/ADD:<файл ключа | код активации> [/R] | /DEL:<ключ | код активации>]
```

**Примеры команды KAVSHELL LICENSE**

► *Чтобы активировать программу, выполните команду:*

```
KAVSHELL.EXE LICENSE / ADD: <код активации или файл ключа>
```

► *Чтобы получить информацию о добавленных ключах, выполните команду:*

```
KAVSHELL LICENSE
```

► *Чтобы удалить добавленный ключ с номером 0000-000000-00000001, выполните команду:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Команда `KAVSHELL LICENSE` может быть выполнена как без ключей, так и с их использованием (см. таблицу ниже).

*Таблица 111. Ключи / параметры команды KAVSHELL LICENSE*

| Параметр | Описание |
|---|---|
| Без ключей | Команда возвращает следующую информацию о добавленных ключах:<br>• Ключ.<br>• Тип лицензии (коммерческая).<br>• Срок действия связанной с ключом лицензии.<br>• Статус ключа (активный или дополнительный). Если значение статуса *, ключ добавлен в качестве дополнительного. |
| /ADD:<имя файла ключа или код активации> | Добавить ключ с помощью указанного файла или кода активации.<br>Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |
| /R | Код активации или ключ /R является дополнительным к коду активации или ключу /ADD и указывает, что код активации или ключ добавляется в качестве дополнительного. |
| /DEL:<ключ или код активации> | Удалить указанный ключ или код активации. |

Коды возврата команды KAVSHELL LICENSE (на стр. 708).

## Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE

Команда `KAVSHELL TRACE` позволяет включать или выключать ведение журнала трассировки всех подсистем Kaspersky Embedded Systems Security для Windows, а также устанавливать уровень детализации информации в журнале.

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

### Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<путь к папке с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] [/r:<максимальное количество файлов трассировки для ротации>] | /OFF>
```

Если ведется журнал трассировки и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом /ON и с помощью ключей /S и /LVL задайте параметры журнала трассировки (см. таблицу ниже).

*Таблица 112. Ключи / параметры команды KAVSHELL TRACE*

| Ключ | Описание |
|---|---|
| `/ON` | Включить ведение журнала трассировки. |
| `/F:<папка с файлами журнала трассировки>` | Этот параметр указывает полный путь к папке, в которую будут сохранены файлы журнала трассировки (обязательный).<br>Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Пути к папкам на сетевых дисках других защищаемых устройств указывать нельзя.<br>Если указанный параметром путь содержит пробел, заключите его в кавычки, например: /F:"C:\Trace Folder".<br>Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |
| `/S: <максимальный размер файла журнала в мегабайтах>` | Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Embedded Systems Security для Windows начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.<br>Если значение этого параметра не указано, максимальный размер одного файла журнала составит 50 МБ. |

| Ключ | Описание |
|---|---|
| /LVL:debug\|info\|warning\|error\|critical | Этот параметр устанавливает уровень детализации журнала от максимального (**Вся отладочная информация**), при котором в журнал записываются все события, до минимального (**Критические события**), при котором в журнал записываются только критические события.<br>Если значение этого параметра не указано, в журнал трассировки будут записываться все события с уровнем детализации **Вся отладочная информация**. |
| /r:<максимальное количество файлов трассировки для ротации> | Этот параметр включает ротацию файлов трассировки. Если включена ротация файлов трассировки и достигнуто <максимальное количество файлов трассировки для ротации>, перед созданием нового файла самый старый файл удаляется.<br><br>Доступные значения: от 1 до 999. Если значение не указано, ротация файлов трассировки не включается и программа возвращает ошибку. |
| /OFF | Этот параметр выключает ведение журнала трассировки. |

**Пример команды KAVSHELL TRACE**

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Вся отладочная информация** и максимальным размером файла журнала 200 МБ и сохранить файл журнала в папке C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Важные события** и сохранить файл журнала в папку C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Чтобы включить журнал трассировки с использованием уровня детализации **Важные события**, сохранить файл журнала в папку C:\Trace Folder и включить ротацию файлов трассировки при достижении предельного количества 50 файлов, выполните следующую команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

► *Чтобы выключить ведение журнала трассировки, выполните команду:*

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE (на стр. 708).

## Дефрагментация файлов журнала Kaspersky Embedded Systems Security для Windows. KAVSHELL VACUUM

Команда `KAVSHELL VACUUM` позволяет выполнить дефрагментацию файлов журнала программы. Это помогает избежать системных ошибок и ошибок программы из-за хранения большого количества файлов журнала, сформированных на основе событий программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Рекомендуется применять команду `KAVSHELL VACUUM` для оптимизации хранения файлов журналов в случае частых запусков задач проверки по требованию и задач обновления. При выполнении команды Kaspersky Embedded Systems Security для Windows обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом устройстве по указанному пути.

По умолчанию файлы журнала программы сохраняются в папку C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security для Windows\3.3\Reports. Если вы вручную указали другой путь для хранения файлов журнала, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журнала Kaspersky Embedded Systems Security для Windows.

Файлы большого размера увеличивают время, необходимое команде `KAVSHELL VACUUM` на выполнение дефрагментации.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля компьютера. Процедура дефрагментации блокирует доступ к журналу Kaspersky Embedded Systems Security для Windows и запрещает запись событий в журнал. Чтобы избежать снижения защиты, рекомендуется планировать запуск команды `KAVSHELL VACUUM`.

► *Чтобы выполнить дефрагментацию файлов журнала Kaspersky Embedded Systems Security для Windows, выполните команду:*

```
KAVSHELL VACUUM
```

Для выполнения команды необходимы права учетной записи Локальная система (Local System).

## Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security для Windows использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Embedded Systems Security для Windows создает файлы klamfb.dat и klamfb2.dat в папке %SYSTEMDRIVE%\System Volume Information. Эти файлы содержат информацию о проверенных незараженных объектах. Размер файла klamfb.dat (klamfb2.dat) увеличивается пропорционально количеству файлов, проверенных Kaspersky Embedded Systems Security для Windows. В этом файле хранится только актуальная информация о существующих в системе файлах: если файл был удален, то Kaspersky Embedded Systems Security для Windows удаляет информацию о нем из файла klamfb.dat.

Для очистки данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла klamfb.dat с помощью команды KAVSHELL FBRESET, Kaspersky Embedded Systems Security для Windows не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Embedded Systems Security для Windows может увеличить нагрузку на защищаемое устройство. При этом после очистки файла klamfb.dat Kaspersky Embedded Systems Security для Windows проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Embedded Systems Security для Windows заново добавляет информацию о каждом проверенном объекте в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не проверять файл повторно, если он не был изменен.

Для выполнения команды `KAVSHELL FBRESET` нужно запускать интерпретатор командной строки с правами учетной записи SYSTEM.

## Включение и выключение создания файла дампа. KAVSHELL DUMP

Команда `KAVSHELL DUMP` позволяет включать и выключать создание образов памяти (файлов дампов) процессов Kaspersky Embedded Systems Security для Windows при их аварийном завершении (см. таблицу ниже). Кроме того, можно в любой момент создать файл дампа для выполняющихся процессов Kaspersky Embedded Systems Security для Windows.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена с правами учетной записи локальной системы (SYSTEM).

Kaspersky Embedded Systems Security для Windows записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.
Команда KAVSHELL DUMP не используется для 64-разрядных процессов.

**Синтаксис команды KAVSHELL DUMP**

```
KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом дампа>
/ P:<pid> | /OFF>
```

*Таблица 113. Ключи / параметры команды KAVSHELL DUMP*

| Ключ | Описание |
|---|---|
| /ON | Включить создание файла дампа при аварийном завершении процесса. |
| /F:<папка с файлами дампов> | Это обязательный параметр. Указывает путь к папке, в которой будет сохранен файл дампа. Нельзя указывать пути к папкам на сетевых дисках других незащищенных устройств.<br>При указании пути к папке с файлом дампа можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя. |
| /SNAPSHOT | Снимает образ памяти выполняющегося процесса с указанным идентификатором и сохраняет файл дампа в папку, указанную параметром /F. |
| /P | Идентификатор процесса (PID); отображается в Диспетчере задач Microsoft Windows. |
| /OFF | Выключить создание файла дампа при аварийном завершении процесса. |

Коды возврата команды KAVSHELL DUMP (на стр. 709).

**Пример команды KAVSHELL DUMP**

► *Чтобы включить создание файла дампа и сохранить файл дампа в папку C:\Dump Folder, выполните команду:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Чтобы снять образ памяти процесса с идентификатором 1234 в папку C:/Dumps, выполните команду:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

► *Чтобы выключить создание файлов дампа, выполните команду:*

```
KAVSHELL DUMP /OFF
```

## Импорт параметров. KAVSHELL IMPORT

Команда `KAVSHELL IMPORT` позволяет импортировать параметры Kaspersky Embedded Systems Security для Windows и текущих задач программы из конфигурационного файла в Kaspersky Embedded Systems Security для Windows на защищаемом устройстве. Вы можете создать конфигурационный файл с помощью команды `KAVSHELL EXPORT`.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

**Синтаксис команды KAVSHELL IMPORT**

```
KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>
```

**Пример команды KAVSHELL IMPORT**

```
KAVSHELL IMPORT Host1.xml
```

*Таблица 114. Параметр команды KAVSHELL IMPORT*

| Параметр | Описание |
|---|---|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, из которого будут импортированы параметры.<br>Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |

Коды возврата команды KAVSHELL IMPORT (на стр. 709).

## Экспорт параметров. KAVSHELL EXPORT

Команда KAVSHELL EXPORT позволяет экспортировать все параметры Kaspersky Embedded Systems Security для Windows и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Embedded Systems Security для Windows на других защищаемых устройствах.

**Синтаксис команды KAVSHELL EXPORT**

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

**Пример команды KAVSHELL EXPORT**

```
KAVSHELL EXPORT Host1.xml
```

*Таблица 115. Параметр команды KAVSHELL EXPORT*

| Параметр | Описание |
|---|---|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, в котором будут сохранены параметры.<br>Конфигурационному файлу можно присвоить любое расширение.<br>Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |

Коды возврата команды KAVSHELL EXPORT (на стр. 710).

# Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

Команда KAVSHELL OMSINFO позволяет просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами. Информация об угрозах поступает из доступных журналов событий.

### Синтаксис команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <полный путь к сформированному файлу с именем файла>
```

### Пример команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

*Таблица 116. Параметр команды KAVSHELL OMSINFO*

| Параметр | Описание |
|---|---|
| <путь к сформированному файлу с именем файла> | Имя сформированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах. |

# Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE

Команда `KAVSHELL FIM /BASELINE` позволяет настраивать режим работы задачи Мониторинг целостности файлов на основе эталона и контролировать загрузку DLL-модулей.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

### Синтаксис команды KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<область мониторинга> | /L:<путь к TXT-файлу
со списком областей мониторинга>] [/MD5 | /SHA256] [/SF]] | [/CLEAR
[/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/EXPORT:<путь
к TXT-файлу> [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] |
[/SHOW [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SCAN
[/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] |
[/PWD:<пароль>]
```

### Примеры команды KAVSHELL FIM /BASELINE

► *Чтобы удалить эталон, выполните следующую команду:*

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<идентификатор эталона>
```

Вы можете настраивать параметры задачи Мониторинг целостности файлов на основе эталона с помощью параметров командной строки (см. таблицу ниже).

*Таблица 117. Ключи / параметры команды KAVSHELL FIM/ BASELINE*

| Ключ / параметр | Описание |
|---|---|
| /CREATE | Создать задачу Мониторинг целостности файлов на основе эталона.<br>Kaspersky Embedded Systems Security для Windows запустит новую задачу Мониторинг целостности файлов на основе эталона, чтобы создать эталон. |
| /L | Укажите путь к TXT-файлу, содержащему список областей мониторинга. |
| /MD5 | Укажите алгоритм MD5 для расчета контрольной суммы (необязательный параметр).<br>Параметр /MD5 не используется совместно с параметром /SHA256.<br>Алгоритм MD5 используется по умолчанию. |
| /SHA256 | Укажите алгоритм SHA256 для расчета контрольной суммы (необязательный параметр).<br>Параметр /SHA256 не используется совместно с параметром /MD5.<br>Алгоритм MD5 используется по умолчанию. |
| /SF | Включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона (необязательный параметр).<br>По умолчанию вложенные папки не входят в область задачи Мониторинг целостности файлов на основе эталона. |
| /CLEAR | Удалить эталон с указанным <идентификатором эталона> или эталон задачи с указанным <существующим названием>.<br>Удалить все эталоны, если не указан ни один из параметров <идентификатор эталона> или <существующее название>.<br>Необязательный параметр. |
| /BL | Укажите уникальный идентификатор эталона (необязательный параметр). |
| /EXPORT | Экспортировать данные всех эталонов в TXT-файл. |
| /SHOW | Показать данные всех эталонов. |
| /SCAN | Запустить новую задачу Мониторинг целостности файлов на основе эталона с указанным <идентификатором эталона> или <существующим названием>. |
| /ALIAS | Укажите название новой или существующей задачи. |

| | |
|---|---|
| <область мониторинга> | Укажите файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.<br>Этот параметр позволяет указать только одну область. |
| <путь к TXT-файлу со списком областей мониторинга> | Укажите путь к TXT-файлу, содержащему список областей мониторинга.<br>Файл должен быть в кодировке UTF-8, а путь к каждой области мониторинга необходимо указывать на отдельной строке. |
| <путь к TXT-файлу> | Укажите путь к файлу, в который вы хотите экспортировать данные всех эталонов. |
| <идентификатор эталона> | Укажите уникальный идентификатор эталона.<br>Чтобы просмотреть идентификатор эталона, используйте параметр /SHOW. |
| <существующее название> | Укажите название существующей задачи. |
| <новое название> | Укажите название новой задачи. |

kaspersky

# Коды возврата команд

## В этом разделе


Коды возврата команд KAVSHELL START и KAVSHELL STOP ..... 704
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL ..... 705
Коды возврата команды KAVSHELL TASK LOG-INSPECTOR ..... 705
Коды возврата команды KAVSHELL TASK ..... 706
Коды возврата команды KAVSHELL RTP ..... 706
Коды возврата команды KAVSHELL UPDATE ..... 707
Коды возврата команды KAVSHELL ROLLBACK ..... 707
Коды возврата команды KAVSHELL LICENSE ..... 708
Коды возврата команды KAVSHELL TRACE ..... 708
Коды возврата команды KAVSHELL FBRESET ..... 709
Коды возврата команды KAVSHELL DUMP ..... 709
Коды возврата команды KAVSHELL IMPORT ..... 709
Коды возврата команды KAVSHELL EXPORT ..... 710
Коды возврата команды KAVSHELL FIM /BASELINE ..... 710


## Коды возврата команд KAVSHELL START и KAVSHELL STOP

*Таблица 118. Коды возврата команд KAVSHELL START и KAVSHELL STOP*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -3 | Ошибка прав доступа |
| -5 | Неверный синтаксис команды |
| -6 | Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена) |
| -7 | Служба не зарегистрирована |
| -8 | Автоматический запуск службы отключен |
| -9 | Неудачная попытка запустить управляемое устройство под другой учетной записью (по умолчанию служба Kaspersky Security работает под учетной записью Локальная система). |
| -99 | Неизвестная ошибка |

## Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

*Таблица 119. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно (Угроз не обнаружено) |
| 1 | Операция отменена |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (не найден файл со списком областей проверки) |
| -5 | Неверный синтаксис команды или не определена область проверки |
| -80 | Зараженных и других обнаруживаемых объектов |
| -81 | Возможно зараженных объектов |
| -82 | Обнаружены ошибки обработки |
| -83 | Обнаружены непроверенные объекты |
| -84 | Обнаружены поврежденные объекты |
| -85 | Не удалось создать журнал выполнения задачи |
| -99 | Неизвестная ошибка |
| -301 | Недействительный ключ |

## Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

*Таблица 120. Коды возврата команды KAVSHELL TASK LOG-INSPECTOR*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -6 | Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена) |
| 402 | Задача уже запущена (для параметра /STATE) |

## Коды возврата команды KAVSHELL TASK

*Таблица 121. Коды возврата команды KAVSHELL TASK*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (задача не найдена) |
| -5 | Неверный синтаксис команды |
| -6 | Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена) |
| -99 | Неизвестная ошибка |
| -301 | Недействительный ключ |
| 401 | Задача не запущена (для параметра /STATE) |
| 402 | Задача уже запущена (для параметра /STATE) |
| 403 | Задача уже приостановлена (для параметра /STATE) |
| -404 | Сбой выполнения операции (изменение состояния задачи привело ее к сбою) |

## Коды возврата команды KAVSHELL RTP

*Таблица 122. Коды возврата команды KAVSHELL RTP*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (не найдена одна или все задачи постоянной защиты компьютера) |
| -5 | Неверный синтаксис команды |
| -6 | Неверная операция (например, задача уже запущена или уже остановлена) |
| -99 | Неизвестная ошибка |
| -301 | Недействительный ключ |

## Коды возврата команды KAVSHELL UPDATE

*Таблица 123. 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 Embedded Systems Security для Windows не прошел проверку подлинности при соединении с источником обновлений |
| -236 | Базы программы повреждены |
| -301 | Недействительный ключ |

## Коды возврата команды KAVSHELL ROLLBACK

*Таблица 124. 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 125. 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 126. Коды возврата команды KAVSHELL TRACE*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (не найден путь к папке с файлами журнала трассировки) |
| -5 | Неверный синтаксис команды |
| -6 | Недопустимая операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено) |
| -99 | Неизвестная ошибка |

## Коды возврата команды KAVSHELL FBRESET

*Таблица 127. Коды возврата команды KAVSHELL FBRESET*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -99 | Неизвестная ошибка |

## Коды возврата команды KAVSHELL DUMP

*Таблица 128. Коды возврата команды KAVSHELL DUMP*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (не найден путь к папке с файлом дампа; не найден процесс с указанным идентификатором) |
| -5 | Неверный синтаксис команды |
| -6 | Неверная операция (попытка выполнения команды KAVSHELL DUMP /OFF, если создание файла дампа уже выключено) |
| -99 | Неизвестная ошибка |

## Коды возврата команды KAVSHELL IMPORT

*Таблица 129. Коды возврата команды KAVSHELL IMPORT*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (не удается найти конфигурационный файл для импорта) |
| -5 | Неверный синтаксис |
| -99 | Неизвестная ошибка |

| Код возврата | Описание |
|---|---|
| 501 | Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Embedded Systems Security для Windows не импортировала параметры некоторых функциональных компонентов) |
| -502 | Файл импорта отсутствует или имеет неизвестный формат |
| -503 | Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Embedded Systems Security для Windows более поздней или несовместимой версии) |

## Коды возврата команды KAVSHELL EXPORT

*Таблица 130. Коды возврата команды KAVSHELL EXPORT*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -5 | Неверный синтаксис |
| -10 | Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу) |
| -99 | Неизвестная ошибка |
| 501 | Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Embedded Systems Security для Windows не экспортировала параметры некоторых функциональных компонентов) |

## Коды возврата команды KAVSHELL FIM /BASELINE

*Таблица 131. Коды возврата команды KAVSHELL FIM /BASELINE*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -2 | Служба не запущена |
| -3 | Ошибка прав доступа |
| -4 | Объект не найден (задача не найдена) |

| Код возврата | Описание |
|---|---|
| -5 | Неверный синтаксис команды |
| -6 | Неверная операция (например, эталон был удален) |
| -10 | Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу) |
| -12 | Неверный пароль |
| -80 | Не соответствует удаленным эталонным объектам |
| -85 | Не удалось создать журнал выполнения задачи |
| -99 | Внутренняя ошибка |
| -303 | Недопустимый лицензионный ключ |
| -502 | Задача не запущена |
| 200 | Все объекты соответствуют эталону |
| 501 | Задача завершена успешно с ошибкой / комментарием |

# Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## В этом разделе


Способы получения технической поддержки ..... 712

Техническая поддержка через Kaspersky CompanyAccount ..... 712

Использование файла трассировки и скрипта AVZ ..... 713


## Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Поддержка программы предоставляется в течение ее жизненного цикла (см. страницу жизненного цикла программ https://support.kaspersky.com/corporate/lifecycle).
Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки, отправив запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

## Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Дополнительная информация о Kaspersky CompanyAccount приведена на веб-сайте Службы технической поддержки http://support.kaspersky.ru/faq/companyaccount_help.

# Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Embedded Systems Security для Windows и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять защищаемое устройство на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки системы.

kaspersky

# Глоссарий

## K

### Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## O

### OLE-объект

Объект, который присоединен к другому файлу или встроен в другой файл с использованием технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel, встроенная в документ Microsoft Office Word.

## S

### SIEM

Аббревиатура от Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

## A

### Активный ключ

Ключ, используемый в текущий момент для работы приложения.

### Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

### Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

# З

## Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

## Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

# К

## Карантин

Папка, в которую приложение "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

# Л

## Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

## Ложное срабатывание

Ситуация, когда незараженный объект определяется приложением "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

## Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

# М

## Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

# Н

## Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

# О

## Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

## Объекты автозапуска

Набор приложений, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

# П

## Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

## Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

# Р

## Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

# С

## Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

## Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

### Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

## У

### Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

### Уровень важности события

Характеристика события, зафиксированного в работе приложения "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

### Уязвимость

Недостаток в операционной системе или приложении, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или приложение и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных приложений.

## 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).

# Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Domino, Lotus и Lotus Notes – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, PowerShell, Outlook, SharePoint, SQL Server, Windows, Windows Server, Windows Vista, Windows XP являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.