KASPERSKY lab

Kaspersky Embedded Systems Security

Руководство пользователя

Версия программы: 2.1

Уважаемый пользователь!

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

Дата редакции документа: 28.03.2018

http://www.kaspersky.ru

http://support.kaspersky.ru

Содержание

Об этом руководстве

Руководство пользователя Kaspersky Embedded Systems Security 2.1 адресовано специалистам, которые осуществляют администрирование Консоли Kaspersky Embedded Systems Security 2.1 на защищаемом устройстве.

В этом руководстве вы можете найти информацию о настройке и использовании Консоли управления Kaspersky Embedded Systems Security 2.1.

В этом разделе

В этом документе

Руководство пользователя Kaspersky Embedded Systems Security 2.1 содержит следующие разделы:

Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о назначении, ключевых возможностях и составе программы.

Интерфейс Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию об основных элементах интерфейса программы.

Запуск и остановка Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о запуске Консоли Kaspersky Embedded Systems Security 2.1, а также запуске и остановке службы Kaspersky Security Service.

Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о состоянии защиты компьютера и информацию о Kaspersky Embedded Systems Security 2.1.

Права доступа к функциям Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.1 и службами Windows®, которые регистрирует программа, а также инструкции по настройке этих прав.

Работа с Консолью Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о Консоли Kaspersky Embedded Systems Security 2.1 и об управлении программой через Консоль Kaspersky Embedded Systems Security 2.1, установленную на защищаемом компьютере или на другом компьютере.

Настройка доверенной зоны

Этот раздел содержит информацию о доверенной зоне Kaspersky Embedded Systems Security 2.1, инструкции по добавлению объектов в доверенную зону и по применению доверенной зоны в задачах Kaspersky Embedded Systems Security 2.1.

Управление задачами Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security 2.1, их создании, настройке параметров выполнения, запуске и остановке.

Постоянная защита

Этот раздел содержит информацию о задачах постоянной защиты: задаче Постоянная защита файлов и задаче Использование KSN.Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты и по настройке параметров безопасности защищаемого компьютера.

Контроль компьютера

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.1, которая позволяет контролировать запуски программ, подключения флеш-накопителей и других внешних устройств по USB, а также контролировать работу сетевого экрана Windows.

Диагностика системы

Этот раздел содержит информацию о задаче контроля файловых операций и возможностях анализа системного журнала операционной системы.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и по настройке параметров безопасности защищаемого компьютера.

Обновление баз и модулей Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Embedded Systems Security 2.1, копировании обновлений и откате обновления баз Kaspersky Embedded Systems Security 2.1, а также инструкции по настройке параметров задач обновления баз и модулей программы.

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.

Запись событий. Журналы Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о работе с журналами Kaspersky Embedded Systems Security 2.1: журналом системного аудита, журналами выполнения задач Kaspersky Embedded Systems Security 2.1 и журналом событий Kaspersky Embedded Systems Security 2.1.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Embedded Systems Security 2.1 о событиях программы и состоянии защиты компьютера, а также инструкцию по настройке уведомлений.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО «Лаборатория Касперского»

Этот раздел содержит информацию об АО «Лаборатория Касперского».

Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.

Пример текста	Описание условного обозначения
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: новые термины; названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: Укажите дату в формате `ДД:ММ:ГГ`.	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

О Kaspersky Embedded Systems Security 2.1

Kaspersky Embedded Systems Security 2.1 защищает компьютеры и другие встроенные системы, работающие под управлением операционных систем Microsoft® Windows®, от вирусов и других угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security 2.1 являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Вы можете установить Kaspersky Embedded Systems Security 2.1 на любых типах встроенных систем под управлением Windows, в том числе на следующих классах устройств:

- банковские автоматы;
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security 2.1 следующими способами:

- через Консоль Kaspersky Embedded Systems Security 2.1, установленную на одном компьютере с Kaspersky Embedded Systems Security 2.1 или на другом компьютере;
- с помощью команд командной строки;
- через плагин Kaspersky Embedded Systems Security 2.1 для Kaspersky Security Center (для централизованного управления защитой группы компьютеров, на каждом из которых установлен Kaspersky Embedded Systems Security 2.1).

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security 2.1 для программы «Системный монитор», а также счетчики и ловушки SNMP.

Компоненты и функции Kaspersky Embedded Systems Security 2.1

В состав программы входят следующие компоненты:

- **Постоянная защита**. Kaspersky Embedded Systems Security 2.1 проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security 2.1 проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - главную загрузочную запись и загрузочные секторы локальных жестких и съемных дисков.
- **Проверка по требованию**. Kaspersky Embedded Systems Security 2.1 однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память защищаемого устройства, а также объекты автозапуска.
- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование запоминающих устройств и устройств чтения CD/DVD дисков в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с подключаемым по USB флеш-накопителем или внешним устройством другого типа.
- **Управление сетевым экраном.** Компонент предоставляет возможность управления сетевым экраном Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана другими способами.
- **Мониторинг файловых операций**. Kaspersky Embedded Systems Security 2.1 выявляет изменения файлов, в областях мониторинга, заданных в параметрах задачи, которые могут свидетельствовать о нарушении безопасности на защищаемом компьютере.

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

В программе реализованы следующие функции:

- **Обновление баз и модулей программы**. Kaspersky Embedded Systems Security 2.1 загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений «Лаборатории Касперского», Сервера администрирования Kaspersky Security Center или других источников обновлений.

- **Карантин**. Kaspersky Embedded Systems Security 2.1 помещает объекты, которые он признает возможно зараженными, на карантин, то есть переносит объекты из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.

- **Резервное хранилище**. Kaspersky Embedded Systems Security 2.1 сохраняет зашифрованные копии объектов со статусами *зараженный или обнаруживаемый* и *возможно зараженный* в *резервном 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 компьютеру, о событиях, связанных с работой Kaspersky Embedded Systems Security 2.1 и состоянием антивирусной защиты компьютера.

- **Импорт и экспорт параметров**. Вы можете экспортировать параметры Kaspersky Embedded Systems Security 2.1 в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security 2.1 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 компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security 2.1.

- **Управление правами доступа к функциям Kaspersky Embedded Systems Security 2.1**.Вы можете настраивать права на управление Kaspersky Embedded Systems

Security 2.1 и службами Windows, которые регистрирует программа, для пользователей и групп пользователей.

- **Запись событий в журнал событий программы**.Kaspersky Embedded Systems Security 2.1 записывает в журналы 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 2.1, 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 2.1 будет применять в задачах проверки по требованию и постоянной защиты файлов.

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

Интерфейс Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию об основных элементах интерфейса программы.

В этом разделе

Интерфейс окна Консоли Kaspersky Embedded Systems Security 2.1

Консоль Kaspersky Embedded Systems Security 2.1 отображается в дереве Microsoft Management Console в виде узла с именем **Kaspersky Embedded Systems Security 2.1**.

После подключения к Kaspersky Embedded Systems Security 2.1, установленному на другом компьютере, в название узла добавляется имя компьютера, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Embedded Systems Security 2.1 <Имя компьютера> как <имя учетной записи>**. При подключении к Kaspersky Embedded Systems Security 2.1, установленному на том же компьютере, что и Консоль, название узла имеет вид: **Kaspersky Embedded Systems Security 2.1**.

По умолчанию окно Консоли Kaspersky Embedded Systems Security 2.1 содержит следующие элементы:

- дерево Консоли;
- панель результатов;
- панель быстрого доступа;
- панель инструментов.

Также вы можете включить отображение в окне Консоли области описания и панели действия.

Дерево Консоли

В дереве Консоли отображается узел **Kaspersky Embedded Systems Security 2.1** и вложенные в него узлы функциональных компонентов программы.

В состав узла **Kaspersky Embedded Systems Security** входят следующие вложенные узлы:

- **Постоянная защита**: управление постоянной защитой файлов и параметрами использования служб KSN. Узел **Постоянная защита** позволяет управлять следующими задачами:
  - **Постоянная защита файлов**.
  - **Использование KSN**.
- **Контроль компьютера**: контроль подключаемых устройств, а также контроль программ, запускаемых на защищаемом компьютере. Узел **Контроль компьютера** позволяет управлять следующими задачами:
  - **Контроль запуска программ**.
  - **Контроль устройств**.
  - **Управление сетевым экраном**.
- **Автоматическая генерация правил**: настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ и Контроль устройств.
  - **Генерация правил контроля запуска программ**.
  - **Генерация правил контроля устройств**.
  - Групповые задачи формирования правил **<Имя задач>** (если есть).

Групповые задачи (см. раздел «Категории задач Kaspersky Embedded Systems Security 2.1« на стр. 71) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль Kaspersky Embedded Systems Security 2.1.

- **Диагностика системы**: управление параметрами контроля файловых операций и настройка 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 **<Имя задач>** (если есть).

  В узле отображаются системные задачи (см. раздел «Категории задач Kaspersky Embedded Systems Security 2.1« на стр. 71), созданные при установке программы, добавленные пользовательские задачи, а также групповые задачи проверки по требованию, сформированные и переданные на компьютер с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Embedded Systems Security 2.1, а также копированием обновлений для сохранения их в папке локального источника обновлений. Узел содержит вложенные узлы для управления каждой задачей обновления и задачей отката последнего обновления баз программы:
  - **Обновление баз программы**.
  - **Обновление модулей программы**.
  - **Копирование обновлений**.
  - **Откат обновления баз программы**.

В узле отображаются все пользовательские и групповые задачи (см. раздел «Категории задач Kaspersky Embedded Systems Security 2.1« на стр. 71) обновления, сформированные и переданные на компьютер с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами карантина и резервного хранилища.
  - **Карантин**.
  - **Резервное хранилище**.
- **Журналы**: управление журналами выполнения задач постоянной защиты, проверки по требованию, контроля компьютера и обновления; управление журналом событий безопасности и журналом системного аудита Kaspersky Embedded Systems Security 2.1.
  - **Журнал событий безопасности**.
  - **Журнал системного аудита**.
  - **Журналы выполнения задач**.
- **Лицензирование**: добавление и удаление ключей и кодов активации Kaspersky Embedded Systems Security 2.1, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Embedded Systems Security**, в панели результатов отображается информация о текущем состоянии защиты компьютера (см. раздел «Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security 2.1« на стр. 31), информация о Kaspersky Embedded Systems Security 2.1, состоянии его функциональных компонентов и статусе лицензии или ключа.

Контекстное меню узла Kaspersky Embedded Systems Security

С помощью пунктов контекстного меню узла **Kaspersky Embedded Systems Security** вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключиться к другому компьютеру для управления установленным на этом компьютере Kaspersky Embedded Systems Security 2.1. Для выполнения этой операции вы также можете воспользоваться

ссылкой в правом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.

- **Запустить Kaspersky Embedded Systems Security 2.1 / Остановить Kaspersky Embedded Systems Security 2.1** (**Запустить / Остановить**). Запустить или остановить программу или выбранную задачу (см. раздел «Запуск / приостановка / возобновление / остановка задачи вручную« на стр. 73). 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**. Посмотреть и настроить проверку съемных дисков при подключении (см. раздел «Проверка съемных дисков» на стр. 291).

- **Защита от эксплойтов: общие параметры защиты**. Выбрать режим защиты компьютера от эксплойтов и действия по снижению рисков (см. раздел «Настройка параметров защиты памяти процессов» на стр. 148).

- **Защита от эксплойтов: параметры защиты процессов**. Добавить процессы в список защищаемых и настроить параметры их защиты (см. раздел «Настройка области защиты» на стр. 150).

- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны (см. раздел «О доверенной зоне Kaspersky Embedded Systems Security 2.1« на стр. 61).

- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Embedded Systems Security 2.1 (см. раздел «О правах на управление Kaspersky Embedded Systems Security 2.1« на стр. 40).

- **Изменить права пользователей на управление Kaspersky Security Service**. Просмотреть и настроить права доступа к управлению службой Kaspersky Security Service.

- **Настроить параметры уведомлений**. Просмотреть и настроить параметры уведомлений администратора и пользователей Kaspersky Embedded Systems Security 2.1 (см. раздел «Настройка уведомлений администратора и пользователей« на стр. 353).

- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел «Экспорт параметров« на стр. 82). 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. 84). 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 2.1 и текущих доступных обновлениях модулей программы.

- **О программе**. Перейти к просмотру информации о Kaspersky Embedded Systems Security 2.1.

- **Новое окно**. Открыть новое окно в Консоли Kaspersky Embedded Systems Security 2.1. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Обновить**. Обновить содержимое окна Консоли Kaspersky Embedded Systems Security 2.1. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Embedded Systems Security 2.1 или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  > Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Embedded Systems Security** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Embedded Systems Security 2.1. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель быстрого доступа и контекстное меню задач Kaspersky Embedded Systems Security 2.1

Вы можете управлять задачами Kaspersky Embedded Systems Security 2.1 с помощью пунктов контекстного меню каждой задачи в дереве Консоли.

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

- **Возобновить / Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел «Запуск / приостановка / возобновление / остановка задачи вручную« на стр. 73). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты и задач проверки по требованию.

- **Добавить задачу**. Создать новую пользовательскую задачу (см. раздел «Создание задачи проверки по требованию« на стр. 273). Операция доступна для задач проверки по требованию.

- **Открыть журнал выполнения**. Перейти к просмотру и работе с журналом выполнения задачи. (см. раздел «О журналах выполнения задач« на стр. 332) Операция доступна для всех задач.

- **Сохранить задачу**. Сохранить и применить измененные параметры задачи (см. раздел «Сохранение задачи после изменения ее параметров« на стр. 72). Операция доступна для задач постоянной защиты файлов и задач проверки по требованию.

- **Удалить задачу**. Удалить пользовательскую задачу (см. раздел «Удаление задачи« на стр. 277). Операция доступна для задач проверки по требованию.

- **Статистика**. Перейти к просмотру статистики задачи. Операция доступна для задачи проверки целостности программы.

- **Шаблоны параметров**. Перейти к работе с шаблонами. Операция доступна для задач постоянной защиты файлов и проверки по требованию.

Значок Kaspersky Embedded Systems Security в области уведомлений панели задач

Каждый раз, когда Kaspersky Embedded Systems Security 2.1 автоматически запускается после перезагрузки защищаемого компьютера, в области уведомлений панели задач отображается значок Kaspersky Embedded Systems Security . Он отображается по умолчанию, если при установке программы вы установили компонент **Значок области уведомлений Kaspersky Embedded Systems Security**.

Внешний вид значка области уведомлений Kaspersky Embedded Systems Security 2.1 является индикатором текущего состояния защиты компьютера. Значок может иметь одно из следующих состояний:

- активное (цветной значок), если в текущий момент выполняется хотя бы одна из задач: Постоянная защита файлов, Контроль запуска программ, Контроль устройств;
- неактивное (черно-белый значок), если в текущий момент не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ, Контроль устройств.

Вы можете открыть контекстное меню значка по правой клавише мыши.

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

Таблица 2. Команды контекстного меню значка области уведомлений Kaspersky Embedded Systems Security 2.1

Команда	Описание
Открыть Консоль Kaspersky Embedded Systems Security 2.1	Открывает Консоль Kaspersky Embedded Systems Security 2.1 (если она установлена).
О программе	Открывает окно **О программе** с информацией о Kaspersky Embedded Systems Security 2.1. Если вы зарегистрированы в качестве пользователя Kaspersky Embedded Systems Security 2.1, окно **О программе** содержит информацию об установленных срочных обновлениях.
Скрыть	Скрывает значок Kaspersky Embedded Systems Security в области уведомлений панели задач.

Вы можете снова отобразить скрытый значок Kaspersky Embedded Systems Security в любой момент.

► *Чтобы снова отобразить значок программы,*

в меню **Пуск** Microsoft Windows выберите **Программы** → **Kaspersky Embedded Systems Security 2.1** → **Значок Kaspersky Embedded Systems Security**.

Названия параметров могут отличаться в разных операционных системах Windows.

В параметрах программы вы можете включать и выключать отображение значка Kaspersky Embedded Systems Security в области уведомлений при автоматическом запуске программы после перезагрузки компьютера.

Запуск и остановка Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о запуске Консоли Kaspersky Embedded Systems Security 2.1, а также запуске и остановке службы Kaspersky Security Service.

В этом разделе

Запуск Консоли Kaspersky Embedded Systems Security 2.1 из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль программы из меню Пуск:*

в меню **Пуск** выберите **Программы** → **Kaspersky Embedded Systems Security 2.1** → **Средства администрирования** → **Консоль Kaspersky Embedded Systems Security 2.1**.

Если вы планируете добавлять в Консоль программы другие оснастки, запустите Консоль в авторском режиме.

► *Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы** → **Kaspersky Embedded Systems Security 2.1** → **Средства администрирования**.
2. В контекстном меню программы **Консоль Kaspersky Embedded Systems Security 2.1** выберите команду **Автор**.

Консоль Kaspersky Embedded Systems Security 2.1 будет запущена в авторском режиме.

Если вы запустили Консоль на защищаемом компьютере, откроется окно Консоли (см. раздел «Интерфейс окна Консоли Kaspersky Embedded Systems Security 2.1« на стр. 19).

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

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла Kaspersky Embedded Systems Security.
2. Выберите команду **Подключиться к другому компьютеру**.

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

Консоль Kaspersky Embedded Systems Security 2.1 будет подключена к защищаемому компьютеру.

Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе управления Kaspersky Embedded Systems Security 2.1 на компьютере, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

Запуск и остановка службы Kaspersky Security Service

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

По умолчанию при запуске службы Kaspersky Security Service запускаются задачи Постоянная защита файлов, Проверка при старте операционной системы, Проверка целостности программы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

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

Вы можете запускать и останавливать службу Kaspersky Security Service с помощью контекстного меню узла **Kaspersky Embedded Systems Security** или с помощью оснастки **Службы** Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Embedded Systems Security 2.1, если вы входите в группу «Администраторы» на защищаемом сервере.

► *Чтобы остановить или запустить программу с помощью Консоли управления, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите одну из следующих команд:
   - **Остановить Kaspersky Embedded Systems Security 2.1**, чтобы остановить службу Kaspersky Security Service;
   - **Запустить Kaspersky Embedded Systems Security 2.1**, чтобы запустить службу Kaspersky Security Service.

Служба Kaspersky Security Service будет запущена или остановлена.

Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security 2.1

► *Чтобы просмотреть информацию о состоянии защиты компьютера и информацию о Kaspersky Embedded Systems Security 2.1,*

выберите узел **Kaspersky Embedded Systems Security 2.1** в дереве Консоли.

По умолчанию информация в панели результатов Консоли Kaspersky Embedded Systems Security 2.1 обновляется автоматически:

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

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле Kaspersky Embedded Systems Security 2.1,*

в контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Обновить**.

В панели результатов Консоли отображается следующая информация о программе:

- состояние защиты компьютера;
- данные об обновлении баз и модулей программы;
- данные о лицензии;
- данные о задачах контроля компьютера;
- статус интеграции с Kaspersky Security Center: данные компьютера с установленным Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

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

Таблица 3. Информация о состоянии защиты компьютера

Блок Защита	Информация
Индикатор состояния защиты компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что задачи постоянной защиты выполняются, а задача проверки важных областей завершилась не более 30 дней назад (по умолчанию). • Желтый цвет панели – одна или несколько задач постоянной защиты не запущены или остановлены, а задача проверки важных областей давно не выполнялась. • Красный цвет панели – не удалось запустить задачу постоянной защиты файлов.

Блок Защита	Информация
Постоянная защита файлов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Обнаружено** – количество объектов, которые обнаружил Kaspersky Embedded Systems Security 2.1. Например, если Kaspersky Embedded Systems Security 2.1 обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ превышает 0, значение выделяется красным цветом.
Использование KSN	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Недоверенных заключений** – количество объектов, признанных недоверенными службами KSN. Например, если при проверке пяти файлов служба KSN вынесла заключение о вредоносности одного из них, значение в этом поле увеличится на единицу. Если количество недоверенных заключений превышает 0, значение строки выделяется красным цветом.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз компьютерной безопасности. *Не проводилась* – событие, которое возникает, если задача проверки важных областей выполнялась 30 и более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.
Объектов в резервном хранилище	*Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если порог доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Embedded Systems Security 2.1 при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом.

	Превышен максимальный размер резервного хранилища – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Embedded Systems Security 2.1 при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом. **Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище в текущий момент. **Используемое пространство** – объем используемого пространства в резервном хранилище.
Защита памяти	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. Режим работы – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: • Предотвращать использование уязвимостей в процессах. • Только сообщать о подозрительном вторжении в процессы. **Процессов в списке защиты** – общее количество процессов, которые находятся под защитой и обрабатываются в соответствие с выбранным режимом.

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

Таблица 4. Информация о состоянии баз и модулей Kaspersky Embedded Systems Security 2.1

Блок Обновление	Информация
Индикатор состояния баз и модулей программы	Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что базы программы актуальны, а также отсутствуют доступные критические обновления модулей программы. • Желтый цвет панели – возникло одно из следующих событий: *Базы программы устарели*; *Доступно критическое обновление модулей программ*; *Объявлен отзыв критического обновления модулей программы*; *Для завершения обновления модулей программы требуется перезагрузить компьютер.* • Красный цвет панели – возникло событие *Базы программы сильно устарели* или *Базы повреждены*.

Блок Обновление	Информация
Обновление баз и модулей программы	**Актуальность баз программы** – оценка актуальности баз программы. Параметр может принимать следующие значения: • **Базы программы актуальны** – базы программы обновлены не более чем 7 дней назад (по умолчанию); • **Базы программы устарели** – базы программы обновлены 7–14 дней назад (по умолчанию); • **Базы программы сильно устарели** – базы программы обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий *Базы программы устарели* и *Базы программы сильно устарели*. **Дата выпуска баз программы** – дата и время выпуска последнего установленного обновления баз программы. Дата и время указаны в UTC. **Количество записей в базах программы** – количество записей об угрозах в установленных базах программы. **Статус последней запущенной задачи обновления баз программы** – дата и время последнего обновления базы программы. Дата и время указаны по местному времени защищаемого компьютера. Значение в поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*. **Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Embedded Systems Security 2.1, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Embedded Systems Security 2.1.

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

Таблица 5. Информация о состоянии контроля компьютера

Блок Контроль	Информация
Индикатор состояния контроля компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что все задачи контроля компьютера выполняются. • Желтый цвет панели – одна или несколько задач защиты компьютера не запущены; возникает событие *Не выполняется*. • Красный цвет панели – не удалось запустить задачу контроля запуска программ или контроля внешних устройств; возникает событие *Завершена с ошибкой*.
Контроль запуска программ	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Контроль запуска программ: • Применять правила контроля запуска программ. • Только статистика. **Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Embedded Systems Security 2.1 в ходе выполнения задачи контроля запуск программ. Если количество заблокированных запусков программ превышает 0, значение поля окрашивается в красный цвет. **Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Embedded Systems Security 2.1 для обработки попытки запуска программ на защищаемом компьютере.

Блок Контроль	Информация
Контроль устройств	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Контроль запуска программ: • Запрещать недоверенные устройства. • Только статистика. **Заблокировано устройств** – количество подключений устройств с попыткой их использования в качестве запоминающих, заблокированных Kaspersky Embedded Systems Security 2.1 в ходе выполнения задачи контроля устройств. Если количество заблокированных устройств превышает 0, значение поля окрашивается в красный цвет.
Управление сетевым экраном	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. Заблокировано соединений – количество подключений к защищаемому устройству, которые не были разрешены заданными правилами сетевого экрана.

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

Таблица 6. Информация о состоянии диагностики системы

Блок Диагностика	Информация
Индикатор состояния безопасности в сети	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. Индикатор может принимать следующие значения: • Зеленый цвет панели – отображается по умолчанию и означает, что все задачи диагностики системы выполняются. • Желтый цвет панели – одна или несколько задач диагностики системы не запущены; возникает событие *Не выполняется*. • Красный цвет панели – не удалось запустить задачу Мониторинг файловых операций или Анализ журналов; возникает событие *Завершена с ошибкой*.
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированных операций** – количество изменений файлов, находящихся в области мониторинга, которые могут свидетельствовать о нарушении безопасности защищаемого устройства.
Анализ журналов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Возможных нарушений** – количество зафиксированных нарушений по данным журнала событий Windows, выявленных на основе заданных правил задачи или применения эвристического анализатора.

Информация о статусе лицензии Kaspersky Embedded Systems Security 2.1 отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.

Вы можете настроить свойства Kaspersky Embedded Systems Security 2.1 перейдя по ссылке **Свойства программы** (см. раздел «**Параметры работы Kaspersky Embedded Systems Security 2.1 в Консоли** « на стр. 50).

Вы можете выполнить подключение к другому компьютеру перейдя по ссылке **Подключиться к другому компьютеру** (см. раздел «**Управление Kaspersky Embedded Systems Security 2.1 через Консоль на другом компьютере**« на стр. 60).

Права доступа к функциям Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.1 и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

В этом разделе

О правах на управление Kaspersky Embedded Systems Security 2.1

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security 2.1 имеют пользователи, входящие в группу «Администраторы» на защищаемом компьютере, пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.1, а также системная группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Embedded Systems Security 2.1, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security 2.1 другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Embedded Systems Security 2.1, он не может открыть Консоль Kaspersky Embedded Systems Security 2.1.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security 2.1 один из следующих предустановленных уровней доступа к функциям Kaspersky Embedded Systems Security 2.1:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1, права пользователей Kaspersky Embedded Systems Security 2.1, а также просматривать статистику работы Kaspersky Embedded Systems Security 2.1.

- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1.

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1, статистику работы Kaspersky Embedded Systems Security 2.1 и права пользователей Kaspersky Embedded Systems Security 2.1.

Также вы можете выполнять расширенную настройку прав доступа (см. раздел «Настройка прав доступа на управление Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Service« на стр. 45): разрешать или запрещать доступ к отдельным функциям Kaspersky Embedded Systems Security 2.1.

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

Таблица 7. Права доступа к функциям Kaspersky Embedded Systems Security 2.1

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security 2.1.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможность импортировать из конфигурационного файла параметры работы Kaspersky Embedded Systems Security 2.1.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Embedded Systems Security 2.1 и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security 2.1; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Embedded Systems Security 2.1.

Права доступа	Описание
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Embedded Systems Security 2.1.
Удаление программы	Возможность удалять Kaspersky Embedded Systems Security 2.1.
Чтение прав	Возможность просматривать список пользователей Kaspersky Embedded Systems Security 2.1 и права доступа каждого пользователя.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security 2.1.

О правах на управление регистрируемыми службами

Подробная информация о регистрируемых службах Windows и настройке доступа к регистрируемым службам содержится в *Руководстве администратора Kaspersky Embedded Systems Security 2.1.*

При установке Kaspersky Embedded Systems Security 2.1 регистрирует в Windows службу Kaspersky Security Service (KAVFS) и службу управления программой Kaspersky Security Management Service (KAVFSGT).

Служба Kaspersky Security Service

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

Пользователи, которые имеют доступ к функции уровня Изменение прав (см. раздел «О правах на управление Kaspersky Embedded Systems Security 2.1« на стр. 40), могут предоставлять доступ к управлению Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Служба Kaspersky Security Management Service

Для управления программой через Консоль Kaspersky Embedded Systems Security 2.1, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security 2.1 имела полный доступ к Kaspersky Security Management Service на защищаемом компьютере.

По умолчанию доступ к управлению Kaspersky Security Management Service имеют пользователи, входящие в группу «Администраторы» на защищаемом компьютере, и пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.1.

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

Настройка прав доступа на управление Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Service

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security 2.1 и управлению службой Kaspersky Security Service, а также изменять права доступа этих пользователей и групп пользователей.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:

   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security 2.1.

   - Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security Service.

     Откроется окно **Разрешения для группы «Kaspersky Embedded Systems Security 2.1»**.

2. В открывшемся окне выполните следующие действия:

   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.

   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

3. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security 2.1 или службой Kaspersky Security Service, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:

   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите настроить права доступа к функциям Kaspersky Embedded Systems Security 2.1.

   - Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите настроить права доступа к службе Kaspersky Security Service.

     Откроется окно **Разрешения для группы «Kaspersky Embedded Systems Security 2.1»**.

2. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.

3. В блоке **Разрешения для группы «<Пользователь (Группа)>«** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:

   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security 2.1 или службой Kaspersky Security Service.

   - **Чтение**:

     - следующие права на управление Kaspersky Embedded Systems Security 2.1: **Чтение статистики**, **Чтение параметров**, **Чтение журналов** и **Чтение прав**;

     - следующие права на управление службой Kaspersky Security Service: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Перечисление зависимых служб, Чтение прав**.

- **Изменение**:
  - все права на управление Kaspersky Embedded Systems Security 2.1, кроме **Изменение прав**;
  - следующие права на управление службой Kaspersky Security Service: **Изменение параметров службы, Чтение прав**.
- **Исполнение**: следующие права на управление службой Kaspersky Security Service: **Запуск службы**, **Остановка службы**, **Приостановка / Возобновление службы**, **Чтение прав**, **Пользовательские запросы к службе**.

4. Если вы хотите выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security 2.1** выберите нужного пользователя или группу.
   b. Нажмите на кнопку **Изменить**.
   c. В открывшемся окне перейдите по ссылке **Показать особые разрешения**.
   d. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить** или **Запретить**).
   e. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
   f. Нажмите на кнопку **ОК**.
   g. В окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security 2.1** нажмите на кнопку **ОК.**
5. В окне **Разрешения для группы «Kaspersky Embedded Systems Security 2.1»** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Embedded Systems Security 2.1 или службой Kaspersky Security Service будут сохранены.

Работа с Консолью Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о Консоли Kaspersky Embedded Systems Security 2.1 (далее также »Консоль») и об управлении программой через Консоль Kaspersky Embedded Systems Security 2.1, установленную на защищаемом или другом компьютере.

В этом разделе

О Консоли Kaspersky Embedded Systems Security 2.1

Консоль Kaspersky Embedded Systems Security 2.1 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль, установленную на защищаемом компьютере или на другом компьютере в сети организации. После того как вы установили Консоль Kaspersky Embedded Systems Security 2.1 на другом компьютере, вам нужно выполнить дополнительную настройку (см. раздел «Управление Kaspersky Embedded Systems Security 2.1 через Консоль на другом компьютере« на стр. 60).

Если Консоль Kaspersky Embedded Systems Security 2.1 и программа установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в доставке информации от Kaspersky Embedded Systems Security 2.1 в Консоль. Например, после старта какой-либо задачи Kaspersky Embedded Systems Security 2.1 статус этой задачи может не обновиться в Консоли.

При установке Консоли программа установки сохраняет файл kavfs.msc в папке установки и добавляет оснастку Kaspersky Embedded Systems Security 2.1 в список изолированных оснасток Microsoft Windows.

Вы можете открыть Консоль Kaspersky Embedded Systems Security 2.1 из меню **Пуск**. На защищаемом устройстве вы также можете открыть Консоль с помощью значка Kaspersky Embedded Systems Security 2.1 в области уведомлений панели задач.

Вы можете запустить msc-файл оснастки Kaspersky Embedded Systems Security 2.1 или добавить оснастку программы в существующую консоль Microsoft Management Console, как новый элемент в ее дереве (см. раздел «Интерфейс окна Консоли Kaspersky Embedded Systems Security 2.1« на стр. 19).

В 64-битной версии Microsoft Windows вы можете добавить оснастку Kaspersky Embedded Systems Security 2.1 только в Microsoft Management Console 32-битной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

В одну Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток программы, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Embedded Systems Security 2.1.

Параметры работы Kaspersky Embedded Systems Security 2.1 в Консоли

Общие параметры и параметры диагностики сбоев Kaspersky Embedded Systems Security 2.1 определяют общие условия работы программы. Эти параметры позволяют регулировать количество рабочих процессов, используемых Kaspersky Embedded Systems Security 2.1, включать восстановление задач Kaspersky Embedded Systems Security 2.1 после их аварийного завершения, вести журнал трассировки, включать создание файла дампа процессов Kaspersky Embedded Systems Security 2.1 при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров работы программы в Консоли Kaspersky Embedded Systems Security 2.1 недоступна, если в активной политике Kaspersky Security Center установлен запрет на изменение данных параметров.

► *Чтобы настроить параметры работы Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security 2.1** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.

2. В открывшемся окне настройте общие параметры работы Kaspersky Embedded Systems Security 2.1 согласно вашим требованиям:

   - На закладке **Масштабируемость и интерфейс** вы можете настроить следующие параметры:
     - В блоке **Параметры масштабируемости**:
       - Максимальное количество активных процессов, которые Kaspersky Embedded Systems Security 2.1 может запустить.

Таблица 8. Максимальное количество активных процессов

<table>
<tr><td>Параметр</td><td>Максимальное количество активных процессов.</td></tr>
<tr><td>Описание</td><td>Этот параметр относится к группе Параметры масштабируемости Kaspersky Embedded Systems Security 2.1. Он устанавливает максимальное количество рабочих процессов, которые программа может запустить одновременно.

Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Kaspersky Embedded Systems Security 2.1 к сбоям. Однако, высокое значение этого параметра может снизить общую производительность компьютера и повысить потребление оперативной памяти.

В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр Максимальное количество активных процессов только для Kaspersky Embedded Systems Security 2.1 на отдельном компьютере (в диалоговом окне Параметры программы); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.</td></tr>
<tr><td>Возможные значения</td><td>1 – 8</td></tr>
<tr><td>Значение по умолчанию</td><td>Kaspersky Embedded Systems Security 2.1 выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:
<table><tr><th>Количество процессоров</th><th>Максимальное количество активных процессов</th></tr><tr><td>1</td><td>1</td></tr><tr><td>1 < кол-во процессоров < 4</td><td>2</td></tr><tr><td>4 и более</td><td>4</td></tr></table></td></tr>
</table>

- Количество процессов для постоянной защиты.

Таблица 9. Количество процессов для постоянной защиты

Параметр	Число процессов для постоянной защиты.
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Embedded Systems Security 2.1. С помощью этого параметра вы можете устанавливать фиксированное количество процессов, в которых Kaspersky Embedded Systems Security 2.1 будет выполнять задачи постоянной защиты. Более высокое значение этого параметра повысит скорость проверки объектов в задачах постоянной защиты. Однако чем больше рабочих процессов задействует Kaspersky Embedded Systems Security 2.1, тем больше будет его влияние на общую производительность защищаемого компьютера и его потребление оперативной памяти. В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр **Количество процессов для постоянной защиты** только для Kaspersky Embedded Systems Security 2.1 на отдельном компьютере (в окне **Параметры программы**); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.

<table>
<tr><td>Возможные значения</td><td>Возможные значения: 1-N, где N – значение, заданное параметром Максимальное количество активных процессов.

Если вы установите значение параметра Количество процессов для постоянной защиты равным максимальному числу активных процессов, вы снизите влияние Kaspersky Embedded Systems Security 2.1 на скорость файлового обмена компьютеров с компьютером, еще повысив его быстродействие во время постоянной защиты. Однако задачи обновления и задачи проверки по требованию с базовым приоритетом Средний (Normal) будут выполняться в уже запущенных рабочих процессах Kaspersky Embedded Systems Security 2.1. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени.

Задачи проверки по требованию с базовым приоритетом Низкий (Low) всегда выполняются в отдельном процессе или процессах.</td></tr>
<tr><td>Значение по умолчанию</td><td>Kaspersky Embedded Systems Security 2.1 выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:<table><tr><th>Количество процессоров</th><th>Число процессов для постоянной защиты</th></tr><tr><td>=1</td><td>1</td></tr><tr><td>>1</td><td>2</td></tr></table></td></tr>
</table>

- Количество рабочих процессов для фоновых задач проверки по требованию.

Таблица 10. 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 2.1. С помощью этого параметра вы можете указывать максимальное количество процессов, в которых Kaspersky Embedded Systems Security 2.1 будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, которое вы устанавливаете этим параметром, не входит в общее количество рабочих процессов Kaspersky Embedded Systems Security 2.1, заданное параметром **Максимальное количество активных процессов**. Например, если вы установите следующие значения параметров: • максимальное количество активных процессов – 3; • количество процессов для задач постоянной защиты – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты и одну задачу проверки по требованию в фоновом режиме, общее количество рабочих процессов kavfswp.exe Kaspersky Embedded Systems Security 2.1 составит 4. В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию. Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.
Возможные значения	1-4
Значение по умолчанию	1

- В блоке **Взаимодействие с пользователем** настройте отображение значка Kaspersky Embedded Systems Security 2.1 в области уведомлений панели задач (см. раздел «Значок Kaspersky Embedded Systems Security в области уведомлений панели задач« на стр. 26) при каждом запуске программы.

- На закладке **Безопасность и надежность** вы можете настроить следующие параметры:

  - В блоке **Параметры надежности** укажите количество попыток восстановления задач проверки по требованию после их аварийного завершения.

Таблица 11. Восстановление задач

Параметр	Восстановление задач (**Выполнять восстановление задач**).
Описание	Этот параметр относится к группе **Параметры надежности** Kaspersky Embedded Systems Security 2.1. Он включает восстановление задач, если они завершаются аварийно, и устанавливает количество попыток восстановления задач проверки по требованию. Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Embedded Systems Security 2.1 пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения. Если восстановление задач выключено, Kaspersky Embedded Systems Security 2.1 не восстанавливает задачи постоянной защиты и проверки по требованию. Если восстановление задач включено, Kaspersky Embedded Systems Security 2.1 пытается восстановить задачи постоянной защиты, пока они не будут успешно запущены, и пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.
Возможные значения	Включено / выключено. Количество попыток восстановления задач проверки по требованию: 1-10.
Значение по умолчанию	Восстановление задач включено. Количество попыток восстановления задач проверки по требованию – 2.

- В блоке **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Embedded Systems Security 2.1 при работе от источника бесперебойного питания.

Таблица 12. Использование источника бесперебойного питания

Параметр	Действия при переходе на источник бесперебойного питания.
Описание	Этот параметр определяет действия, которые Kaspersky Embedded Systems Security 2.1 выполнит, когда компьютер перейдет на питание от источника бесперебойного питания.
Возможные значения	Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию. Выполнять или останавливать все выполняемые задачи проверки по требованию.
Значение по умолчанию	По умолчанию при работе компьютера от источника бесперебойного питания Kaspersky Embedded Systems Security 2.1 работает в следующем режиме: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию; • автоматически останавливает все выполняемые задачи проверки по требованию.

- В блоке **Параметры применения пароля** настройте параметры защиты паролем при доступе к функциям программы.

  - На закладке **Параметры соединения**:

    - В блоке **Параметры прокси-сервера** укажите параметры использования прокси-сервера.

    - В блоке **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и необходимые данные для аутентификации на прокси-сервере.

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

- На закладке **Диагностика сбоев**:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
    - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security 2.1 будет сохранять файлы трассировки.
    - Настройте уровень детализации отладочной информации.

    В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки.

    Вы можете выбрать один из следующих уровней детализации:

    - **Критические события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки только информацию о критических событиях.
    - **Ошибки** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях и об ошибках.
    - **Важные события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях, об ошибках и о важных событиях.
    - **Информационные события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях, об ошибках, о важных событиях и об информационных событиях.
    - **Вся отладочная информация** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки всю отладочную информацию.

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

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

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

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

Список кодов подсистем Kaspersky Embedded Systems Security 2.1, о работе которых программа сохраняет отладочную информацию в файле трассировки. Коды подсистем требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Таблица 13. Коды подсистем Kaspersky Embedded Systems Security 2.1

Код подсистемы	**Название подсистемы**
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security 2.1 в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security 2.1.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Embedded Systems Security 2.1.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.

prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Embedded Systems Security 2.1 (gui) и плагина управления Kaspersky Embedded Systems Security 2.1 для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Embedded Systems Security 2.1 применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security 2.1 сохраняет отладочную информацию о работе всех подсистем Kaspersky Embedded Systems Security 2.1 (рекомендуется).

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

- Если вы хотите создавать файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
    - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security 2.1 будет сохранять файл дампа.

Kaspersky Embedded Systems Security 2.1 записывает информацию в файлы трассировки и файл дампа в незашифрованном виде.

3. Нажмите на кнопку **ОК**.

Параметры работы Kaspersky Embedded Systems Security 2.1 будут сохранены.

Управление Kaspersky Embedded Systems Security 2.1 через Консоль на другом компьютере

Вы можете управлять Kaspersky Embedded Systems Security 2.1 через Консоль, которая установлена на удаленном компьютере.

Чтобы управление программой с помощью Консоли Kaspersky Embedded Systems Security 2.1 на удаленном компьютере было доступно, убедитесь, что:

- Пользователи Консоли Kaspersky Embedded Systems Security 2.1 на удаленном компьютере добавлены в группу ESS Administrators на защищаемом компьютере.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management Service kavfsgt.exe, если на защищаемом компьютере включен брандмауэр Windows.
- Во время установки Kaspersky Embedded Systems Security 2.1 был установлен флажок **Разрешить удаленный доступ** в окне Мастера установки.

Если Kaspersky Embedded Systems Security 2.1 на удаленном компьютере защищен паролем, вам нужно ввести пароль для получения доступа к управлению программой через Консоль.

Настройка доверенной зоны

Этот раздел содержит информацию о доверенной зоне Kaspersky Embedded Systems Security 2.1, инструкции по добавлению объектов в доверенную зону и по применению доверенной зоны в задачах Kaspersky Embedded Systems Security 2.1.

В этом разделе

О доверенной зоне Kaspersky Embedded Systems Security 2.1

Доверенная зона – это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах проверки по требованию, постоянной защиты файлов.

Если при установке Kaspersky Embedded Systems Security 2.1 вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные «Лабораторией Касперского»**, Kaspersky Embedded Systems Security 2.1 добавляет в доверенную зону файлы, рекомендованные Microsoft и »Лабораторией Касперского», для задач постоянной защиты.

Вы можете формировать доверенную зону Kaspersky Embedded Systems Security 2.1 по следующим правилам:

- **Доверенные процессы**. В доверенную зону помещаются объекты, к которым обращаются процессы программ, чувствительных к файловым перехватам.

- **Операции резервного копирования**. В доверенную зону помещаются объекты, доступ к которым выполняется в операциях систем резервного копирования жестких дисков на внешние устройства.

- **Исключения**. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задачах постоянной защиты файлов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи проверки объектов на карантине.

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

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный файл в формате XML, чтобы затем импортировать его в Kaspersky Embedded Systems Security 2.1 на другом компьютере.

Доверенные процессы

Применяется в задаче постоянной защиты файлов.

Некоторые программы на компьютере могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Embedded Systems Security 2.1. К таким программам относятся, например, системные программы домен-контроллеров.

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

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

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

> Если исполняемый файл процесса изменяется, например, обновляется, Kaspersky Embedded Systems Security 2.1 исключает его из списка доверенных процессов.

Kaspersky Embedded Systems Security 2.1 не использует значение пути к файлу на локальном компьютере для идентификации процесса как доверенного. Путь к файлу на локальном компьютере применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

Операции резервного копирования

Применяется в задачах постоянной защиты.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства вы можете выключить функцию постоянной защиты объектов, доступ к которым осуществляется в операциях резервного копирования. Kaspersky Embedded Systems Security 2.1 не проверяет объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Исключения

Применяется в задачах постоянной защиты файлов и проверки по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в настройках параметров уровня безопасности каждой задачи Kaspersky Embedded Systems Security 2.1 по отдельности.

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

На основании исключения Kaspersky Embedded Systems Security 2.1 может пропускать в указанных задачах объекты согласно следующим параметрам:

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

Включение и выключение применения доверенной зоны в задачах Kaspersky Embedded Systems Security 2.1

По умолчанию доверенная зона применяется в задачах 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 2.1, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню задачи, для которой хотите настроить применение доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** в соответствующем блоке выполните одно из следующих действий:
   - Если вы хотите применять доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Если вы хотите выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Если вы хотите настроить параметры доверенной зоны, перейдите по ссылке, расположенной в названии флажка **Применять доверенную зону** (см. раздел «**Добавление исключений в доверенную зону**« на стр. 65).
5. Нажмите на кнопку **ОК**.

Внесенные изменения будут сохранены.

Добавление исключений в доверенную зону

Этот раздел содержит инструкции по добавлению единых исключений в доверенную зону Kaspersky Embedded Systems Security 2.1.

В этом разделе

Добавление процессов в список доверенных

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

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

  Если исполняемый файл процесса изменится, Kaspersky Embedded Systems Security 2.1 исключит этот процесс из списка доверенных процессов.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.

3. В окне **Доверенная зона** на закладке **Доверенные процессы** установите флажок **Не проверять файловую активность указанных процессов**.

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление доверенного процесса**.

5. Добавьте доверенный процесс одним из следующих способов:

   - Если вы хотите добавить процесс из списка выполняемых процессов, выполните следующие действия:

     a. В окне **Добавление доверенного процесса** нажмите на кнопку **Процессы**.

     Откроется окно **Активные процессы**.

     b. В окне **Активные процессы** выберите нужный процесс в списке выполняемых процессов и нажмите на кнопку **ОК**.

     Блок **Критерии доверенности** автоматически заполнится данными указанного процесса.

     > Требуется, чтобы учетная запись, с правами которой запускается задача постоянной защиты файлов, имела права администратора на компьютере с установленным Kaspersky Embedded Systems Security 2.1, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, PID или пути к исполняемому файлу процесса на локальном компьютере.

   - Если вы хотите указать исполняемый файл процесса, выполните следующие действия:

     a. В окне **Добавление доверенного процесса** нажмите на кнопку **Обзор**.

     Откроется стандартное окно выбора файла Microsoft Windows.

     b. Выберите исполняемый файл процесса и нажмите на кнопку **ОК**.

     Блок **Критерии доверенности** автоматически заполнится данными указанного файла.

Kaspersky Embedded Systems Security 2.1 не использует значение пути к файлу на локальном компьютере для идентификации процесса как доверенного. Путь к файлу на локальном компьютере применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

6. Выберите, какие критерии доверенности вы хотите учитывать для выбранного исполняемого файла или процесса:

   - Использовать полный путь для определения доверенности процесса.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет использовать полный путь к папке для определения статуса доверенности процесса.

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

     По умолчанию флажок установлен.

   - Использовать хеш файла для определения доверенности процесса.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет использовать хеш выбранного файла для определения статуса доверенности процесса.

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

     По умолчанию флажок установлен.

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

7. В окне **Добавление доверенного процесса** нажмите на кнопку **ОК**.

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

Удаление процесса из списка доверенных

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

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

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

Выключение постоянной защиты файлов на время резервного копирования

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

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

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

Добавление исключения в доверенную зону

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.

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

   Откроется окно **Исключение**.

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

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

     a. Установите флажок **Проверяемый объект**.

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

        Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает указанную предопределенную область, файл, папку, диск или файл скрипта при проверке с использованием компонента Kaspersky Embedded Systems Security 2.1, выбранного в блоке **Область применения правила**.

        По умолчанию флажок установлен.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

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

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

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

  a. Установите флажок **Обнаруживаемые объекты**.

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные обнаруживаемые объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

  b. Нажмите на кнопку **Изменить**.

  Откроется окно **Список обнаруживаемых объектов**.

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

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

5. Нажмите на кнопку **ОК**.

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

Управление задачами Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security 2.1, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

Категории задач Kaspersky Embedded Systems Security 2.1

Функции постоянной защиты, контроля компьютера, проверки по требованию и обновления Kaspersky Embedded Systems Security 2.1 реализованы в виде задач.

Вы можете управлять задачей с помощью пунктов контекстного меню названия задачи в дереве Консоли, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Embedded Systems Security 2.1: *локальные* и *групповые*.

Локальные задачи

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

- **Локальные системные задачи**. Создаются автоматически при установке Kaspersky Embedded Systems Security 2.1. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.

- **Локальные пользовательские задачи**. В Консоли Kaspersky Embedded Systems Security 2.1 вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые задачи и задачи для наборов компьютеров, созданные через Kaspersky Security Center, отображаются в Консоли Kaspersky Embedded Systems Security 2.1. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли Kaspersky Embedded Systems Security 2.1 вы можете только просматривать состояние групповых задач.

Сохранение задачи после изменения ее параметров

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

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

► *Чтобы сохранить измененные параметры задачи,*

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

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

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

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

Запуск / приостановка / возобновление / остановка задачи вручную

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

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

1. Откройте контекстное меню названия задачи в Консоли Kaspersky Embedded Systems Security 2.1.
2. Выберите один из пунктов: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (см. раздел «Журнал системного аудита« на стр. 328).

После возобновления задачи проверки по требованию Kaspersky Embedded Systems Security 2.1 продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Embedded Systems Security 2.1 по расписанию, а также настраивать параметры запуска по расписанию.

В этом разделе

Настройка параметров расписания запуска задач

В Консоли Kaspersky Embedded Systems Security 2.1 вы можете настроить расписание запуска локальных системных и пользовательских задач (см. стр. 71). Вы не можете настраивать расписание запуска групповых задач.

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

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

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Выполнять по расписанию**.

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

4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. В списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество часов, и укажите количество часов в поле **Раз в <количество> ч**;
   - **Ежесуточно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут**;
   - **Еженедельно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
   - **При запуске программы**, если хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security 2.1;
   - **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.

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

Значение **Запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики Kaspersky Security Center.

5. На закладке **Дополнительно** настройте в соответствии с вашими требованиями следующие параметры расписания.

   - В блоке **Параметры остановки задачи**:

     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.

     b. Установите флажок **Приостановить с … до** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.

   - В блоке **Дополнительные параметры**:

     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.

     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.

     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **Применить**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Включение и выключение запуска по расписанию

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

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:

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

   > Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
4. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Использование учетных записей для запуска задач

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

В этом разделе

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Embedded Systems Security 2.1:

- задачи автоматической генерации правил контроля устройств и контроля запуска программ;
- задачи проверки по требованию;
- задачи обновления.

По умолчанию указанные задачи выполняются с правами системной учетной записи.

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

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом компьютере в сети;

- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной проверкой подлинности Microsoft Windows (NTLM-authentication);

- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к каким-либо из проверяемых объектов (например, к файлам в общих сетевых папках компьютера);

- в задаче автоматической генерации правил, если после окончания выполнения задачи сформированные правила импортируются в конфигурационный файл, который расположен по недоступному для системной учетной записи пути (например, в одной из общих сетевых папок компьютера).

Вы можете запускать задачи обновления, проверки по требованию и автоматической генерации правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Embedded Systems Security 2.1 обращается к папкам общего доступа на другом компьютере в сети, если этот компьютер зарегистрирован в одном домене с защищаемым компьютером. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Embedded Systems Security 2.1 будет обращаться к компьютеру с правами учетной записи <имя домена \ имя компьютера>.

Указание учетной записи для запуска задачи

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню названия задачи, для которой хотите настроить запуск с правами учетной записи.

2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.

3. В открывшемся окне на закладке **Запуск с правами** выполните следующие действия:

    a. Выберите пункт **Имя пользователя**.

    b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

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

    c. Подтвердите введенный пароль.

4. Нажмите на кнопку **Применить**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

Этот раздел содержит информацию об экспорте параметров работы Kaspersky Embedded Systems Security 2.1 или параметров работы отдельных компонентов программы в конфигурационный файл в формате XML и импорте этих параметров из конфигурационного файла в программу.

В этом разделе

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Embedded Systems Security 2.1 в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security 2.1 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 2.1, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Embedded Systems Security 2.1:

- Постоянная защита файлов.
- Использование KSN.
- Контроль устройств.
- Контроль запуска программ.
- Генерация правил контроля устройств.
- Генерация правил контроля запуска программ.
- Проверка по требованию.
- Обновление баз и модулей Kaspersky Embedded Systems Security 2.1.
- Карантин.
- Резервное хранилище.
- Журналы.
- Уведомления администратора и пользователей.
- Доверенная зона.

Также вы можете сохранять в файле общие параметры Kaspersky Embedded Systems Security 2.1 и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Embedded Systems Security 2.1 экспортирует все пароли, которые используются для работы программы, например, учетные данные для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Вы можете импортировать пароли только с помощью Kaspersky Embedded Systems Security 2.1, установленного на этом же компьютере, если он не был переустановлен или обновлен.

Вы не можете импортировать ранее сохраненные пароли с помощью Kaspersky Embedded Systems Security 2.1, установленного на другом компьютере. После импорта параметров на другом компьютере вам нужно ввести все пароли вручную.

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

Вы можете импортировать параметры из конфигурационного файла, содержащего параметры только некоторых компонентов Kaspersky Embedded Systems Security 2.1 (например, созданного в Kaspersky Embedded Systems Security 2.1, который был установлен с неполным набором компонентов). После импорта параметров в Kaspersky Embedded Systems Security 2.1 изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

Импортируемые параметры задач не применяются во время выполнения задачи. Для применения импортированных параметров необходимо перезапустить задачу.

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

Экспорт параметров

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выполните одно из следующих действий:

- В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Embedded Systems Security 2.1.

- В контекстном меню названия задачи, параметры которой вы хотите экспортировать, и выберите пункт **Экспортировать параметры,** чтобы экспортировать параметры отдельного функционального компонента программы.

- Чтобы экспортировать параметры компонента Доверенная зона:

  a. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

  b. Выберите пункт **Настроить параметры доверенной зоны**.

  Откроется окно **Доверенная зона**.

  c. Нажмите на кнопку **Экспорт**.

  Откроется окно приветствия мастера экспорта параметров.

2. Выполните инструкции в окнах мастера: задайте имя конфигурационного файла, в котором вы хотите сохранить параметры, и путь к файлу.

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

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

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

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

Импорт параметров

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выполните одно из следующих действий:

   - В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Embedded Systems Security 2.1.

   - В контекстном меню названия задачи, параметры которой вы хотите импортировать, и выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.

   - Чтобы импортировать параметры компонента Доверенная зона:

     a. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

     b. Выберите пункт **Настроить параметры доверенной зоны**.

     Откроется окно **Доверенная зона**.

     c. Нажмите на кнопку **Импорт**.

     Откроется окно приветствия мастера импорта параметров.

2. Выполните инструкции в окнах мастера: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После того как вы импортируете общие параметры Kaspersky Embedded Systems Security 2.1 или его функциональных компонентов на компьютере, вы не сможете вернуть их прежние значения.

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

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.

4. В панели инструментов Консоли Kaspersky Embedded Systems Security 2.1 нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли.

Kaspersky Embedded Systems Security 2.1 не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом компьютере или на том же компьютере, после того как на нем переустановили или обновили Kaspersky Embedded Systems Security 2.1. После завершения импорта вам нужно ввести пароли вручную.

Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Embedded Systems Security 2.1.

В этом разделе

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security 2.1.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Embedded Systems Security 2.1:

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

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

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел «Применение шаблона параметров безопасности« на стр. 88).
- Если вложенные узлы являются виртуальными. Вам нужно применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке файловых ресурсов компьютера выберите узел, параметры безопасности которого хотите сохранить в шаблон.
4. В нижней части окна нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.

5. В поле **Название шаблона** введите название шаблона.

6. В поле **Описание** введите любую дополнительную информацию о шаблоне.

7. Нажмите на кнопку **ОК**.

Шаблон с набором значений параметров безопасности будет сохранен.

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

Просмотр параметров безопасности в шаблоне

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите задачу, шаблон безопасности которой хотите просмотреть.

2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.

3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.

4. Нажмите на кнопку **Просмотреть**.

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

Применение шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке файловых ресурсов компьютера откройте контекстное меню узла, для которого вы хотите применить шаблон.
4. Выберите **Применить шаблон → <Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню названия настраиваемой задачи.
6. Выберите пункт **Сохранить задачу**.

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

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

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

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите задачу, параметры безопасности которой хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.

3. В дереве или списке файловых ресурсов компьютера выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем вложенным узлам.

4. Выберите **Применить шаблон → <Имя шаблона>**.

5. В дереве Консоли откройте контекстное меню настраиваемой задачи.

6. Выберите пункт **Сохранить задачу**.

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

Удаление шаблона параметров безопасности

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите задачу, для настройки которой больше не хотите использовать шаблон параметров безопасности.

2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

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

   Откроется окно **Шаблоны**.

3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения операции удаления.

5. В открывшемся окне нажмите на кнопку **Да**. Выбранный шаблон будет удален.

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

Постоянная защита

Этот раздел содержит информацию о задачах постоянной защиты: задаче Постоянная защита файлов и задаче Использование KSN.Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты и по настройке параметров безопасности защищаемого компьютера.

В этом разделе

Постоянная защита файлов

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

В этом разделе

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Embedded Systems Security 2.1 проверяет следующие объекты защищаемого компьютера при доступе к ним:

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

Когда какая-нибудь программа записывает на компьютер или считывает с него файл, Kaspersky Embedded Systems Security 2.1 перехватывает этот файл, проверяет его на наличие угроз компьютерной безопасности и, если находит угрозу, выполняет действия, указанные в параметрах задачи вами или по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Kaspersky Embedded Systems Security 2.1 возвращает файл программе, если он не заражен или успешно вылечен.

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Embedded Systems Security 2.1 обработал с момента запуска задачи по текущий момент.

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

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

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

Вы можете просмотреть следующую информацию об объектах, которые Kaspersky Embedded Systems Security 2.1 обработал с момента запуска задачи по текущий момент (см. таблицу ниже).

Таблица 14. Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Embedded Systems Security 2.1. Например, если Kaspersky Embedded Systems Security 2.1 обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 признал зараженными, или обнаруженных объектов, являющихся легальными программами, которые не были исключены из области действия задач постоянной защиты или проверки.
Возможно зараженных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 признал возможно зараженными.
Объектов не вылечено	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 не вылечил по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые Kaspersky Embedded Systems Security 2.1 не удалось проверить, например, если доступ к объекту был заблокирован другой программой.

Поле	Описание
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Kaspersky Embedded Systems Security 2.1 попытался сохранить в резервном хранилище, но это ему не удалось, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Embedded Systems Security 2.1 сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Embedded Systems Security 2.1 пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 пропустил, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые Kaspersky Embedded Systems Security 2.1 обработал.

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

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

Настройка параметров задачи Постоянная защита файлов

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

Таблица 15. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь компьютер, исключая виртуальные диски.	Вы можете ограничить область защиты.
Уровень безопасности	Единый для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для выбранных узлов в дереве файловых ресурсов компьютера вы можете: • применить другой предустановленный уровень безопасности; • вручную изменить уровень безопасности; • сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Режим защиты объектов	При открытии и изменении.	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security 2.1 проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.

Параметр	Значение по умолчанию	Описание
Доверенная зона	Применяется. Исключаются файлы, рекомендованные корпорацией Microsoft, если при установке Kaspersky Embedded Systems Security 2.1 вы выбрали **Добавить к исключениям файлы, рекомендованные Microsoft**.	Единый список исключений, который вы можете применять в выбранных задачах.
Использование служб KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Расписание запуска задачи	При запуске программы	Вы можете настраивать параметры запуска задачи по расписанию.

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

1. В зависимости от используемого интерфейса программы, выполните следующие действия:

   - Если вы хотите настроить параметры задачи локально, в дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите **Постоянная защита** → **Постоянная защита файлов.** Затем, в панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Свойства**.

   - Если вы хотите настроить параметры политики, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Настройка** (блок **Постоянная защита файлов**).

- Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно **Параметры задачи** в Kaspersky Security Center.

Откроется окно **Параметры задачи**.

2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим защиты объектов (см. раздел «Выбор режима защиты объектов» на стр. 97);
     - Применение эвристического анализатора (на стр. 98);
     - Параметры интеграции с другими компонентами Kaspersky Embedded Systems Security 2.1 (см. раздел «Интеграция задачи с другими компонентами Kaspersky Embedded Systems Security 2.1» на стр. 99).
   - На закладках **Расписание** и **Дополнительно**:
     - Параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).
3. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров будут сохранены.
4. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
5. Выполните следующие действия:
   - В дереве или списке файловых ресурсов компьютера выберите узлы, которые хотите включить в область защиты задачи (см. раздел «Об области защиты в задаче Постоянная защита файлов« на стр. 106).
   - Выберите один из предустановленных уровней безопасности (см. раздел «Выбор предустановленных уровней безопасности« на стр. 115) или настройте параметры защиты объектов вручную (см. раздел «Настройка параметров безопасности вручную« на стр. 118).
6. В контекстном меню названия задачи выберите пункт **Сохранить**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. Блок **Режим защиты объектов** позволяет определить, при каком типе доступа к объектам Kaspersky Embedded Systems Security 2.1 их проверяет.

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

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:

   - **Интеллектуальный режим**.

     Kaspersky Embedded Systems Security 2.1 выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security 2.1 повторно проверяет объект только после его последнего сохранения этим процессом.

   - **При открытии и изменении**.

     Kaspersky Embedded Systems Security 2.1 проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

     Этот вариант выбран по умолчанию.

- **При открытии**.

  Kaspersky Embedded Systems Security 2.1 проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.

- **При выполнении**.

  Kaspersky Embedded Systems Security 2.1 проверяет файл только при открытии на выполнение.

5. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

Применение эвристического анализатора

В задаче Постоянная защита файлов вы можете применять эвристический анализатор и настраивать уровень анализа.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

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

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

   Существуют следующие уровни детализации проверки:

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

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

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

6. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

Интеграция задачи с другими компонентами Kaspersky Embedded Systems Security 2.1

В задаче Постоянная защита файлов вы можете настроить параметры интеграции задачи с другими функциональными компонентами Kaspersky Embedded Systems Security 2.1.

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

Если вы приняли Положение о KSN во время установки программы, задача Использование KSN будет запускаться автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы также можете вручную запустить выполнение задачи (см. раздел «Запуск и остановка задачи Использование KSN« на стр. 128) или настроить ее запуск по расписанию (см. раздел «Настройка параметров задачи Использование KSN« на стр. 128).

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Интеграция с другими компонентами** настройте следующие параметры:

   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

     По умолчанию флажок установлен.

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

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

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

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

По умолчанию флажок установлен.

5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены.

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

По умолчанию Kaspersky Embedded Systems Security 2.1 проверяет файлы, имеющие следующие расширения:

- *386*;
- *acm*;
- *ade*, *adp*;
- *asp*;
- *asx*;
- *ax*;
- *bas*;
- *bat*;
- *bin*;
- *chm*;
- *cla*, *clas**;
- *cmd*;

- *com*;
- *cpl*;
- *crt*;
- *dll*;
- *dpl*;
- *drv*;
- *dvb*;
- *dwg*;
- *efi*;
- *emf*;
- *eml*;
- *exe*;
- *fon*;
- *fpm*;
- *hlp*;
- *hta*;
- *htm*, *html**;
- *htt*;
- *ico*;
- *inf*;
- *ini*;
- *ins*;
- *isp*;
- *jpg*, *jpe*;
- *js*, *jse*;

- *lnk*;
- *mbx*;
- *msc*;
- *msg*;
- *msi*;
- *msp*;
- *mst*;
- *nws*;
- *ocx*;
- *oft*;
- *otm*;
- *pcd*;
- *pdf*;
- *php*;
- *pht*;
- *phtm**;
- *pif*;
- *plg*;
- *png*;
- *pot*;
- *prf*;
- *prg*;
- *reg*;
- *rsc*;
- *rtf*;

- *scf*;
- *scr*;
- *sct*;
- *shb*;
- *shs*;
- *sht*;
- *shtm**;
- *swf*;
- *sys*;
- *the*;
- *them**;
- *tsp*;
- *url*;
- *vb*;
- *vbe*;
- *vbs*;
- *vxd*;
- *wma*;
- *wmf*;
- *wmv*;
- *wsc*;
- *wsf*;
- *wsh*;
- *do?*;
- *md?*;

- *mp?*;
- *ov?*;
- *pp?*;
- *vs?*;
- *xl?*.

Область защиты в задаче Постоянная защита файлов

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

В этом разделе

Об области защиты в задаче Постоянная защита файлов

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы компьютера. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли Kaspersky Embedded Systems Security 2.1 область защиты представляет собой дерево или список файловых ресурсов компьютера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

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

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

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

☑ Узел включен в область защиты.

☐ Узел исключен из области защиты.

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

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

Имена виртуальных узлов области защиты отображаются шрифтом синего цвета.

Предопределенные области защиты

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

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

В Kaspersky Embedded Systems Security 2.1 предусмотрены следующие предопределенные области защиты:

- **Локальные жесткие диски**. Kaspersky Embedded Systems Security 2.1 защищает файлы на жестких дисках компьютера.
- **Съемные диски**. Kaspersky Embedded Systems Security 2.1 защищает файлы на внешних устройствах, например, 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 2.1 защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на компьютере. Kaspersky Embedded Systems Security 2.1 не защищает файлы в сетевых папках, когда к ним обращаются программы с других компьютеров.
- **Виртуальные диски**. Вы можете включать в область защиты динамические папки и файлы, а также диски, которые монтируются на компьютер временно, например, общие диски кластера.

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

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

Псевдодиски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Embedded Systems Security 2.1. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на компьютере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Настройка параметров отображения файловых ресурсов области защиты

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:

   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.
   - Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

   По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

5. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** будет закрыто. Настроенные параметры задачи будут применены.

Формирование области защиты

Процедура формирования области защиты в задаче Постоянная защита файлов зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел «Настройка параметров отображения файловых ресурсов области защиты« на стр. 108). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

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

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В левой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:

   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:

- если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на компьютере, установите флажок **Съемные диски**);
- если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**;
- если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.

6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** будет закрыто. Настроенные параметры задачи будут сохранены.

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:

   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В открывшемся окне **Добавление области защиты** выберите тип объекта, который вы хотите добавить в область защиты:

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

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

5. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:

   a. Откройте контекстное меню области защиты по правой клавише мыши.

   b. В контекстном меню выберите пункт **Добавить исключение**.

   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.

6. Чтобы изменить добавленную область защиты или исключение, в контекстном меню области, которую хотите изменить, выберите пункт **Изменить область**.

7. Чтобы скрыть отображение ранее добавленной области защиты или исключения в списке файловых ресурсов, в контекстном меню области, которую хотите скрыть, выберите пункт **Удалить из списка**.

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

8. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** будет закрыто. Настроенные параметры задачи будут сохранены.

Вы можете запустить задачу **Постоянная защита файлов,** если по крайней мере один узел файловых ресурсов компьютера включен в область защиты.

Если вы укажете сложную область защиты, например, установите различные значения параметров безопасности для многих отдельных узлов в дереве файловых ресурсов компьютера, это может привести к замедлению проверки объектов при доступе.

О виртуальной области защиты

Kaspersky Embedded Systems Security 2.1 может проверять не только существующие папки и файлы на жестких и съемных дисках, но и папки и файлы, которые динамически создаются на компьютере различными программами и службами.

Если вы включили в область защиты все объекты компьютера, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для этих динамических узлов или вы выбрали для постоянной защиты не весь компьютер, а отдельные области, то, для того, чтобы включить в область защиты динамические диски, файлы или папки, вам нужно предварительно создать их в Консоли Kaspersky Embedded Systems Security 2.1 – задать виртуальную область защиты. Созданные вами диски, файлы и папки существуют только в Консоли Kaspersky Embedded Systems Security 2.1, но не в структуре файловой системы защищаемого компьютера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, динамические папки или файлы, которые появятся в ней, не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли Kaspersky Embedded Systems Security 2.1 и добавить их в область защиты.

Создание виртуальной области защиты

Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел «Настройка параметров отображения файловых ресурсов области защиты« на стр. 108).

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. Откройте контекстное меню узла **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.
6. Установите флажок рядом с добавленным диском, чтобы включить этот диск в область защиты.
7. В контекстном меню названия задачи выберите пункт **Сохранить**.

Настроенные параметры задачи будут сохранены.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

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

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

6. В поле ввода задайте имя для папки или файла.
7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
8. В контекстном меню названия задачи выберите пункт **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задаче Постоянная защита файлов

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

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

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

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

Выбор предустановленных уровней безопасности

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

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Embedded Systems Security 2.1 на компьютерах, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

Рекомендуемый

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

Максимальная защита

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

Таблица 16. Предустановленные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Защита объектов	По расширению	По формату	По формату
Оптимизация	Включена	Включена	Выключена
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Помещать на карантин	Помещать на карантин	Помещать на карантин
Исключать объекты	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	• Упакованные объекты* • Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* • Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* *Все объекты

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

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

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

   В окне отобразится список значений параметров безопасности, соответствующих выбранному вами уровню безопасности.
7. В контекстном меню названия задачи выберите пункт **Сохранить**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый** (см. раздел «**Выбор предустановленных уровней безопасности**» на стр. 115).

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

При работе с деревом файловых ресурсов параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

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

   Для выбранной области защиты вы можете применить предварительно созданный шаблон с набором параметров безопасности (см. раздел «О шаблонах параметров безопасности» на стр. 85).
5. Настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, настройте следующие параметры:

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

- **Все объекты**.

  Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

- **Объекты, проверяемые по формату**.

  Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании формата файла.

  Список форматов составляется специалистами «Лаборатории Касперского» и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**.

  Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами «Лаборатории Касперского» и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по указанному списку расширений**.

  Kaspersky Embedded Systems Security 2.1 проверяет файлы на основании расширения файла. Список расширения файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

- **Загрузочные секторы дисков MBR**.

  Включение защиты загрузочных секторов дисков и главных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет загрузочные секторы и загрузочные надписи на жестких и съемных дисках компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**.

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет дополнительные потоки файлов и папок.

  По умолчанию флажок установлен.

В блоке **Оптимизация** установите или снимите флажок:

- **Проверка только новых и измененных файлов**.

  Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security 2.1 новыми или измененными с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет и защищает все файлы.

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

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 2.1 проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые SFX-архивы**.

  Проверка архивов, имеющих в своем составе программный модуль-распаковщик.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает исполняемые файлы, упакованные программами-упаковщиками, при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

> Вы можете выбрать защиту всех или только новых составных объектов, если установлен флажок **Защита только новых и измененных файлов**. Если флажок **Защита только новых и измененных файлов** снят, Kaspersky Embedded Systems Security 2.1 защищает все указанные составные объекты.

- На закладке **Действия**, если требуется, настройте следующие параметры:

  - выберите действие над зараженными и другими обнаруживаемыми объектами;
  - выберите действие над возможно зараженными объектами;
  - настройте действия над объектами в зависимости от типа обнаруженного объекта;
  - выберите действия над неизменяемыми контейнерами: снимите или установите флажок **Форсировать удаление родительского файла-контейнера при обнаружении вложенного зараженного или другого объекта**, если изменение контейнера невозможно.

Флажок включает или выключает форсированное удаление родительского файла-контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта.

Если флажок установлен и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 принудительно выполняет удаление всего родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта. Принудительное удаление родительского контейнера со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если родительский контейнер неизменяем).

Если флажок снят и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 не выполняет указанное действие для родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта в случае, если родительский контейнер неизменяем.

По умолчанию флажок установлен для уровня безопасности **Максимальная защита**. По умолчанию флажок снят для уровней безопасности **Рекомендуемый** и **Максимальное быстродействие**.

- На закладке **Производительность**, если требуется, настройте следующие параметры:

  В блоке **Исключения**:

  - **Исключать файлы**.

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

    Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные объекты.

    Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

    По умолчанию флажок снят.

- **Не обнаруживать**.

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные обнаруживаемые объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

В блоке **Дополнительные параметры**:

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

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

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

  Если флажок снят, максимальная продолжительность проверки не ограничена.

  По умолчанию флажок установлен.

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

  Исключение из проверки составных объектов больше указанного размера. По умолчанию установлено значение 8 МБ.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет составные объекты, не учитывая размер.

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

- **Использовать технологию iChecker**.

  Проверка только новых или измененных с момента последней проверки файлов.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет файлы, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

- **Использовать технологию iSwift**.

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Использование KSN

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

В этом разделе

О задаче Использование KSN

Kaspersky Security Network (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Embedded Systems Security 2.1 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 2.1 получает от Kaspersky Security Network только информацию о репутации программ.

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

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

Подробная информация о локальной обработке данных содержится в разделе "О предоставлении данных" в Руководстве администратора Kaspersky Embedded Systems Security 2.1.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Embedded Systems Security 2.1. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network может использоваться в следующих задачах Kaspersky Embedded Systems Security 2.1:

- Постоянная защита файлов (см. раздел «Настройка параметров задачи Постоянная защита файлов« на стр. 94).
- Проверка по требованию (см. раздел «Настройка параметров задач проверки по требованию« на стр. 239).
- Контроль запуска программ (см. раздел «Настройка параметров задачи Контроль запуска программ« на стр. 146).

Использование Локального KSN

Подробную информацию о том, как настроить Локальный Kaspersky Security Network (также "Kaspersky Private Security Network"), вы можете прочитать в *Справочной системе Kaspersky Security Center*.

Если вы используете Локальный KSN на защищаемом компьютере, в окне **Обработка данных** (см. раздел "Настройка обработки данных" на стр.) задачи Использование KSN вы можете прочитать Положение о KPSN и включить или выключить использование компонента в любой момент с помощью флажка **Я принимаю условия участия в Kaspersky Private**

Security Network. Принимая условия, вы соглашаетесь отправлять все типы данных (запросы безопасности, статистические данные), предусмотренные в Положении о KPSN, в службы KSN.

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

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

Настройка параметров задачи Использование KSN

По умолчанию задача Использование KSN имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 17. Параметры по умолчанию задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Embedded Systems Security 2.1 будет выполнять над объектами, имеющими репутацию зараженных в KSN.
Отправка данных	Контрольная сумма файла (хеш MD5) 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 2.1 рассчитывает хеш MD5 для файлов любого размера.

Параметр	Значение по умолчанию	Описание
Положение о KSN	Флажок **Я принимаю условия участия в Kaspersky Security Network** снят или установлен.	Вы можете принять Положение о KSN во время установки программы. Вы можете изменять свое решение об использовании KSN в любой момент.
Отправлять статистику Kaspersky Security Network	Флажок установлен (Активно, если принтяно Положение о KSN)	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимите флажок.
Отправлять данные о проверенных файлах	Флажок установлен (Активно, если принтяно Положение о KSN)	Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент.
Расписание запуска задачи	Следующий запуск не определен.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Embedded Systems Security 2.1 необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалить**

Kaspersky Embedded Systems Security 2.1 удаляет зараженный по данным KSN объект и помещает его копию в резервное хранилище.

Этот вариант выбран по умолчанию.

- **Фиксировать информацию в отчете**

  Kaspersky Embedded Systems Security 2.1 фиксирует в журнале выполнения задач информацию об обнаруженном зараженном по данным KSN объекте. Kaspersky Embedded Systems Security 2.1 не удаляет зараженный объект.

- В блоке **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 2.1 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (МБ).

    Если флажок снят, Kaspersky Embedded Systems Security 2.1 рассчитывает контрольную сумму для файлов любого размера.

    По умолчанию флажок установлен.

  - Если требуется, в поле справа укажите максимальный размер файлов, для которых Kaspersky Embedded Systems Security 2.1 будет рассчитывать контрольную сумму.

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

   Программа будет запускать задачу Использование KSN по расписанию.

5. Нажмите на кнопку **ОК**.

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

Настройка обработки данных

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.

   Откроется окно **Обработка данных**.
4. Прочитайте Положение о Kaspersky Security Network (или Положение о Kaspersky Private Security Network, если вы используете KPSN).
5. Если вы принимаете условия, упомянутые в Положении о KSN, установите флажок **Я принимаю условия участия в Kaspersky Security Network** .
6. Для повышения уровня защиты следующие флажки установлены по умолчанию:

   - **Отправлять данные о проверенных файлах**.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отправляет контрольную сумму проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не отправляет контрольную сумму файлов в KSN.

     По умолчанию флажок установлен.

   - **Отправлять статистику Kaspersky Security Network.**

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отправляет дополнительную статистику, включая персональные данные. Данные, полученные "Лабораторией Касперского", используются

для улучшения качества программ и повышения скорости обнаружения угроз.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не отправляет дополнительную статистику.

По умолчанию флажок установлен.

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

7. Нажмите на кнопку **ОК**.

Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые Kaspersky Embedded Systems Security 2.1 обработал с момента ее запуска по текущий момент. Информация обо всех событиях, возникающих во время работы задачи, записывается в журнал выполнения задачи (см. раздел «О журналах выполнения задач« на стр. 332).

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**.

2. Выберите вложенный узел **Использование KSN**.

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

Вы можете просмотреть информацию об объектах, которые Kaspersky Embedded Systems Security 2.1 обработал за время работы задачи (см. таблицу ниже).

Таблица 18. Статистика задачи Использование KSN

Поле	Описание
Отправлено файловых запросов	Количество запросов о репутации файлов, которые Kaspersky Embedded Systems Security 2.1 отправил для проверки в службы KSN.
Получено недоверенных заключений	Количество объектов, признанных недоверенными службами KSN.
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Удалено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 удалил в результате работы задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Embedded Systems Security 2.1 сохранил в резервном хранилище.
Объектов не удалено	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 попытался удалить, но ему это не удалось, 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 Kaspersky Embedded Systems Security 2.1 попытался сохранить в резервном хранилище, но это ему не удалось, 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.

Защита от эксплойтов

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

В этом разделе

О защите от эксплойтов

Kaspersky Embedded Systems Security 2.1 предоставляет возможность защиты памяти процессов от эксплойтов, которая реализуется в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

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

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Embedded Systems Security 2.1, 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. Для выполнения удаления компонента при наличии защищенных процессов в системе может потребоваться перезагрузка защищаемого компьютера.

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Embedded Systems Security 2.1 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.

Если при удалении Агент внедрен хотя бы в один из защищаемых процессов, требуется перезагрузка защищаемого компьютера.

Служба Kaspersky Security Broker Host

Для максимальной эффективности выполнения функций компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Broker Host на защищаемом компьютере. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемом компьютере создается и запускается процесс kavfswh, который обеспечивает сообщение информации о защищаемых процессах от компонента к Агенту защиты.

После остановки службы Kaspersky Security Broker Host Kaspersky Embedded Systems Security 2.1 продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники снижения рисков для защиты памяти процессов.

В случае остановки службы Kaspersky Security Broker Host программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе, данные

об атаках эксплойтов, завершении процессов). Также Агент не сможет получать данные о новых параметрах защиты и о добавлении новых процессов в список защищаемых процессов.

Режимы защиты от эксплойтов

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

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

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень критический в операционной системе, Kaspersky Embedded Systems Security 2.1 не выполняет завершение такого процесса, независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- Только статистика: применяйте данный режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в Журнале нарушений безопасности.

  Если выбран данный режим, Kaspersky Embedded Systems Security 2.1 фиксирует все попытки эксплуатации уязвимостей посредством создания событий.

Настройка параметров защиты памяти процессов

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

1. Выберите основной узел **Kaspersky Embedded Systems Security 2.1** в дереве Консоли.

2. В панели результатов узла в блоке **Защита** перейдите по ссылке **Только статистика**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.

3. Настройте основные параметры защиты памяти процессов:

   - **Защищать память процессов от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не защищает процессы на компьютере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Embedded Systems Security 2.1 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 2.1 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 2.1 обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим *Только сообщать об эксплойте*.

4. В блоке **Действия по снижению рисков** настройте следующие параметры:

   - **Сообщать о скомпрометированных процессах посредством службы терминалов**

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 выводит на экран терминальное окно с описанием причины срабатывания защиты и указанием на процесс, где была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не будет

выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса.

Терминальное окно отображается независимо от статуса работы службы Kaspersky Security Broker Host.

По умолчанию флажок установлен.

- **Применять защиту от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет снижать риски эксплуатации уязвимостей уже запущенных процессов не зависимо от статуса выполнения службы Kaspersky Security. Kaspersky Embedded Systems Security 2.1 не будет защищать процессы, которые были добавлены после остановки службы Kaspersky Security. После того как служба будет запущена, снижение рисков эксплуатации уязвимостей всех процессов будет остановлено.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

  По умолчанию флажок установлен.

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

   Kaspersky Embedded Systems Security 2.1 сохранит и применит настроенные параметры защиты процессов.

Добавление защищаемого процесса

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

1. Выберите основной узел **Kaspersky Embedded Systems Security 2.1** в дереве Консоли.
2. В панели результатов узла в блоке **Защита** перейдите по ссылке **Защита от эксплойтов**.

   Откроется окно **Область защиты**.
3. Добавьте процесс в список защищаемых процессов, выполнив следующие действия:

   a. Нажмите на кнопку **Обзор**.

   Откроется стандартное окно Microsoft Windows **Открыть**.

   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.

   c. Нажмите на кнопку **Открыть**.

   d. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.
4. Выберите добавленный процесс в списке.
5. На закладке **Параметры защиты процесса** отобразятся текущие настройки:

   - **Статус**.
   - **Пусть к исполняемому файлу**.
   - **Техники снижения рисков**.
6. Чтобы отредактировать применяемые к данному процессу техники снижения рисков, выберите закладку **Техники снижения рисков**.
7. Выберите один из вариантов применения техник снижения рисков:

- **Применять все доступные техники снижения рисков**.

  Если выбран этот вариант, редактирование списка недоступно, все техники применяются по умолчанию.

- **Применять указанные техники снижения рисков**.

  Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска, установив флажки напротив техник, которые хотите применять.

8. В блоке **Запуск модулей из процесса** вы можете настроить параметры работы техники снижения риска **Attack Surface Reduciton**:

   - Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать модули**.

   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, запуск модулей в которых вы хотите разрешить:

     - Интернет
     - Интранет
     - Доверенные сайты
     - Сайты с ограниченным доступом
     - Компьютер

     > Данные параметры применимы только для Internet Explorer.

9. Нажмите на кнопку **ОК**.

Техники снижения рисков

Таблица 19. Техники снижения рисков

Техника снижения рисков	Описание
Data Execution Prevention (DEP)	Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.
Address Space Layout Randomization (ASLR)	Изменение расположения структур данных в адресном пространстве процесса.
Structured Exeption Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Export Adress Table Access Moitor (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
Heapspray Allocation	Защита от выделения памяти под исполнение вредоносного кода.

Техника снижения рисков	Описание
Execution Flow Simulation (Anti Return Oriented Programming)	Обнаружение подозрительных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile.
Attack Surface Reduction	Блокирование запуска уязвимых модулей через защищаемый процесс.

Контроль компьютера

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.1, которая позволяет контролировать запуски программ, подключения флеш-накопителей и других внешних устройств по USB, а также контролировать работу сетевого экрана Windows.

В этом разделе

Контроль запуска программ

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

В этом разделе

О задаче Контроль запуска программ

В ходе выполнения задачи Контроль запуска программ Kaspersky Embedded Systems Security 2.1 отслеживает попытки запуска программ пользователями и разрешает или запрещает их запуск. Основой работы задачи Контроль запуска программ является технология блокировки по умолчанию (Default Deny), которая предполагает автоматическое блокирование запуска любых программ, неразрешенных в параметрах задачи.

Вы можете разрешить запуск программ одним из следующих способов:

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

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

> Все попытки запуска программ фиксируются в журнале выполнения задач (см. раздел «О журналах выполнения задач« на стр. 332).

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

- **Применять правила контроля запуска программ**. Kaspersky Embedded Systems Security 2.1 контролирует с помощью заданных правил запуск программ, которые подпадают под область применения правил задачи Контроль запуска программ. Область применения правил задачи Контроль запуска программ указывается в параметрах этой задачи. Если программа подпадает под область применения правил задачи Контроль запуска программ, и ее параметры не удовлетворяют ни одному из правил контроля запуска программ, то запуск такой программы запрещен.

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

Запуск задачи Контроль запуска программ в режиме **Применять правила контроля запуска программ** невозможен, если не создано ни одно правило или количество созданных правил для одного компьютера превышает порог в 65 535 правил.

- **Только статистика**. Kaspersky Embedded Systems Security 2.1 не контролирует запуск программ с помощью правил, а только фиксирует в журнале выполнения задач информацию о запусках программ и правилах контроля запуска программ, которым удовлетворяют запущенные программы. Запуск всех программ разрешен. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации, зафиксированной в журнале выполнения задач (см. раздел «Формирование списка правил по событиям задачи Контроль запуска программ« на стр. 172).

Вы можете построить работу задачи Контроль запуска программ в соответствии с одним из следующих сценариев:

- Расширенная настройка правил и их применение для контроля запуска программ.
- Минимальная настройка правил и использование KSN для контроля запуска программ (см. раздел «Использование KSN в задаче Контроль запуска программ« на стр. 152).

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Настройка параметров задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 20. Параметры задачи Контроль запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только статистика**. Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Применять правила контроля запуска программ** для защиты компьютера после того, как будет сформирован окончательный список правил.
Область применения правил в задаче	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.
Использование KSN	Данные о репутации программ в KSN не используются.	Вы можете использовать заключения о репутации программ в KSN в работе задачи Контроль запуска программ.

Параметр	Значение по умолчанию	Описание
Разрешение распространения программ для указанных пакетов установки	Не применяется.	Вы можете автоматически разрешать установку или обновление программного обеспечения через указанные пакеты установки.
Разрешение распространения программ через Windows Installer	Применяется.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются через Windows Installer.
Расписание запуска задачи	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел «Выбор режима работы задачи Контроль запуска программ« на стр. 148).
     - Область применения правил в задаче (см. раздел «Формирование области применения задачи Контроль запуска программ« на стр. 150).

- Использование KSN (см. раздел «Использование KSN в задаче Контроль запуска программ« на стр. 152).

- На закладке **Контроль пакетов установки**:

  - Параметры контроля распространения программного обеспечения (см. раздел «Формирование списка доверенных пакетов установки« на стр. 155).

- На закладках **Расписание** и **Дополнительно**:

  - Параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

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

   Изменения параметров будут сохранены.

6. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

7. Если требуется, отредактируйте список правил контроля запуска программ.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль запуска программ**.

3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи** на закладке **Общие**.

4. В списке **Режим работы задачи Контроль запуска программ** укажите режим выполнения задачи.

   В раскрывающемся списке вы можете выбрать один из режимов работы задачи Контроль запуска программ:

   - **Применять правила контроля запуска программ**. Kaspersky Embedded Systems Security 2.1 контролирует запуск программ с помощью заданных правил.
   - **Только статистика**. Kaspersky Embedded Systems Security 2.1 не контролирует запуск программ с помощью заданных правил, а только фиксирует в журнале выполнения задач информацию о запусках программ. Запуск всех программ разрешен. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации, зафиксированной в журнале выполнения задач.

   По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

5. Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска** .

   Флажок включает или выключает контроль повторного запуска программ на основе записей кеша о прецедентах.

   Если флажок установлен, Kaspersky Embedded Systems Security 2.1 запрещает или разрешает выполнение повторно запущенной программы на основе решения, которое было принято при первом запуске программы задачей контроля запуска программ. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом событии сохраняется в кеше и повторный запуск этой программы будет разрешен без повторной проверки на наличие разрешающих правил.

   Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет программу при каждом ее последующем запуске заново.

По умолчанию флажок установлен.

Kaspersky Embedded Systems Security 2.1 заводит новый список прецедентов в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом запуск программ контролируется в соответствии с актуальными настройками безопасности.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Формирование области применения задачи Контроль запуска программ

► *Чтобы сформировать область применения задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Область применения правил** задайте следующие параметры:

   - **Использовать правила для исполняемых файлов**.

     Флажок включает / выключает контроль запуска исполняемых файлов программ.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 разрешает или запрещает запуск исполняемых файлов программ с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не контролирует запуск исполняемых файлов программ с помощью заданных правил. Запуск исполняемых файлов программ разрешен.

По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**.

  Флажок включает / выключает контроль загрузки DLL-модулей.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 разрешает или запрещает загрузку DLL-модулей с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

  Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

  По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**.

  Флажок включает или выключает контроль запуска скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 2.1 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Использование KSN в задаче Контроль запуска программ

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

> Если вы приняли Положение о KSN во время установки программы, задача Использование KSN будет запускаться автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы также можете вручную запустить выполнение задачи (см. раздел «Запуск и остановка задачи Использование KSN« на стр. 128) или настроить ее запуск по расписанию (см. раздел «Настройка параметров задачи Использование KSN« на стр. 128).

При использовании данных KSN о репутации программ в задаче Контроль запуска программ репутация программы в KSN является критерием разрешения или блокировки запуска этой программы. Если при попытке запуска программы Kaspersky Embedded Systems Security 2.1 получает недоверенное заключение KSN, запуск такой программы запрещен. Если при попытке запуска программы Kaspersky Embedded Systems Security 2.1 получает доверенное заключение KSN, запуск такой программы разрешен. Вы можете применять KSN совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом компьютере без расширенной настройки списка правил.

Вы можете применять заключения KSN в работе Kaspersky Embedded Systems Security 2.1 совместно с единственным заданным правилом.Программа будет разрешать запуск только тех программ, которые имеют доверенный статус в KSN или разрешены заданным правилом.

> При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом блокировки по умолчанию. Применение KSN, при отсутствии правил, позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании KSN совместно с правилами контроля запуска программ действуют следующие сценарии:

- Kaspersky Embedded Systems Security 2.1 всегда блокирует запуск программы, если программа подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет вам вручную расширять список нежелательных программ.

- Kaspersky Embedded Systems Security 2.1 всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для такой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу, но не были учтены при предварительной настройке правил.

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль запуска программ**.

3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В блоке **Использование KSN** задайте параметры использования служб KSN:

   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые подпадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

По умолчанию флажок снят.

- Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

  Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 разрешает запуск программ, имеющих статус доверенных в KSN. При этом запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

  По умолчанию флажок снят.

- Если флажок **Разрешать запуск программ, доверенных в KSN** установлен, укажите пользователей и / или группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

a. Нажмите на кнопку **Изменить**.

Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

b. Задайте список пользователей и / или групп пользователей.

c. Нажмите на кнопку **ОК**.

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

Настроенные параметры будут сохранены.

Формирование списка доверенных пакетов установки

Формирование правил контроля запуска программ может значительно усложняться, если вам требуется учитывать распространение программного обеспечения на защищаемом компьютере: например, для компьютеров, на которых выполняется периодическое автоматическое обновление установленных программ. В этом случае требуется обновлять списки разрешающих правил при каждом обновлении программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались запуски новых файлов, созданных в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения вы можете использовать соответствующую подсистему задачи Контроль запуска программ.

Подсистема *Контроль распространения программного обеспечения* реализована в виде дополнительного списка исключений. Вы можете добавлять в этот список доверенные пакеты установки (далее также “*доверенные пакеты*”) – программа будет разрешать распаковку доверенных пакетов и автоматический запуск программного обеспечения, установленного и измененного доверенным пакетом.

Учитывайте, что программа контролирует только полный цикл распространения программного обеспечения. Kaspersky Embedded Systems Security 2.1 не сможет корректно обработать запуски файлов, измененных доверенным пакетом, если при первом запуске такого пакета установки контроль распространения программного обеспечения отключен или не установлен компонент Контроль запуска программ.

Контроль распространения программного обеспечения невозможен, если в настройках задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш контроля распространения программного обеспечения

Kaspersky Embedded Systems Security 2.1 определяет связь между файлами, созданными при распространении программного обеспечения, и доверенными пакетами с помощью динамического формирования *кеша контроля распространения программного обеспечения* (далее – *кеш распространения*). При первом запуске доверенного пакета, Kaspersky Embedded Systems Security 2.1 обнаруживает все файлы, созданные при распространении программного обеспечения с помощью данного пакета, и сохраняет их контрольные суммы и полные пути в кеше распространения. В дальнейшем запуски всех файлов, сохраненных в кеше распространения, разрешаются автоматически.

Вы не можете просматривать, очищать, а также вручную изменять кеш распространения через пользовательский интерфейс. Kaspersky Embedded Systems Security 2.1 самостоятельно наполняет его, а также контролирует его актуальность.

Вы можете экспортировать кеш распространения в конфигурационный файл (в формате XML), а также полностью очищать кеш распространения с помощью команд командной строки.

► *Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Чтобы полностью очистить кеш распространения, выполните команду:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 2.1 обновляет кеш распространения раз в сутки. Если значение полного пути или контрольной суммы ранее разрешенного файла изменены, программа удаляет запись о таком файле из кеша распространения. При активном режиме работы задачи Контроль запуска программ, дальнейшие запуски такого файла будут заблокированы.

Взаимодействие с основным списком правил контроля запуска программ

Список доверенных пакетов подсистемы контроля распространения программного обеспечения – 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 распространения программного обеспечения учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если для таких пакетов и файлов отсутствуют правила в основном списке правил контроля запуска программ.

Использование KSN заключений

Недоверенные заключения KSN имеют больший приоритет, чем исключение контроля распространения программного обеспечения: распаковка доверенного пакета установки или запуск созданных и измененных им файлов будут заблокированы, если для таких файлов получено недоверенное заключение от KSN.

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль запуска программ**.

3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**

4. На выбранной закладке установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск

файлов, запущенных с помощью доверенных пакетов установки. Список программ и пакетов для установки, разрешенных к запуску, доступен для редактирования.

Если флажок снят, программа не применяет указанные в списке исключения.

По умолчанию флажок снят.

Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если установлен флажок **Использовать правила для исполняемых файлов** в параметрах задачи Контроль запуска программ.

5. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью Windows Installer**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью подсистемы Windows Installer.

   Если флажок установлен, программа всегда разрешает запуск файлов, установленных с помощью Windows Installer.

   Если флажок снят, использование Windows Installer для запуска программы не является критерием для разрешения такой программы.

   По умолчанию флажок установлен.

   Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью Windows Installer** рекомендуется снимать только в случае крайней необходимости. Снятие флажка может привести к проблемам при обновлении файлов операционной системы, а также блокированию запуска файлов, дочерних по отношению к доверенным пакетам установки.

6. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

   Если флажок установлен, Kaspersky Embedded Systems Security 2.1 автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

   Система контролирует запуск объектов со следующими расширениями:

   - .exe
   - .msi

   По умолчанию флажок снят.

   Программа контролирует цикл распространения программного обеспечения от доставки пакета на компьютер до факта установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки системы на компьютере.

7. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в раскрывшемся меню выберите один из доступных способов:

   - **Добавить один вручную.**

     a. Нажмите на кнопку **Обзор** и выберете файл запуска программы или пакет установки.

     Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

     b. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

- **Использовать цифровой сертификат**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  Этот вариант выбран по умолчанию.

- **Использовать хеш SHA256**

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

  Этот вариант рекомендуется применять, если требуется создать максимально надежные правила: контрольная сумма, рассчитанная по алгоритму SHA256, является уникальным идентификатором файла. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Добавить несколько по хешу**.

  > Вы можете выбрать неограниченное число файлов запуска и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security 2.1 учитывает хеш и разрешает запуск при обращении операционный системы к указанным файлам.

- **Изменить выбранный**.

  Используйте этот вариант, чтобы выбрать другой файл запуска или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**.

Вы можете импортировать список доверенных пакетов установки из сохраненного конфигурационного файла. Распознаваемый Kaspersky Embedded Systems Security 2.1 файл должен удовлетворять следующим параметрам:

- иметь текстовое расширение;
- содержать информацию в виде списка строк, каждая из которых - данные для одного доверенного файла;
- содержать список, соответствующий одному из двух форматов:
  - <имя файла>:<хеш SHA256>;
  - <хеш SHA256>*<имя файла>.

В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

8. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск вложенных файлов будет разрешен.

   Чтобы запретить запуск вложенных файлов, полностью удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

9. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

О правилах контроля запуска программ

Принцип работы правил контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешать или запрещать запуск программ и называются *разрешающими* или *запрещающими*, соответственно. Для создания списков разрешающих правил контроля запуска программ вы можете использовать задачу формирования резрешающих правил (см. раздел «О задаче Генерация правил

контроля запуска программ« на стр. 174). или режим **Только статистика** в задаче Контроль запуска программ (см. раздел «Формирование списка правил по событиям задачи Контроль запуска программ« на стр. 172). Вы также можете добавлять разрешающие правила вручную (см. раздел «Добавление одного правила контроля запуска программ« на стр. 168) по одному.

- Пользователь и / или группа пользователей.

  Правила контроля запуска программ контролируют запуски программ указанными в правиле пользователем и / или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут быть применены к запускам *исполняемых файлов программ* или к запускам *скриптов* и *пакетов MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ контролируют запуск тех файлов, которые удовлетворяют указанному в параметрах правила критерию: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

  Если в качестве критерия срабатывания правила установлен параметр **Цифровой сертификат**, созданное правило контролирует запуск любых программ, доверенных в операционной системе. Вы можете задать более строгие условия для этого критерия, установив флажки:

  - **Использовать заголовок**.

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск

программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**.

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

  По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывания правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для уточнения разрешающих

правил: например, если вы хотите разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в конфигурационный файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. В списке правил выберите одно или несколько правил, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить выбранные**.

6. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль запуска программ**.

3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.

4. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.

5. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.

6. Нажмите на кнопку **Сохранить**.

Параметры правила будут экспортированы в указанный файл.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу на срабатывание правил, чтобы определить, какие правила контролируют запуск выбранной программы.

По умолчанию Kaspersky Embedded Systems Security 2.1 блокирует программы, запуск которых не контролируется ни одним правилом. Чтобы избежать блокировки запуска важных программ, вам нужно создать разрешающие правила для таких программ.

Если запуск программы контролируется несколькими правилами разных типов, приоритетными при запуске программы считаются запрещающие правила: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы протестировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
5. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все найденные правила, которые будут срабатывать при запуске указанного файла.

О формировании списка правил контроля запуска программ

Вы можете импортировать списки правил контроля запуска программ из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль запуска программ или задачи Генерация правил контроля запуска программ. Списки, содержащиеся в таких XML-файлах, могут использоваться для создания только разрешающих правил контроля запуска программ.

Запрещающие правила контроля запуска программ создаются вручную. Также запрещаются запуски программ, для которых не найдено никаких правил.

Использование задачи Генерация правил контроля запуска программ

XML-файл, сформированный по завершении задачи Генерация правил контроля запуска программ, содержит разрешающие правила для запуска программ, указанных при настройке параметров задачи во время ее запуска. Для программ, запуск которых не разрешен в заданных параметрах задачи, не будет создано ни одного правила и их запуск будет заблокирован по умолчанию.

Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Использование отчета задачи Контроль запуска программ в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль запуска программ в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Embedded Systems Security 2.1 фиксирует все запуски программ на защищаемом компьютере в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные сценарии работы защищаемого компьютера и хотя бы одна его перезагрузка.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом компьютере. Запуск задач автоматического формирования разрешающих правил и контроля запуска программ в режиме **Только статистика** для формирования списков правил рекомендуется выполнять на эталонной машине организации, чтобы учесть все используемые программы в сети.

Перед формированием списка разрешающих правил по программам, запущенным на эталонной машине организации, убедитесь, что на эталонной машине нет вредоносных программ.

Вы можете использовать списки правил, полученные по результатам анализа запуска программ на эталонной машине, при настройке политики в Kaspersky Security Center и применении созданных разрешающих правил для всей сети.

В этом разделе

Добавление одного правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется контекстное окно **Параметры правила**.
6. Укажите следующие параметры:

   a. В поле **Название** введите название правила.

   b. В раскрывающемся списке **Тип** выберите тип правила:

   - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
   - **Запрещающее**, если вы хотите, чтобы правило запрещало запуск программ в соответствии с критериями, указанными в параметрах правила.

c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

- **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
- **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.

d. В поле **Пользователь и / или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:

i. Нажмите на кнопку **Выбрать**.

ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.

iii. Задайте список пользователей и / или групп пользователей.

iv. Нажмите на кнопку **OK**.

e. Выполните следующие действия, если вы хотите взять значения для критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла:

i. Нажмите на кнопку **Задать критерий срабатывания файла из свойств файла**.

Откроется стандартное окно Microsoft Windows **Открыть**.

ii. Выберите файл и нажмите на кнопку **OK**.

Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, подписанных цифровым сертификатом:

- Установите флажок **Использовать заголовок**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
- Установите флажок **Использовать отпечаток**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным отпечатком.

- **Хеш SHA256**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, расположенных по указанному пути.

g. Выполните следующие действия, если хотите добавить исключения из правила:

i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения из правила.

iii. Укажите параметры исключения файлов запуска программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**.

Если выбран этот критерий, программа относит к исключению программы, запускаемые с помощью файлов, подписанных цифровым сертификатом.

По умолчанию выбран этот критерий.

- **Использовать заголовок**.

Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия для отнесения файлов к исключениям из правила.

Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия для отнесения файлов

к исключениям из правила. Программа относит к исключениям из правила файлы, подписанные цифровым сертификатом только с таким заголовком.

Если флажок снят, указанный заголовок цифрового сертификата не используется в качестве критерия для отнесения файлов к исключениям из правила. Если выбран критерий **Цифровой сертификат**, программа относит к исключениям из правила файлы, подписанные цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Построить исключение на основе свойств файла**.

По умолчанию флажок снят.

- **Использовать отпечаток**.

Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия для отнесения файлов к исключениям из правила.

Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия для отнесения файлов к исключениям из правила. Программа относит к исключениям из правила файлы, подписанные цифровым сертификатом только с таким отпечатком.

Если флажок снят, указанный отпечаток цифрового сертификата не используется в качестве критерия для отнесения файлов к исключениям из правила. Если выбран критерий **Цифровой сертификат**, программа относит к исключениям из правила файлы, подписанные цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Построить исключение на основе свойств файла**.

По умолчанию флажок снят.

- **Хеш SHA256**.

Если выбран этот критерий, программа относит к исключению

программу, которая запускается с помощью файла, обладающего указанной контрольной суммой.

Контрольную сумму файла вы можете указать только из свойств выбранного файла с помощью кнопки **Построить исключение на основе свойств файла**.

- **Путь к файлу**.

  Если выбран этот критерий, программа относит к исключениям программы, которые запускаются с помощью файлов, расположенных по указанному пути.

i. Нажмите на кнопку **OK**.

ii. Повторите пункты (i)-(iv) при необходимости для добавления дополнительных исключений.

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

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Формирование списка правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл со списком правил контроля запуска программ, сформированным по событиям задачи Контроль запуска программ, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел «**Выбор режима работы задачи Контроль запуска программ**« на стр. 148), чтобы зафиксировать в журнале выполнения задачи все срабатывания правил на запуски программ на защищаемом компьютере.

2. По завершении выполнения задачи в режиме **Только статистика**, откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.

3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security 2.1 создаст конфигурационный файл в формате XML со списком правил, сформированных по работе задачи Контроль запуска программ в режиме **Только статистика**. Вы можете применить этот список в задаче Контроль запуска программ (см. раздел «Импорт правил контроля запуска программ из файла формата XML« на стр. 173).

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что запуск критичных для работы компьютера программ (например, файлов операционной системы) разрешен заданными правилами.

Все события работы задачи фиксируются в журнале в ходе выполнения задачи в любом из двух режимов. Вы можете создать конфигурационный файл со списком правил по событиям задачи в режиме **Применять правила контроля запуска программ**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется формировать списки правил до запуска задачи в режиме применения правил контроля запуска программ.

Импорт правил контроля запуска программ из файла формата XML

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Импортировать правила из файла**.

6. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла**:

   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.

7. В окне Microsoft Windows **Открыть** выберите XML-файл, который содержит параметры правил контроля запуска программ.

8. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

О задаче Генерация правил контроля запуска программ

Задача Генерация правил контроля запуска программ позволяет автоматически формировать список разрешающих правил контроля запуска программ на основе указанных типов файлов из указанных папок. Например, если вы укажете в качестве параметров задачи исполняемые файлы из папки C:\Program Files (x86), программа будет автоматически формировать правила, по которым разрешается запуск этих файлов. В дальнейшем программа будет разрешать запуск программ, для которых были автоматически сформированы разрешающие правила.

Сформированные правила отображаются по ссылке **Правила контроля запуска программ** в узле **Контроль запуска программ**.

Настройка параметров задачи Генерация правил контроля запуска программ

По умолчанию задача Генерация правил контроля запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 21. Параметры задачи Генерация правил контроля запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем компьютера, на котором установлен Kaspersky Embedded Systems Security 2.1.	Вы можете изменить префикс для названий разрешающих правил.
Область применения разрешающих правил	Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов: • файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files; • пакеты MSI, расположенные в папке C:\Windows; • скрипты, расположенные в папке C:\Windows. Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.	Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы.

Параметр	Значение по умолчанию	Описание
Критерии формирования разрешающих правил	Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.	Вы можете использовать хеш SHA256 при формировании разрешающих правил. Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль запуска программ; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи автоматического формирования разрешающих правил с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Первый запуск не определен.	Задача Генерация правил контроля запуска программ не запускается автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Генерация правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Автоматическая генерация правил**.

2. Выберите вложенный узел **Генерация правил контроля запуска программ**.

3. В панели результатов узла **Генерация правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**. Настройте следующие параметры:

   - На закладке **Общие**:

     - Укажите префикс для названий правил.

       Первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя компьютера, на котором установлен Kaspersky Embedded Systems Security 2.1. Вы можете изменить префикс для названий разрешающих правил.

     - Настройте область применения разрешающих правил (см. раздел «Ограничение области действия задачи« на стр. 178).

   - На закладке **Действия** укажите действия, которые Kaspersky Embedded Systems Security 2.1 должен совершать:

     - При формировании правил (см. раздел «Действия при автоматическом формировании правил контроля запуска программ« на стр. 179).

     - По завершении задачи (см. раздел «Действия по завершении автоматического формирования правил контроля запуска программ« на стр. 182).

   - На закладках **Расписание** и **Дополнительно**:

     - Параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

   - На закладке **Запуск с правами**:

     - Параметры запуска задачи с правами учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80).

4. Нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Ограничение области действия задачи

► *Чтобы ограничить область применения задачи Генерация правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Автоматическая генерация правил**.

2. Выберите вложенный узел **Генерация правил контроля запуска программ**.

3. В панели результатов узла **Генерация правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Настройте следующие параметры задачи:

   - **Создавать разрешающие правила на основе запущенных программ**.

     Флажок включает или выключает автоматическое формирование разрешающих правил контроля запуска программ для уже запущенных программ. Этот вариант рекомендуется, если на компьютере запущен эталонный набор программ, по которому вы хотите построить разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются в соответствии с запущенными программами.

Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

По умолчанию флажок установлен.

Флажок не может быть снят, если не выбрана ни одна папка в таблице **Создавать разрешающие правила для программ из папок**.

- **Создавать разрешающие правила для программ из папок**.

  В таблице вы можете выбрать или указать области сканирования задачи и типы исполняемых файлов, которые будут учитываются при формировании правил контроля запуска программ. Задача будут формировать разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

5. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил контроля запуска программ

► *Чтобы настроить действия, которые Kaspersky Embedded Systems Security 2.1 должен совершать во время выполнения задачи Генерация правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Автоматическая генерация правил**.

2. Выберите вложенный узел **Генерация правил контроля запуска программ**.

3. В панели результатов узла **Генерация правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Откройте закладку **Действия**.

5. В блоке **При формировании разрешающих правил** настройте следующие параметры:

- **Использовать цифровой сертификат**.

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  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. В дальнейшем программа будет разрешать запуск программ, которые запускаются с помощью файлов с указанными в правиле заголовком и отпечатком цифрового сертификата.

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

  Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

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

  По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**.

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

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

- **Использовать хеш SHA256**.

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

  Этот вариант рекомендуется применять, если требуется создать максимально надежные правила: контрольная сумма, рассчитанная по алгоритму SHA256, является уникальным идентификатором файла. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать правила для пользователя и / или группы пользователей**.

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

  По умолчанию выбрана группа **Все**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил контроля запуска программ

► *Чтобы настроить действия, которые Kaspersky Embedded Systems Security 2.1 должен совершать по завершении автоматического формирования правил, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Автоматическая генерация правил**.
2. Выберите вложенный узел **Генерация правил контроля запуска программ**.
3. В панели результатов узла **Генерация правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Откройте закладку **Действия**.
5. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается по ссылке **Правила контроля запуска программ** в панели результатов узла

Контроль запуска программ.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 добавляет правила, сформированные в ходе выполнения задачи Генерация правил контроля запуска программ, в список правил контроля запуска программ согласно установленному принципу добавления.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не добавляет сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

Флажок не может быть снят, если не установлен флажок **Экспортировать разрешающие правила в файл**.

- **Принцип добавления**.

  Раскрывающийся список, позволяющий указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила дополняют список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила дополняют список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию установлен способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт сформированных разрешающих правил контроля запуска программ в файл.

  Если флажок установлен, по завершении задачи автоматического формирования разрешающих правил Kaspersky Embedded Systems Security 2.1 экспортирует сформированные правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи автоматического формирования разрешающих правил Kaspersky Embedded Systems Security 2.1 не экспортирует сформированные правила в файл, а только добавляет их в список правил контроля запуска программ.

  По умолчанию флажок снят.

  Флажок не может быть снят, если не установлен флажок **Добавлять разрешающие правила в список правил контроля запуска программ.**

- **Добавлять информацию о компьютере в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются сформированные правила контроля запуска программ.

  Если флажок установлен, программа добавляет имя защищаемого компьютера, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

  Флажок доступен, если установлен флажок **Экспортировать разрешающие правила в файл**.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Контроль устройств

Этот раздел содержит информацию о задаче Контроль устройств и инструкции по настройке ее параметров.

В этом разделе

О задаче Контроль устройств

Kaspersky Embedded Systems Security 2.1 контролирует регистрацию и использование *запоминающих устройств* и устройств чтения CD/DVD дисков в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с подключаемым по USB флеш-накопителем или внешним устройством другого типа. Запоминающее устройство - это внешнее устройство, предназначенное для записи и хранения данных.

Kaspersky Embedded Systems Security 2.1 контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители;
- устройства чтения компакт-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые мобильные устройства MTP.

Задача Контроль устройств отслеживает попытки подключения внешних устройств к защищаемому компьютеру и запрещает их использование в качестве запоминающих, если не находит разрешающих правил для этих устройств. В результате блокировки становится недоступен просмотр содержимого устройства, а также выполнение операций с файлами на этом устройстве (например, чтение или запись файлов).

Программа присваивает каждому подключаемому внешнему устройству один из двух статусов:

- *Доверенное. У*стройство, обмен данными с которым разрешен. Путь к экземпляру такого устройства подпадает под область применения хотя бы одного разрешающего правила.

- *Недоверенное.* Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область определения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Генерация правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Embedded Systems Security 2.1 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 системе Windows и определяется Kaspersky Embedded Systems Security 2.1 в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Запрещать недоверенные устройства**. Kaspersky Embedded Systems Security 2.1 контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом *блокировки по умолчанию* (Default Deny) и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру в момент запуска задачи Контроль устройств в режиме **Запрещать недоверенные устройства**, то такое устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство самостоятельно или перезагрузить компьютер, иначе принцип блокировки по умолчанию не будет применен к такому устройству.

- **Только статистика**. Kaspersky Embedded Systems Security 2.1 не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования списка правил контроля устройств на основе информации, зафиксированной в журнале выполнения задачи (см. раздел «Формирование списка правил по событиям задачи Контроль устройств« на стр. 201).

Настройка параметров задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 22. Параметры задачи Контроль устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только статистика**	Задача фиксирует в журнале выполнения события запрета и разрешения подключения внешних устройств в соответствии с заданными правилами. Фактическая блокировка использования внешних устройств не выполняется. Вы можете выбрать режим **Запрещать недоверенные устройства** для защиты компьютера, чтобы применять фактическую блокировку использования внешних устройств.
Разрешать использование всех внешних устройств, если задача Контроль устройств не выполняется	Не применяется	Kaspersky Embedded Systems Security 2.1 запрещает использование внешних устройств вне зависимости от статуса выполнения задачи Контроль устройств. Это обеспечивает максимальную защиту от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. Вы можете настраивать параметр таким образом, чтобы Kaspersky Embedded Systems Security 2.1 разрешал использование всех внешних устройств, если задача Контроль устройств не выполняется.
Расписание запуска задачи	При запуске программы	Задача Контроль устройств запускается автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы можете настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль устройств**.

3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. На закладке **Общие** настройте следующие параметры задачи:

   - В блоке **Режим работы** укажите режим работы задачи:

     - **Запрещать недоверенные устройства**.

       Kaspersky Embedded Systems Security 2.1 контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом *блокировки по умолчанию* (Default Deny) и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру в момент запуска задачи Контроль устройств в режиме **Запрещать недоверенные устройства**, то такое устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство самостоятельно или перезагрузить компьютер, иначе принцип блокировки по умолчанию не будет применен к такому устройству.

     - **Только статистика**.

       Kaspersky Embedded Systems Security 2.1 не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом компьютере,

а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

- Снимите или установите флажок **Разрешать использование всех внешних устройств, если задача Контроль устройств не выполняется**.

  Флажок разрешает или запрещает использование запоминающих устройств при остановленной задаче Контроль устройств.

  Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security 2.1 разрешает использовать любые запоминающие устройства на защищаемом компьютере.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 запрещает использовать недоверенные запоминающие устройства на защищаемом компьютере, если задача Контроль устройств не выполняется или если служба Kaspersky Security Service остановлена. Рекомендуется применять этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

  По умолчанию флажок снят.

5. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

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

   Изменения параметров будут сохранены.

7. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

8. Если требуется, отредактируйте список правил контроля устройств.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

О правилах контроля устройств

Правила создаются индивидуально для каждого устройства, подключенного в данный момент или подключавшегося ранее к защищаемому компьютеру, если данные об этом устройстве сохранились в системе.

Для создания разрешающих правил контроля устройств вы можете:

- использовать задачу генерации разрешающих правил (см. раздел «О задаче Генерация правил контроля устройств« на стр. 203);
- использовать режим **Только статистика** в задаче Контроль устройств (см. раздел «Формирование списка правил по событиям задачи Контроль устройств« на стр. 201);
- использовать данные системы о подключавшихся устройствах (см. раздел «Добавление разрешающего правила для одного или нескольких внешних устройств« на стр. 200);
- расширять область применения уже созданных правил (см. раздел «Расширение области применения правил контроля устройств« на стр. 196).

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Embedded Systems Security 2.1 - 3072.

Правила контроля устройств содержат следующие параметры:

- тип правила;
- область применения правила;
- данные исходного устройства;
- комментарий.

Тип правила

Тип правила - всегда *разрешающее*. Задача контроля устройств по умолчанию блокирует подключение всех флеш-накопителей и других внешних устройств, если они не подпадают под область действия ни одного разрешающего правила.

Критерий срабатывания и область применения правила

Правила контроля устройств идентифицируют подключаемые флеш-накопители и другие внешние устройства по значению *пути к экземпляру устройства (Device Instance Path).* Путь к экземпляру устройства является уникальным идентификатором, который присваивается устройству системой в момент его подключения и регистрации в качестве запоминающего устройства (Mass Storage) или устройства чтения CD/DVD дисков (например, IDE или SCSI).

Kaspersky Embedded Systems Security 2.1 контролирует подключение внешних устройств чтения CD/DVD дисков вне зависимости от шины подключения. При монтировании таких устройств по USB, операционная система регистрирует два значения пути к экземпляру устройства: для запоминающего устройства (Mass Storage), а также для устройства CD/DVD (например, IDE или SCSI). Для корректного подключения таких устройств требуется наличие разрешающих правил для каждого значения пути к экземпляру устройства.

Kaspersky Embedded Systems Security 2.1 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 2.1 сформировал разрешающее правило. Вы можете редактировать указанные значения с помощью маски в свойствах созданного правила, чтобы расширить область применения правила (см. раздел «Расширение области применения правил контроля устройств« на стр. 196).

Данные исходного устройства

Данные устройства, на основе свойств которого Kaspersky Embedded Systems Security 2.1 сформировал разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Пусть к экземпляру устройства**. На основе этого значения Kaspersky Embedded Systems Security 2.1 определяет критерии срабатывания правила и заполняет поля **Производитель (VID)**, **Тип контроллера (PID)**, **Серийный номер** в блоке **Область применения правила** в окне **Параметры правила**.

- **Адаптированное имя**. Имя, которое задается в свойствах устройства производителем.

Kaspersky Embedded Systems Security 2.1 автоматически определяет данные исходного устройства в момент создания правила. В дальнейшем вы можете использовать эти значения, чтобы определить, на основе данных какого устройства было создано правило. Данные исходного устройства недоступны для редактирования.

Комментарий

Вы можете добавить дополнительную информацию для каждого созданного разрешающего правила контроля устройств в поле **Комментарий**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующей графе таблицы в окне **Правила контроля устройств**.

Комментарий и данные исходного устройства не учитываются при работе правила и служат только для упрощения идентификации устройств и правил пользователем.

Удаление правил контроля устройств

► *Чтобы удалить правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль устройств**.

3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. В списке правил выберите одно или несколько правил, которые вы хотите удалить.

5. Нажмите на кнопку **Удалить выбранные**.

6. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля устройств будут удалены.

Экспорт правил контроля устройств

► *Чтобы экспортировать правила контроля устройств в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Контроль устройств**.

3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.

5. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.

6. Нажмите на кнопку **Сохранить**.

Правила и их параметры будут экспортированы в указанный файл.

Активация и деактивация правила контроля устройств

Вы можете включать и выключать применение созданных разрешающих правил контроля устройств, не удаляя их.

► *Чтобы активировать или деактивировать созданное правило контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла Контроль устройств перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
5. В открывшемся окне снимите или установите флажок **Применять правило**.

   Флажок включает или выключает применение конкретного правила контроля устройств.

   Если флажок установлен в параметрах правила, такое правило будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет разрешено.

   Если флажок снят в параметрах правила, такое правило не будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет запрещено.

   По умолчанию флажок установлен в параметрах каждого созданного правила.
6. Нажмите на кнопку **ОК**.

Статус применения правила будет сохранен и отобразится для указанного правила.

Расширение области применения правил контроля устройств

Каждое автоматически созданное правило контроля устройств разрешает подключение только одного внешнего устройства. Вы можете вручную расширить область применения правила, применив маску пути к экземпляру устройства в свойствах любого заданного правила контроля устройств.

Применение маски пути к экземпляру устройства уменьшает количество разрешающих правил контроля устройств и упрощает процесс их обработки вручную. Однако расширение области применения правил может снижать эффективность контроля запоминающих устройств.

► *Чтобы применить маску пути к экземпляру устройства в свойствах разрешающего правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.
4. В открывшемся окне **Правила контроля устройств** выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
5. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.
6. В открывшемся окне выполните одно из следующих действий:
   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе и типе устройства.

- Установите флажок **Использовать маску** рядом с полем **Серийный номер**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе и серийном номере устройства.

- Установите флажки **Использовать маску** рядом с полями **Тип контроллера (PID)** и **Серийный номер**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе устройства.

Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых этот флажок не установлен, заменяются символом * и не будут учитываться при срабатывании правила.

7. Если требуется, введите дополнительную информацию о правиле в поле **Комментарий**. Например, уточните, на какие устройства должно распространяться правило.

8. Нажмите на кнопку **ОК**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

О формировании списка правил контроля устройств

Вы можете импортировать списки разрешающих правил контроля устройств из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль устройств или задачи Генерация правил контроля устройств.

По умолчанию Kaspersky Embedded Systems Security 2.1 запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие указанных разрешающих правил контроля устройств.

Таблица 23. Цели и сценарии формирования списков правил контроля устройств

Сценарий формирования списка правил	Решаемая задача
Задача Генерация правил контроля устройств	• Нужно создать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском задачи Контроль устройств. • Нужно сформировать список правил для доверенных устройств в сети защищаемых компьютеров.
Сформировать правила на основе данных системы	Нужно добавить разрешающие правила для одного или нескольких новых подключенных устройств.
Режим **Только статистика** задачи Контроль устройств	Нужно добавить разрешающие правила для большого количества новых доверенных устройств или для доверенных MTP-подключаемых мобильных устройств.

Использование задачи Генерация правил контроля устройств

XML-файл, сформированный по завершении задачи Генерация правил контроля устройств, содержит разрешающие правила для флеш-накопителей и других внешних устройств, данные о подключении которых сохранились в системе.

В ходе выполнения задачи, Kaspersky Embedded Systems Security 2.1 получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому компьютеру в данный момент, и создает на основе этих данных список разрешающих правил для обнаруженных устройств. По завершении задачи программа формирует XML-файл в папке по пути, указанному в параметрах задачи. Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль устройств.

Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств, чтобы созданные разрешающие правила учитывали все внешние устройства, используемые на защищаемом компьютере.

Использование данных системы обо всех подключаемых устройствах

В ходе выполнения задачи, Kaspersky Embedded Systems Security 2.1 получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому компьютеру в данный момент, и отображает найденные устройства в списке обнаруженных устройств в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Embedded Systems Security 2.1 определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Вы можете сформировать разрешающие правила для любого устройства, данные о котором были найдены, и сразу добавить новые правила в список заданных правил контроля устройств.

Рекомендуется использовать этот сценарий для обновления списка правил, если нужно разрешить использование небольшого количества новых запоминающих устройств.

Kaspersky Embedded Systems Security 2.1 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил контроля устройств, основанных на применении данных системы о всех устройствах.

Использование отчета задачи Контроль устройств в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль устройств в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Embedded Systems Security 2.1 фиксирует все подключения флеш-накопителей и других запоминающих устройств к защищаемому компьютеру в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** рекомендуется настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные подключения внешних устройств к защищаемому компьютеру.

Рекомендуется использовать этот сценарий для обновления существующего списка правил, если нужно разрешить использование большого количества новых внешних устройств, а также для создания разрешающих правил для MTP-подключаемых мобильных устройств.

Если формирование списка правил по этому сценарию выполняется на эталонной машине, вы можете применить сформированный список разрешающих правил при настройке политики Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на всех компьютерах защищаемой сети.

Добавление разрешающего правила для одного или нескольких внешних устройств

В задаче контроля устройств не предусмотрена функция добавления одного правила вручную. Однако в случае, если вам необходимо добавить разрешающие правила для одного или нескольких новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка правил программа использует данные Windows о всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает внешние устройства, подключенные в текущий момент.

Kaspersky Embedded Systems Security 2.1 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил контроля устройств, основанных на применении данных системы о всех устройствах.

► *Чтобы добавить разрешающее правило для одного или нескольких внешних устройств, подключенных в данный момент, выполните следующие действия:*

1. Подключите новое внешнее устройство, для которого вы хотите добавить разрешающее правило, к защищаемому компьютеру.

2. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Контроль компьютера**.

3. Выберите вложенный узел **Контроль устройств**.

4. В панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

5. Нажмите на кнопку **Добавить**.

6. В контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.

7. В открывшемся окне в списке обнаруженных устройств выберите устройство или несколько устройств, использование которых вы хотите разрешить на защищаемом компьютере.

8. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

Формирование списка правил по событиям задачи Контроль устройств

► *Чтобы создать конфигурационный файл со списком правил контроля устройств, сформированным по событиям задачи Контроль устройств, выполните следующие действия:*

1. Запустите задачу Контроль устройств в режиме **Только статистика** (см. раздел «**Настройка параметров задачи Контроль устройств**« на стр. 188), чтобы зафиксировать в журнале выполнения задачи все события, сформированные по подключениям флеш-накопителей и других внешних устройств к защищаемому компьютеру.

2. По завершении выполнения задачи в режиме **Только статистика**, откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль устройств**.

3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security 2.1 создаст конфигурационный файл в формате XML со списком правил, сформированных по работе задачи Контроль устройств в режиме **Только статистика**. Вы можете применить этот список в задаче Контроль устройств (см. раздел «Импорт правил контроля устройств из файла формата XML« на стр. 202).

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что подключение недоверенных устройств не разрешено заданными правилами.

При конвертации XML-файла с событиями выполнения задачи в список правил контроля устройств, программа создает разрешающие правила для всех зафиксированных событий, в том числе для событий блокирования устройств.

Все события работы задачи фиксируются в журнале в ходе выполнения задачи в любом из двух режимов. Вы можете создать конфигурационный файл со списком правил по событиям задачи в режиме **Запрещать недоверенные устройства**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется формировать списки правил до запуска задачи в режиме активного контроля подключения внешних устройств.

Импорт правил контроля устройств из файла формата XML

► *Чтобы импортировать правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 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. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.

6. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:

   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.

7. В окне Microsoft Windows **Открыть** выберите XML-файл, который содержит параметры правил контроля устройств.

8. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля устройств**.

О задаче Генерация правил контроля устройств

Задача Генерация правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других запоминающих устройств на основе данных операционной системы об устройствах, которые ранее подключались к защищаемому компьютеру.

> Kaspersky Embedded Systems Security 2.1 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил контроля устройств, основанных на применении данных системы о всех устройствах.

По завершении выполнения задачи Kaspersky Embedded Systems Security 2.1 создает конфигурационный файл в формате XML со списком разрешающих правил для обнаруженных запоминающих устройств или сразу добавляет сформированные правила в задачу Контроль устройств в зависимости от настроенных параметров задачи. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются по ссылке **Правила контроля устройств** в узле **Контроль устройств**.

Настройка параметров задачи Генерация правил контроля устройств

По умолчанию задача Генерация правил контроля устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 24. Параметры задачи Генерация правил контроля устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль устройств; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Расписание запуска задачи	Первый запуск не определен.	Задача Генерация правил контроля устройств не запускается автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Генерация правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Автоматическая генерация правил**.

2. Выберите вложенный узел **Генерация правил контроля устройств**.

3. В панели результатов узла **Генерация правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. На закладке **Общие** укажите действия, которые Kaspersky Embedded Systems Security 2.1 должен совершать 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 2.1 добавляет правила, сформированные в ходе выполнения задачи Генерация правил контроля устройств, в список правил контроля устройств согласно заданному принципу добавления.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не добавляет сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

     Флажок не может быть снят, если не установлен флажок **Экспортировать разрешающие правила в файл**.

   - **Принцип добавления**.

     Раскрывающийся список, позволяющий указать способ добавления сформированных разрешающих правил в список правил контроля

устройств.

- **Добавлять к существующим правилам**. Правила дополняют список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Заменять существующие правила**. Правила добавляются вместо существующих правил.
- **Объединять с существующими правилами**. Правила дополняют список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

По умолчанию установлен способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт сформированных разрешающих правил контроля устройств в файл.

  Если флажок установлен, по завершении задачи автоматического формирования разрешающих правил Kaspersky Embedded Systems Security 2.1 экспортирует сформированные правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи автоматического формирования разрешающих правил Kaspersky Embedded Systems Security 2.1 не экспортирует сформированные правила в файл, а только добавляет их в список правил контроля устройств.

  По умолчанию флажок снят.

  Флажок не может быть снят, если не установлен флажок **Добавлять разрешающие правила в список правил контроля устройств.**

- **Добавлять информацию о компьютере в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются сформированные правила контроля устройств.

Если флажок установлен, программа добавляет имя защищаемого компьютера, дату и время формирования файла в имя файла экспорта.

Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

Флажок доступен, если установлен флажок **Экспортировать разрешающие правила в файл**.

По умолчанию флажок установлен.

5. На закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

6. Нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Управление сетевым экраном

Kaspersky Embedded Systems Security 2.1 обеспечивает надежное и эргономичное решение для защиты сетевых подключений с помощью задачи Управление сетевым экраном.

Задача Управление сетевым экраном не выполняет самостоятельную фильтрацию сетевого трафика, но предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Embedded Systems Security 2.1. В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.1 полностью перенимает управление параметрами и правилами сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана другими способами.

В ходе установки программы компонент Управление сетевым экраном считывает и копирует состояние сетевого экрана Windows, а также все заданные правила. Далее изменение набора правил или их параметров, а также остановка или запуск сетевого экрана возможны только через Kaspersky Embedded Systems Security 2.1.

Если при установке Kaspersky Embedded Systems Security 2.1 сетевой экран Windows отключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы сетевой экран Windows включен, задача Управление сетевым экраном выполняется по завершении установки и блокирует все сетевые подключения, на разрешенные заданными правилами.

Компонент Управление сетевым экраном не входит в набор компонентов Рекомендуемой установки и не устанавливается по умолчанию.

Задача Управление сетевым экраном форсирует блокирование всех входящих и исходящих подключений, если они не разрешены заданными правилами задачи.

Задача регулярно опрашивает сетевой экран Windows и контролирует его состояние. По умолчанию интервал опроса составляет 1 минуту и не может быть изменен. Если при совершении опроса Kaspersky Embedded Systems Security 2.1 обнаруживает несовпадение параметров сетевого экрана Windows и параметров задачи Управление

сетевым экраном, программа форсировано сообщает параметры задачи сетевому экрану операционной системы.

При ежеминутном опросе сетевого экрана Windows, Kaspersky Embedded Systems Security 2.1 контролирует следующее:

- статус работы сетевого экрана Windows;
- статус правил, добавленных после установки Kaspersky Embedded Systems Security 2.1 другими программами или инструментами (Например, добавление нового правила программы для порта/приложения с помощью wf.msc).

После сообщения правил сетевому экрану Windows Kaspersky Embedded Systems Security 2.1 создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Embedded Systems Security 2.1 с помощью задачи Управление сетевым экраном. Правила, входящие в группу Kaspersky Security Group, не контролируются программой при ежеминутном опросе и не синхронизируются автоматически со списком правил, заданным в параметрах задачи Управление сетевым экраном.При необходимости вы можете выполнить обновление правил Kaspersky Security Group вручную.

► *Чтобы обновить список правил Kaspersky Security Group вручную,*

перезапустите задачу Управление сетевым экраном Kaspersky Embedded Systems Security 2.1.

Вы также можете изменять правила Kaspersky Security Group вручную через оснастку **Брандмауэр Windows**.

Запуск задачи Управление сетевым экраном невозможен, если сетевой экран Windows находится под управлением групповой политики Kaspersky Security Center.

О правилах сетевого экрана

Задача Управление сетевым экраном контролирует фильтрацию входящего и исходящего трафика с помощью разрешающих правил, которые форсировано сообщаются сетевому экрану Windows при выполнении задачи.

При первом запуске задачи Kaspersky Embedded Systems Security 2.1 считывает и копирует все разрешающие правила для входящего трафика, заданные в параметрах сетевого экрана Windows, в параметры задачи Управление сетевым экраном. При дальнейшей работе программа действует в соответствии со следующими алгоритмами:

- если в параметрах сетевого экрана Windows создается новое правило (вручную или автоматически при установке нового приложения), Kaspersky Embedded Systems Security 2.1 удаляет такое правило;
- если в параметрах сетевого экрана Windows удаляется существующее правило, Kaspersky Embedded Systems Security 2.1 восстанавливает такое правило;
- если в параметрах сетевого экрана Windows изменяются параметры существующего правила, Kaspersky Embedded Systems Security 2.1 отменяет изменения;
- если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Embedded Systems Security 2.1 форсировано сообщает это правило сетевому крану Windows;
- если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Embedded Systems Security 2.1 форсировано удаляет такое правило в параметрах сетевого экрана Windows;
- если в параметрах задачи Управление сетевым экраном изменяются параметры существующего правила, Kaspersky Embedded Systems Security 2.1 форсировано обновляет такое правило в параметрах сетевого экрана Windows.

Kaspersky Embedded Systems Security 2.1 не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.1 удаляет все правила этих типов в параметрах сетевого экрана Windows.

Вы можете задавать, удалять и редактировать правила для фильтрации входящего трафика.

Вы не можете задать новое правило для контроля исходящего трафика через параметры задачи Управление сетевым экраном. Все правила сетевого экрана, заданные через Kaspersky Embedded Systems Security 2.1, контролируют только входящий трафик.

Вы можете работать с правилами сетевого экрана следующих типов:

- правила для приложений;
- правила для портов.

Правила для приложений

Правила этого типа выборочно разрешают сетевые подключения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу.

Вы можете управлять правилами для приложений:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- редактировать параметры заданных правил: указывать имя правила, путь к исполняемому файлу и область применения правила.

Правила для портов

Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола.

Вы можете управлять правилами для портов:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- редактировать параметры заданных правил: указывать имя правила, номер порта, тип протокола и область применения правила.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая подключения с помощью правил для портов, вы снижаете уровень безопасности защищаемого компьютера.

Активация и деактивация правил сетевого экрана

► *Чтобы активировать или деактивровать существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли <PRODUCT_NAME_GEN> разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, статус которого вы хотите изменить, 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 деактивировано.
6. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи Управление сетевым экраном будут сохранены; новые параметры правил будут сообщены сетевому экрану Windows.

Добавление правил сетевого экрана вручную

► *Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли <PRODUCT_NAME_GEN> разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.

3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или закладку **Порты** и выполните одно из следующих действий:

   - Чтобы изменить существующее правило, в списке правил выберите правило, параметры которого вы хотите настроить и нажмите на кнопку **Изменить**.
   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или окно **Настроить правило для порта**.

5. В открывшемся окне выполните следующие действия:

   - Если вы работаете с правилом для приложения, выполните следующие действия:

     a. В поле **Имя правила** укажите имя редактируемого правила.

     b. В поле **Путь к приложению** укажите путь к исполняемому файлу приложения, подключения для которого вы хотите разрешить с помощью редактируемого правила. Вы можете задать путь вручную или с помощью кнопку **Обзор**.

     c. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

     > Допускается указание IP-адресов только в формате IPv4.

   - Если вы работаете с правилом для порта, выполните следующие действия:

     a. В поле **Имя правила** укажите имя редактируемого правила.

     b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.

     c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.

     d. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

Допускается указание IP-адресов только в формате IPv4.

6. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.

7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи Управление сетевым экраном будут сохранены; новые параметры правил будут сообщены сетевому экрану 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 <PRODUCT_NAME_GEN> разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Управление сетевым экраном**.

3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.

5. В списке правил выберите правило, которое вы хотите удалить.

6. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.

7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены; новые параметры правил будут сообщены сетевому экрану Windows.

Диагностика системы

Этот раздел содержит информацию о задаче контроля файловых операций и возможностях анализа системного журнала операционной системы.

В этом разделе

Мониторинг файловых операций

Этот раздел содержит информацию о задаче Мониторинг файловых операций и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу для выявления изменений файлов, которые могут свидетельствовать о нарушении безопасности на защищаемом компьютере. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

Обрыв мониторинга – это период, когда область мониторинга временно выпадает из поля действия задачи, например из-за приостановки выполнения задачи или физического отсутствия запоминающего устройства на защищаемом компьютере. Kaspersky Embedded Systems Security 2.1 сообщит об обнаружении файловых операций в области мониторинга как только запоминающее устройство будет вновь подключено.

> Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

Требования к среде

Для запуска задачи Мониторинг файловых операций должны быть соблюдены следующие условия:

- На защищаемом компьютере установлено запоминающее устройство, поддерживающий файловые системы ReFS и NTFS.
- включен USN-журнал Windows, на основе опроса которого компонент получает данные о файловых операциях.

  > Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинга файловых операций, требуется перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете задать исключения для области мониторинга (см. раздел «Настройка правил мониторинга« на стр. 224).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 (см. раздел «Настройка правил мониторинга« на стр. 224).

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания задачи и регулировать уровень важности событий для обнаруженных файловых операций, фиксируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- доверенные пользователи;
- маркеры файловых операций.

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать

уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Embedded Systems Security 2.1 обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности *Критическое событие* в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Embedded Systems Security 2.1 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 2.1 не может определить пользователя-инициатора для операций, выполненных в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Неизвестный пользователь – данный статус присваивается пользователю в случае, когда Kaspersky Embedded Systems Security 2.1 не может получить данные о пользователе вследствие прерывания задачи или сбоя синхронизации данных драйвера и USN-журнала. Если Kaspersky Embedded Systems Security 2.1 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 2.1 определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия

срабатывания правила мониторинга, программа зафиксирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Embedded Systems Security 2.1 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 25. 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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	файл или папка удалены	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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

Таблица 26. Параметры задачи Мониторинг файловых операций по умолчанию

Параметр	Значение	Как настроить
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.

Параметр	Значение	Как настроить
Список доверенных пользователей	Не задано	Вы можете задать пользователей и/или группы пользователей, действия которых в указанных каталогах будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security 2.1 будет пропускать области мониторинга, заданные в качестве исключений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров для характеристики файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security 2.1 формирует событие мониторинга.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Расписание запуска задачи	Следующий запуск не определен	Вы можете настраивать параметры запуска задачи по расписанию.

► *Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Диагностика системы**.

2. Выберите вложенный узел **Мониторинг файловых операций**.

3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** снимите или установите флажок **Контролировать файловые операции во время простоя задачи**.

   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 2.1 будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

   Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

   По умолчанию флажок установлен.

5. На закладках **Расписание** и **Дополнительно** настройте запуск задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

6. Нажмите на кнопку **ОК**.

   Настроенные параметры будут сохранены.

Настройка правил мониторинга

По умолчанию область мониторинга не задана: задача не контролирует выполнение файловых операций ни в одной папке.

► *Чтобы добавить область мониторинга, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга**.

   Откроется окно **Правила мониторинга**.
4. Добавьте область мониторинга одним из следующих способов:

   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:

     a. В левой части окна нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows **Обзор папок**.

     b. В открывшемся окне выберите папку, операции в которой вы хотите контролировать, и нажмите кнопку **ОК**.

     c. Нажмите на кнопку **Добавить**, чтобы Kaspersky Embedded Systems Security 2.1 начал контролировать файловые операции в указанной области мониторинга.

   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:

     - <*.ext> - все файлы с расширением <ext> вне зависимости от их расположения;
     - <*\name.ext> - все файлы с именем name и расширением <ext> вне зависимости от их расположения;
     - <\dir*> - все файлы в директории <\dir>;

- <\dir*\name.ext> - все файлы с именем name и расширением <ext> в директории <\dir> и всех ее поддиректориях.

> При задании области мониторинга вручную, убедитесь, что путь соответствует формату: <буква тома>:\<маска>. При отсутствии указания тома Kaspersky Embedded Systems Security 2.1 не добавит указанную область мониторинга.

В правой части окна на закладке **Параметры правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.

5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.
6. Выберите закладку **Пользователи**.
7. Нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: «Пользователи» или «Группы»**.
8. Выберите пользователей или группы пользователей, которые Kaspersky Embedded Systems Security 2.1 будет считать доверенными для выбранной области мониторинга.
9. Нажмите на кнопку **ОК**.

> По умолчанию Kaspersky Embedded Systems Security 2.1 считает недоверенными всех пользователей, не указанных в списке доверенных, и формирует для них события с уровнем важности (см. раздел «О правилах мониторинга файловых операций« на стр. 217) *Критическое событие*.

10. Выберите закладку **Маркеры файловых операций**.
11. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:

    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.

b. В открывшемся списке доступных файловых операций (см. раздел «О правилах мониторинга файловых операций« на стр. 217) установите флажки напротив тех операций, которые вы хотите контролировать.

> По умолчанию Kaspersky Embedded Systems Security 2.1 контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы Kaspersky Embedded Systems Security 2.1 рассчитывал контрольную сумму файлов после изменений, выполните следующие действия:

    a. В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

       Если флажок установлен, Kaspersky Embedded Systems Security 2.1 рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаруживается сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех последовательных изменений.

       Если флажок снят, Kaspersky Embedded Systems Security 2.1 не рассчитывает контрольную сумму измененных файлов.

       Kaspersky Embedded Systems Security 2.1 не выполняет расчет контрольной суммы в следующих случаях:

       - если в результате файловой операции файл стал недоступен (например, изменены права доступа к файлу);
       - если файловая операция фиксируется для файла, который впоследствии был удален.

       По умолчанию флажок снят.

    b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из вариантов:

- **Хеш MD5**
- **Хеш SHA256**.

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

    a. Выберите закладку **Исключения**.

    b. Установите флажок **Учитывать исключенные области мониторинга**.

        Флажок включает или выключает применение исключений для папок, в которых не требуется выполнять контроль над файловыми операциями.

        Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security 2.1 будет пропускать области мониторинга, заданные в списке исключений.

        Если флажок снят, Kaspersky Embedded Systems Security 2.1 будет фиксировать события для всех заданных областей мониторинга.

        По умолчанию флажок снят, список исключений пуст.

    c. Нажмите на кнопку **Обзор**.

    Откроется стандартное окно Microsoft Windows **Обзор папок**.

    d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

    e. Нажмите кнопку **Добавить**.

    Указанная папка добавится в список исключенных областей.

    > Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

14. Нажмите на кнопку **Сохранить**.

    Заданные правила мониторинга будут применяться к задаче Мониторинг файловых операций.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и настройке параметров задачи.

В этом разделе

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Embedded Systems Security 2.1 выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Embedded Systems Security 2.1 считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами заданными пользователем или параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Эвристический анализатор

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы на основе предзаданных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом компьютере, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных эвристиках в параметрах эвристического анализатора.

В списке эвристик для задачи Анализ журналов доступно семь эвристик. Вы можете включать и выключать применение любой эвристики. Вы не можете удалять существующие или создавать новые эвристики.

Для каждой эвристики вы можете настраивать следующие критерии срабатывания анализатора:

- 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 2.1 не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании эвристического анализатора программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил задачи вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил задачи Анализ журналов содержит четыре правила. Вы можете включать и выключать применение данных правил, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при появлении новой записи в журнале событий Windows, если в параметрах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать поджурналжурнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал.

Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Embedded Systems Security 2.1 фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает пользовательские правила.

Настройка правил анализа журналов

Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.
   Откроется окно **Правила анализа журналов**.
4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security 2.1 применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять и редактировать правила анализа журналов.

   Если флажок снят, вы не можете добавлять или редактировать пользовательские правила. Kaspersky Embedded Systems Security 2.1 применяет параметры правил по умолчанию.

   Вы не можете удалять или редактировать предустановленные правила.

   По умолчанию флажок снят.

Вы можете контролировать применение предустановленных правил в списке правил. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать новое пользовательское правило, выполните следующие действия:

    a. Введите имя нового правила.

    b. Нажмите на кнопку **Добавить**.

    Созданное правило добавится в общий список правил.

6. Чтобы настроить любое правило, выполните следующие действия:

    a. Выберите правило в списке нажатием левой кнопкой мыши.

    В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

    Комментарии для нового правила пусты.

    b. Выберите закладку **Описание**.

    c. В блоке **Общие отредактируйте Имя** правила, если требуется.

    d. Выберите **Источник для анализа данных.**

        Выберите журнал, события которого будут использоваться для анализа. Для выбора доступны следующие виды журналов Windows:

        - Application
        - Security
        - System

7. В блоке **Параметры срабатывания** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

    a. Введите числовое значение идентификатора.

    b. Нажмите на кнопку **Добавить**.

Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

c. Нажмите на кнопку **Сохранить**.

Настроенные параметры правил анализа журналов будут применены.

Настройка эвристического анализатора

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Эвристический анализатор**.
5. Снимите или установите флажок **Использовать эвристический анализатор для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security 2.1 применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, эвристический анализатор выключен, Kaspersky Embedded Systems Security 2.1 использует предустановленные или пользовательские правила для обнаружения аномальной активности.

   Для работы задачи должен быть выбран хотя бы один режим анализа журналов.

   По умолчанию флажок установлен.
6. Выберите эвристики, которые вы хотите применять для анализа журналов из списка доступных эвристик:

   - Обнаружена возможная попытка взлома пароля.

- 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 Administrators.

7. Чтобы настроить параметры выбранных эвристик, перейдите на закладку **Критерии срабатывания**.
8. В блоке **Обработка подбора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка сетевого входа** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Embedded Systems Security 2.1 расценивает данное действие как аномальную активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:

    a. Нажмите на кнопку **Обзор**.

    b. Выберите пользователя.

    c. Нажмите на кнопку **ОК**.

    Указанный пользователь добавится в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:

    a. Введите IP-адрес.

    b. Нажмите на кнопку **Добавить**.
13. Указанный IP-адрес добавится в список доверенных.
14. Выберите закладку **Управление задачей**, чтобы настроить расписание запуска задачи.
15. Нажмите на кнопку **ОК**.

    Параметры задачи Анализ журналов будут сохранены.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и по настройке параметров безопасности защищаемого компьютера.

В этом разделе

О задачах проверки по требованию

Kaspersky Embedded Systems Security 2.1 однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Embedded Systems Security 2.1 проверяет файлы, оперативную память компьютера, а также объекты автозапуска.

В Kaspersky Embedded Systems Security 2.1 предусмотрено четыре системные задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при старте Kaspersky Embedded Systems Security 2.1. Kaspersky Embedded Systems Security 2.1 проверяет загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. При каждом выполнении задачи Kaspersky Embedded Systems Security 2.1 создает копию незараженных загрузочных секторов, и если при последующем выполнении задачи он обнаружит в них угрозу, он заменяет зараженные загрузочные секторы их резервной копией.

- Задача Проверка важных областей по умолчанию выполняется еженедельно по расписанию. Kaspersky Embedded Systems Security 2.1 проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы, которые содержатся в системных папках, например, в папке %windir%\system32. Kaspersky Embedded Systems Security 2.1 применяет параметры безопасности, значения которых соответствуют уровню **Рекомендуемый** (см. раздел «**Выбор предустановленных уровней безопасности в задачах проверки по требованию**» на стр. 260). Вы можете изменять параметры задачи Проверка важных областей.

- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз. Вы не можете изменять параметры задачи Проверка объектов на карантине.

- Задача Проверка целостности программы запускается каждый раз при старте Kaspersky Embedded Systems Security 2.1. Она обеспечивает проверку модулей Kaspersky Embedded Systems Security 2.1 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. Значения параметров расписания запуска задачи можно изменять.

Вы можете создавать пользовательские задачи проверки по требованию. Например, вы можете создать задачу проверки папок общего доступа на компьютере.

Kaspersky Embedded Systems Security 2.1 может одновременно выполнять несколько задач проверки по требованию.

Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые Kaspersky Embedded Systems Security 2.1 обработал с момента запуска задачи по текущий момент.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел «Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач« на стр. 335).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

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

Вы можете просмотреть следующую информацию об объектах, которые Kaspersky Embedded Systems Security 2.1 обработал с момента запуска задачи по текущий момент (см. таблицу ниже).

Таблица 27. Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружил Kaspersky Embedded Systems Security 2.1. Например, если Kaspersky Embedded Systems Security 2.1 обнаружил в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруженных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 признал зараженными, или обнаруженных объектов, являющихся легальными программами, которые не были исключены из области действия задач постоянной защиты или проверки.
Возможно зараженных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 признал возможно зараженными.
Не вылечено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 не вылечил по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов, не помещенных на карантин	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 попытался поместить на карантин, но ему это не удалось, например, из-за отсутствия доступного пространства на диске.
Не удалено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 попытался удалить, но ему это не удалось, например, если доступ к объекту был заблокирован другой программой.
Не проверено объектов	Количество объектов в области защиты, которые Kaspersky Embedded Systems Security 2.1 не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых Kaspersky Embedded Systems Security 2.1 попытался сохранить в резервном хранилище, но это ему не удалось, например, из-за отсутствия доступного пространства на диске.

Поле	Описание
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые Kaspersky Embedded Systems Security вылечил.
Помещено на карантин	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 поместил на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых Kaspersky Embedded Systems Security 2.1 сохранил в резервном хранилище.
Удалено объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 удалил.
Защищенных паролем объектов	Количество объектов (например, архивов), которые Kaspersky Embedded Systems Security 2.1 пропустил, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 пропустил, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые Kaspersky Embedded Systems Security 2.1 обработал.

Вы также можете посмотреть статистику задач проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи проверки по требованию рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Настройка параметров задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Таблица 28. Параметры задач проверки по требованию

Параметр	Значение	Как настроить
Область проверки	Применяется в системных и пользовательских задачах: • Проверка при старте операционной системы: весь компьютер, исключая папки общего доступа и объекты автозапуска; • Проверка важных областей: весь компьютер, исключая папки общего доступа и некоторые файлы операционной системы; • Пользовательские задачи проверки по требованию: весь компьютер.	Вы можете изменить область проверки. Вы не можете настроить область защиты для системных задач Проверка объектов на карантине и Проверка целостности программы.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**	Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете выполнить следующие действия: • выбрать другой предустановленный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.

Параметр	Значение	Как настроить
Эвристический анализатор	Для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач проверки применяется с уровнем анализа **Средний**. Для задачи Проверка объектов на карантине применяется с уровнем анализа **Глубокий.**	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Применение эвристического анализатора в задаче Проверка целостности программы не предусматривается.
Доверенная зона	Применяется	Единый список исключений, который вы можете применять в выбранных задачах.
Использование KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.

Параметр	Значение	Как настроить
Выполнение в фоновом режиме (низкий приоритет)	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Расписание запуска задачи	Применяется в системных задачах: • Проверка при старте операционной системы – **При запуске программы**; • Проверка важных областей – **Еженедельно**; • Проверка объектов на карантине - **После обновления баз программы**; • Проверка целостности программы – **При запуске программы**. Не применяется во вновь созданных пользовательских задачах.	Вы можете настраивать параметры запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты компьютера	Статус защиты компьютера обновляется еженедельно после выполнения задачи Проверка важных областей.	Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами: • изменяя параметры расписания запуска задачи Проверка важных областей; • изменяя область защиты задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

► *Чтобы настроить задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.

3. В панели результатов узла на закладке **Обзор и управление** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**. Настройте следующие параметры задачи:

   - На закладке **Общие**:

     - Применение эвристического анализатора (на стр. 243).
     - Выполнение задачи в фоновом режиме (см. раздел «Выполнение задачи проверки по требованию в фоновом режиме« на стр. 244).
     - Использование KSN (на стр. 246).
     - Применение доверенной зоны (см. раздел «Включение и выключение применения доверенной зоны в задачах Kaspersky Embedded Systems Security 2.1« на стр. 64).
     - Регистрация выполнения проверки важных областей (на стр. 247).

   - На закладках **Расписание** и **Дополнительно**:

     - Параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

   - На закладке **Запуск с правами**:

     - Параметры запуска задачи с правами учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80).

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

   Изменения параметров будут сохранены.

5. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов компьютера выберите узлы, которые хотите включить в область проверки.
   - Выберите один из предустановленных уровней безопасности (см. раздел «Выбор предустановленных уровней безопасности в задачах проверки по требованию« на стр. 260) или настройте параметры проверки вручную (см. раздел «Настройка параметров безопасности вручную« на стр. 263).

6. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Применение эвристического анализатора

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Снимите или установите флажок **Использовать эвристический анализатор**.
5. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

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

операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

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

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

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

6. Нажмите на кнопку **ОК**.

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

Выполнение задачи проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Embedded Systems Security 2.1, имеют базовый приоритет **Средний** (**Normal**).

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, базовый приоритет **Низкий** (**Low**). Понижение приоритета процесса увеличивает время выполнения задачи, но также может положительно повлиять на скорость выполнения процессов других активных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Вы можете установить максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, приоритет которой вы хотите изменить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

   Флажок изменяет приоритет задачи.

   Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Embedded Systems Security 2.1 и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки и увеличивается при уменьшении нагрузки.

   Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security 2.1 и другие программы. В этом случае скорость выполнения задачи увеличивается.

   По умолчанию флажок снят.
5. Нажмите на кнопку **ОК**.

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

Использование KSN

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

Если вы приняли Положение о KSN во время установки программы, задача Использование KSN будет запускаться автоматически при старте Kaspersky Embedded Systems Security 2.1. Вы также можете вручную запустить выполнение задачи (см. раздел «Запуск и остановка задачи Использование KSN« на стр. 128) или настроить ее запуск по расписанию (см. раздел «Настройка параметров задачи Использование KSN« на стр. 128).

► *Чтобы настроить использование KSN в задачах проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Установите или снимите флажок **Использовать KSN для проверки**.

   Флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.
   Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

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

   По умолчанию флажок установлен.
5. Нажмите на кнопку **ОК**.

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

Регистрация выполнения проверки важных областей

По умолчанию статус защиты компьютера отображается в панели результатов узла **Kaspersky Embedded Systems Security** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты компьютера привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. Флажок установлен только для задачи Проверка важных областей и недоступен для редактирования.

Вы можете перепривязать задачу проверки по требованию к статусу защиты компьютера только из Kaspersky Security Center.

Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

В этом разделе

Об области проверки

Вы можете настроить область проверки для задач Проверка при старте операционной системы и Проверка важных областей, а также для пользовательских задач проверки по требованию.

По умолчанию задачи проверки по требованию проверяют все объекты файловой системы компьютера. Если по требованиям к безопасности нет необходимости проверять все объекты файловой системы, вы можете ограничить область проверки.

В Консоли Kaspersky Embedded Systems Security 2.1 область проверки представляет собой список или дерево файловых ресурсов компьютера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

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

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

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

☑ Узел включен в область проверки.

☐ Узел исключен из области проверки.

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

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

Имена виртуальных узлов области проверки отображаются шрифтом синего цвета.

Настройка параметров отображения файловых ресурсов области проверки

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:

- Выберите пункт **Отображать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.
- Выберите пункт **Отображать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

> По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

5. Нажмите на кнопку **Сохранить**.

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

Предопределенные области проверки

Дерево или список файловых ресурсов компьютера отображается в панели результатов узла выбранной задачи проверки по требованию по ссылке **Настроить область проверки**.

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

В Kaspersky Embedded Systems Security 2.1 предусмотрены следующие предопределенные области проверки:

- **Мой компьютер**. Kaspersky Embedded Systems Security 2.1 проверяет весь компьютер.
- **Локальные жесткие диски**. Kaspersky Embedded Systems Security 2.1 проверяет объекты на жестких дисках компьютера. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Kaspersky Embedded Systems Security 2.1 проверяет объекты на внешних устройствах, например, компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.

- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, которую вы используете для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются под системной учетной записью.

- **Системная память**. Kaspersky Embedded Systems Security 2.1 проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.

- **Объекты автозапуска**. Kaspersky Embedded Systems Security 2.1 проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули программ, которые автоматически запускаются при старте компьютера.

- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом компьютере.

- **Виртуальные диски**. Вы можете включать в область проверки динамические диски, папки и файлы, а также диски, которые монтируются на компьютер, например, общие диски кластера.

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

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**;
  - **Съемные диски**;
  - **Системная память**.
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows);

- **Съемные диски**;
- **Системная память**;
- **Объекты автозапуска**.

- Пользовательские задачи проверки по требованию:
  - **Локальные жесткие диски** (исключая папки Windows);
  - **Съемные диски**;
  - **Системная память**;
  - **Объекты автозапуска**;
  - **Папки общего доступа**.

Псевдодиски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Embedded Systems Security 2.1. Чтобы проверить объекты на псевдодиске, включите в область проверки папку на компьютере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Формирование области проверки

Если вы управляете Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере удаленно, через Консоль Kaspersky Embedded Systems Security 2.1, установленную на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом компьютере, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы измените область проверки в задачах Проверка при старте системы и Проверка важных областей, вы можете восстановить область проверки по умолчанию в этих задачах, выполнив восстановление Kaspersky Embedded Systems Security 2.1 (**Пуск** → **Программы** → **Kaspersky Embedded Systems Security 2.1** → **Изменение или удаление**). В мастере установки установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел «Настройка параметров отображения файловых ресурсов области защиты« на стр. 108). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В правой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:

   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:

- если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на компьютере, установите флажок **Съемные диски**);
- если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**;
- если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.

6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** будет закрыто. Настроенные параметры задачи будут сохранены.

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

1. В Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:

   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.
   c. В открывшемся окне **Добавление области проверки** выберите тип объекта, который вы хотите добавить в область проверки:

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

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

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

Область проверки исключается из области действия задачи проверки по требованию при ее удалении из списка файловых ресурсов.

8. Нажмите на кнопку **Сохранить**.

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

Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы не можете сканировать сетевые папки при работе под системной учетной записью.

► *Чтобы добавить в область проверки сетевой объект, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в область проверки которой вы хотите добавить сетевой путь.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В контекстном меню названия узла **Сетевое окружение** выполните следующие действия:

   - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
   - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
6. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.

7. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.

8. Если требуется, измените параметры безопасности для добавленного сетевого объекта.

9. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Вы можете включать в область проверки динамические диски, папки и файлы – создавать виртуальную область проверки.

> Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел «Настройка параметров отображения файловых ресурсов области защиты« на стр. 108).

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Выберите задачу проверки по требованию, область проверки которой вы хотите сформировать.

3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

5. В дереве файловых ресурсов компьютера откройте контекстное меню на узле **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.

6. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.

7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Выберите задачу проверки по требованию, в которой вы хотите создать виртуальную область проверки.

3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

5. В дереве файловых ресурсов компьютера откройте контекстное меню диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:

   - **Добавить виртуальную папку**, если хотите добавить виртуальную папку в область защиты.

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

6. В поле ввода задайте имя для папки или файла.

Указывая имя файла, вы можете задать его маску с помощью специальных символов * и ?.

7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область проверки.

8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задачах проверки по требованию

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

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех предустановленных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);

- вручную изменить параметры безопасности для выбранных узлов в дереве или списке файловых ресурсов компьютера (уровень безопасности примет значение **Другой**).

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

Выбор предустановленных уровней безопасности в задачах проверки по требованию

Для выбранного узла в дереве файловых ресурсов компьютера вы можете задать один из трех предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из предустановленных уровней безопасности имеет свой набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Embedded Systems Security 2.1 на компьютерах, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

Рекомендуемый

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

Максимальная защита

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

Таблица 29. Предустановленные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Проверка объектов	По формату	Все объекты	Все объекты
Оптимизация	Включена	Выключена	Выключена
Действия над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно (**Выполнять рекомендуемое действие**)	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Помещать на карантин	Помещать на карантин (**Выполнять рекомендуемое действие**)	Помещать на карантин
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	Нет	Нет
Не проверять составные объекты размером более (МБ)	8 МБ	Нет	Нет
Альтернативные потоки NTFS	Да	Да	Да

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Загрузочные секторы дисков и MBR	Да	Да	Да
Проверка составных объектов	• SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • почтовые базы* • файлы почтовых форматов* • упакованные объекты* • вложенные OLE-объекты* * Все объекты

Параметры безопасности **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** не входят в набор параметров предустановленных уровней безопасности. Если вы измените состояние параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, или **Использовать эвристический анализатор**, выбранный вами предустановленный уровень безопасности не изменится.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, в которой вы хотите настроить параметры безопасности.

3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В дереве или в списке файловых ресурсов компьютера выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.

5. Убедитесь, что выбранный узел включен в область проверки.

6. В правой части окна на закладке **Уровень безопасности** выберите уровень безопасности, который вы хотите применить.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

7. Нажмите на кнопку **Сохранить**.

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

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый** (см. раздел «**Выбор предустановленных уровней безопасности в задачах проверки по требованию**« на стр. 260).

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

При работе с деревом 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 вручную настроить параметры безопасности, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Выберите вложенный узел, соответствующий задаче, в которой вы хотите настроить параметры безопасности.

3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.
   Для выбранной области проверки вы можете применить предварительно созданный шаблон с набором параметров безопасности (см. раздел «О шаблонах параметров безопасности« на стр. 85).

5. Настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, настройте следующие параметры:

     В блоке **Проверка объектов** укажите объекты, которые вы хотите включить в область проверки:

     - **Все объекты.**

       Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

     - **Объекты, проверяемые по формату.**

       Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании формата файла.

       Список форматов составляется специалистами «Лаборатории Касперского» и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

  Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами «Лаборатории Касперского» и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по указанному списку расширений.**

  Kaspersky Embedded Systems Security 2.1 проверяет файлы на основании расширения файла. Список расширения файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

- **Загрузочные секторы дисков MBR.**

  Включение защиты загрузочных секторов дисков и главных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет загрузочные секторы и загрузочные надписи на жестких и съемных дисках компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS.**

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет дополнительные потоки файлов и папок.

  По умолчанию флажок установлен.

В блоке **Оптимизация** установите или снимите флажок:

- **Проверка только новых и измененных файлов**

  Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security 2.1 новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет и защищает все файлы.

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

В блоке **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Все / Только новые архивы.**

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые SFX-архивы.**

  Проверка архивов, имеющих в своем составе программный модуль-распаковщик.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

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

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает исполняемые файлы, упакованные программами-упаковщиками, при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает встроенные в файл объекты при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

Вы можете выбрать проверку всех или только новых составных объектов, если установлен флажок **Проверка только новых и измененных файлов**. Если флажок **Проверка только новых и измененных файлов** снят, Kaspersky Embedded Systems Security 2.1 проверяет все указанные составные объекты.

- На закладке **Действия**, если требуется, выполните следующие действия:
  - выберите действие над зараженными и другими обнаруживаемыми объектами;
  - выберите действие над возможно зараженными объектами;
  - если требуется, настройте действия в зависимости от типа обнаруженного объекта;
  - выберите действия над неизменяемыми контейнерами: снимите или установите флажок **Форсировать удаление родительского файла-контейнера при обнаружении вложенного зараженного или другого объекта**, если изменение контейнера невозможно.

    Флажок включает или выключает форсированное удаление родительского файла-контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта.

    Если флажок установлен и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 принудительно выполняет удаление всего родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта. Принудительное удаление родительского контейнера со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если родительский контейнер неизменяем).

    Если флажок снят и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 не выполняет указанное действие для родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта в случае, если

родительский контейнер неизменяем.

По умолчанию флажок установлен для уровня безопасности **Максимальная защита**. По умолчанию флажок снят для уровней безопасности **Рекомендуемый** и **Максимальное быстродействие**.

- На закладке **Производительность**, если требуется, настройте следующие параметры:

  В блоке **Исключения**:

  - **Исключать файлы.**

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

    Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные объекты.

    Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

    По умолчанию флажок снят.

  - **Не обнаруживать**.

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

    Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные обнаруживаемые объекты.

    Если флажок снят, Kaspersky Embedded Systems Security 2.1 обнаруживает все объекты, указанные в программе по умолчанию.

    По умолчанию флажок снят.

  В блоке **Дополнительные параметры**:

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

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

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

Если флажок снят, максимальная продолжительность проверки не ограничена.

По умолчанию флажок установлен.

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

  Исключение из проверки составных объектов больше указанного размера. По умолчанию установлено значение 8 МБ.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет составные объекты, не учитывая размер.

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

- **Использовать технологию iChecker.**

  Проверка только новых или измененных с момента последней проверки файлов.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет файлы, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

- **Использовать технологию iSwift**.

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

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет

объекты файловой системы NTFS, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

Проверка съёмных дисков

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

Kaspersky Embedded Systems Security 2.1 выполняет проверку съёмного диска с помощью задачи Проверка по требованию (см. раздел «О задачах проверки по требованию« на стр. 234). Программа автоматически создает новую задачу Проверка по требованию в момент подключения съёмного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется с предустановленным уровнем безопасности, указанным для проверки съёмных дисков. Вы не можете настроить параметры временной задачи Проверка по требованию.

Если вы установили Kaspersky Embedded Systems Security 2.1 без антивирусных баз, проверка съёмных дисков будет недоступна.

Kaspersky Embedded Systems Security 2.1 запускает проверку съёмных дисков, подключаемых по USB при их регистрации в операционной системе в качестве запоминающего устройства (USB Mass Storage Device). Программа не выполняет проверку съёмного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Embedded Systems Security 2.1 не блокирует доступ к съёмному диску на время проверки. Результаты проверки каждого съёмного диска доступны в журнале выполнения задачи Проверка по требованию, созданной при подключении этого диска.

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

Таблица 30. Параметры проверки съёмных дисков

Параметр	Значение по умолчанию	Описание
Проверять съёмные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске. Kaspersky Embedded Systems Security 2.1 не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	**Максимальная защита**	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • **Максимальная защита**; • **Рекомендуемый**; • **Максимальное быстродействие**. Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют предустановленным уровням безопасности в задачах проверки по требованию (см. раздел «Выбор предустановленных уровней безопасности в задачах проверки по требованию» на стр. 260).

► *Чтобы настроить параметры проверки съёмных дисков при подключении, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security** и выберите пункт **Проверка съёмных дисков**.

   Откроется окно **Проверка съёмных дисков**.

2. В блоке **Параметры проверки при подключении** выполните следующие действия:

   - Установите флажок **Проверять съёмные диски при их подключении по USB**, если вы хотите, чтобы Kaspersky Embedded Systems Security 2.1 автоматически выполнял проверку съёмных дисков при подключении.

   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное пороговое значение объема данных в поле справа.

   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съёмных дисков.

3. Нажмите на кнопку **ОК**.

   Настроенные параметры будут сохранены и применены.

Создание задачи проверки по требованию

Вы можете создавать пользовательские задачи в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Embedded Systems Security 2.1 создание пользовательских задач не предусмотрено.

► *Чтобы создать новую задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Проверка по требованию**.

2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.

3. Введите следующую информацию о задаче:

   - **Имя** – имя задачи, не более 100 символов, может содержать любые символы, кроме **% ? I \ | / : * < >**.

     Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано имя задачи.

   - **Описание** – любая дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.

4. Если требуется, настройте следующие параметры задачи:

5. На закладке **Общие**:

   - **Использовать эвристический анализатор**.

     Флажок включает или выключает использование эвристического анализатора при проверке объектов.

     Если флажок установлен, эвристический анализатор включен.

     Если флажок снят, эвристический анализатор выключен.

     По умолчанию флажок установлен.

   - **Выполнять задачу в фоновом режиме**.

     Флажок изменяет приоритет задачи.

     Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Embedded Systems Security 2.1 и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки

и увеличивается при уменьшении нагрузки.

Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security 2.1 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 2.1 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security 2.1 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

  По умолчанию флажок установлен.

- **Считать выполнение задачи проверкой важных областей**.

Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты компьютера. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security 2.1. Вы можете изменять значение этого параметра на стороне Kaspersky Security Center.

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

Если флажок снят, задача проверки выполняется с низким приоритетом.

Флажок установлен по умолчанию для задачи Проверка важных областей.

- **Использовать KSN для защиты**.

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

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

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

  По умолчанию флажок установлен.

- На закладках **Расписание** и **Дополнительно**:

  - Параметры запуска задачи по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

- На закладке **Запуск с правами**:

  - Параметры запуска задачи с правами учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80).

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

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли. Операция будет зарегистрирована в журнале системного аудита (см. раздел «Журнал системного аудита« на стр. 328).

7. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов компьютера выберите узлы, которые хотите включить в область проверки.

   - Выберите один из предустановленных уровней безопасности (см. раздел «Выбор предустановленных уровней безопасности в задачах проверки по требованию« на

стр. 260) или настройте параметры проверки вручную (см. раздел «Настройка параметров безопасности вручную« на стр. 263).

8. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Пользовательская задача проверки по требованию будет создана. Настроенные параметры будут применены при последующем запуске задачи.

Удаление задачи

В Консоли Kaspersky Embedded Systems Security 2.1 вы можете удалять только пользовательские задачи проверки по требованию. Вы не можете удалять системные или групповые задачи.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.
2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите удалить.
3. Выберите пункт **Удалить задачу**.

   Откроется окно подтверждения операции.
4. Нажмите на кнопку **Да**, чтобы подтвердить операцию удаления.

Задача будет удалена, операция удаления будет зарегистрирована в журнале системного аудита.

Переименование задачи

В Консоли Kaspersky Embedded Systems Security 2.1 вы можете переименовывать только пользовательские задачи. Вы не можете переименовывать системные или групповые задачи.

► *Чтобы переименовать задачу, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**.

2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите переименовать.
3. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне введите новое имя задачи в поле **Имя**.
5. Нажмите на кнопку **ОК**.

Задача будет переименована. Операция будет зарегистрирована в журнале системного аудита.

Обновление баз и модулей Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Embedded Systems Security 2.1, копировании обновлений и откате обновления баз Kaspersky Embedded Systems Security 2.1, а также инструкции по настройке параметров задач обновления баз и модулей программы.

В этом разделе

О задачах обновления

В Kaspersky Embedded Systems Security 2.1 предусмотрены четыре системные задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Embedded Systems Security 2.1 соединяется с источником обновлений – одним из серверов обновлений «Лаборатории Касперского», автоматически определяя параметры прокси-сервера в сети и не используя проверку подлинности при доступе к прокси-серверу.

Вы можете настраивать все задачи обновления (см. раздел «Настройка задач обновления« на стр. 288), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Embedded Systems Security 2.1 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 2.1 копирует базы из источника обновлений на защищаемый компьютер и сразу переходит к их использованию в выполняющейся задаче Постоянная защита. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.
По умолчанию Kaspersky Embedded Systems Security 2.1 запускает задачу Обновление баз программы ежечасно.

Обновление модулей программы

По умолчанию Kaspersky Embedded Systems Security 2.1 проверяет наличие программных модулей из источника обновлений на защищаемом компьютер. Для применения установленных программных модулей может потребоваться перезагрузка компьютера и / или перезапуск Kaspersky Embedded Systems Security 2.1.

По умолчанию Kaspersky Embedded Systems Security 2.1 запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого компьютера). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Embedded Systems Security 2.1, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Embedded Systems Security 2.1 загружает файлы обновлений баз и программных модулей 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 2.1 возвращается к использованию баз с предыдущими установленными обновлениями.
По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении модулей Kaspersky Embedded Systems Security 2.1

«Лаборатория Касперского» может выпускать пакеты обновлений модулей Kaspersky Embedded Systems Security 2.1. Пакеты обновлений делятся на *срочные* (или *критические*) и *плановые*. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные пакеты обновлений публикуются на серверах обновлений «Лаборатории Касперского». Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Embedded Systems Security 2.1 запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого компьютера).

«Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматизированной установки; вы можете загружать их с веб-сайта «Лаборатории Касперского». Вы можете получать информацию о выходе плановых обновлений Kaspersky Embedded Systems Security 2.1 с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя обновления на него без их установки, а затем распределяя их на компьютеры защищаемой сети. Чтобы копировать и сохранять обновления без их установки, используйте задачу Копирование обновлений.

Перед тем как установить обновления модулей, Kaspersky Embedded Systems Security 2.1 создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Embedded Systems Security 2.1 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 Service автоматически останавливается, а затем снова запускается.

Об обновлении баз Kaspersky Embedded Systems Security 2.1

Базы Kaspersky Embedded Systems Security 2.1, хранящиеся на защищаемом компьютере, быстро становятся неактуальными. Вирусные аналитики «Лаборатории Касперского» ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения компьютера к минимуму, регулярно получайте обновления баз.

По умолчанию, если базы Kaspersky Embedded Systems Security 2.1 не обновляются в течение недели с момента создания последних установленных обновлений баз, возникает событие *Базы устарели.* Если базы не обновляются в течение двух недель, возникает событие *Базы сильно устарели*. Информация об актуальности баз отображается в узле **Kaspersky Embedded Systems Security 2.1** дерева Консоли (см. раздел «Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security 2.1« на стр. 31). Вы можете указать другое количество дней перед наступлением этих событий с помощью общих параметров Kaspersky Embedded Systems Security 2.1, а также настроить параметры уведомления администратора об этих событиях (см. раздел «Настройка уведомлений администратора и пользователей« на стр. 353).

Kaspersky Embedded Systems Security 2.1 загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений «Лаборатории Касперского», Сервера администрирования Kaspersky Security Center или других источников обновлений.

Вы можете загружать обновления на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя обновления на него и затем распределяя их на компьютеры. Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров в организации, вы можете использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз вручную или по расписанию (см. раздел «Настройка параметров расписания запуска задач« на стр. 74). По умолчанию Kaspersky Embedded Systems Security 2.1 запускает задачу Обновление баз программы ежечасно.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Embedded Systems Security 2.1 автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Embedded Systems Security 2.1, вы можете сами откатить базы до предыдущих установленных обновлений (см. раздел «Откат обновления баз Kaspersky Embedded Systems Security 2.1« на стр. 297).

Схемы обновления баз и модулей антивирусных программ в организации

Ваш выбор источника обновлений в задачах обновления зависит от того, какую схему обновления баз и модулей антивирусных программ вы используете в организации.

Вы можете обновлять базы и модули Kaspersky Embedded Systems Security 2.1 на защищаемых компьютерах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый компьютер (схема 1);
- загружать обновления из интернета на компьютер-посредник и распределять обновления на компьютеры с этого компьютера.

  Посредником может служить любой компьютер, на котором установлена одна из следующих программ:

  - Kaspersky Embedded Systems Security 2.1 (один из защищаемых компьютеров) (схема 2);
  - Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через компьютер-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность компьютеров сети..

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление напрямую из интернета

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security 2.1 напрямую из интернета,*

на каждом защищаемом компьютере в настройках параметров задач Обновление баз программы и Обновление модулей программы в качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».

Вы можете указать в качестве источника обновлений другие HTTP- или FTP-серверы, которые содержат папку с файлами обновлений.

Figure 1: Схема обновления баз и программных модулей

Схема 2. Обновление через один из защищаемых компьютеров

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security 2.1 через один из защищаемых компьютеров, выполните следующие действия:*

1. Скопируйте обновления на выбранный защищаемый компьютер. Для этого выполните следующие действия:

   - На выбранном компьютере настройте параметры задачи Копирование обновлений:

     a. В качестве источника обновлений укажите компьютеры обновлений «Лаборатории Касперского».

     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.

2. Распределите обновления на остальные защищаемые компьютеры. Для этого выполните следующие действия:

- На каждом из защищаемых компьютеров настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже):

    a. В качестве источника обновлений укажите папку на диске компьютера-посредника, в которую вы скопировали обновления.

Kaspersky Embedded Systems Security 2.1 будет получать обновления через один из защищаемых компьютеров.

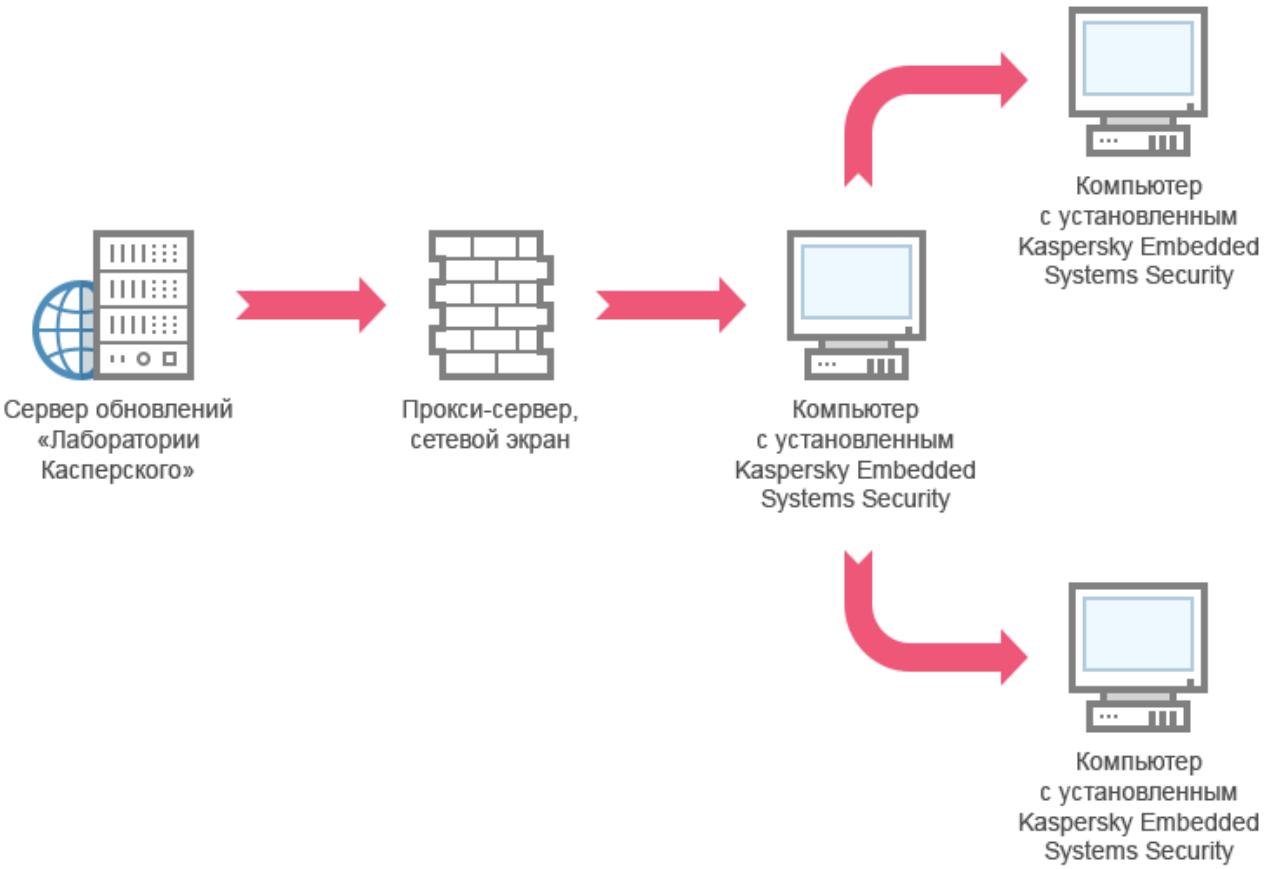

Figure 2: Обновление через один из защищаемых серверов

Схема 3. Обновите через Сервер администрирования Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров, вы можете загружать обновления через Сервер администрирования Kaspersky Security Center (см. рис. ниже).

Figure 3: Обновление через Сервер администрирования Kaspersky Security Center

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security 2.1 через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с сервера обновлений «Лаборатории Касперского» на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора компьютеров:
     a. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».

2. Распределите обновления на защищаемые компьютеры. Для этого выполните одно из следующих действий:

   - Настройте на Сервере администрирования Kaspersky Security Center групповую задачу обновления для распределения обновлений на защищаемые компьютеры:

     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

     Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

     Вы не можете указывать частоту запуска **После получения обновлений Сервером администрирования** в Консоли Kaspersky Embedded Systems Security 2.1.

   - Настройте на каждом из защищаемых компьютеров задачи Обновление баз программы и Обновление модулей программы:

     a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.

     b. Если требуется, настройте расписание задачи.

     При редких обновлениях антивирусных баз Kaspersky Embedded Systems Security 2.1 (от одного раза в месяц, до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

   Kaspersky Embedded Systems Security 2.1 будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых компьютеров программный компонент Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Embedded Systems Security 2.1 на защищаемом

компьютере. Подробная информация об Агенте администрирования и его настройке с помощью программы Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center*.

Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Embedded Systems Security 2.1.

В этом разделе

Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security 2.1

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, вы можете указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► *Чтобы указать тип источника обновлений, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.

2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.

3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В блоке **Источник обновлений** выберите тип источника обновлений Kaspersky Embedded Systems Security 2.1:

   - **Сервер администрирования Kaspersky Security Center**.

     Kaspersky Embedded Systems Security 2.1 использует в качестве источника обновления Сервер администрирования Kaspersky Security Center.

     Вы можете выбрать этот вариант, если в вашей сети управление программами «Лаборатории Касперского» выполняется с помощью системы удаленного управления Kaspersky Security Center и на защищаемом компьютере установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь компьютеров с Сервером администрирования.

   - **Серверы обновлений «Лаборатории Касперского»**.

     Kaspersky Embedded Systems Security 2.1 использует в качестве источника обновлений интернет-сайты «Лаборатории Касперского», на которых публикуются обновления баз и программных модулей для всех программ «Лаборатории Касперского».

     Данный вариант выбран по умолчанию.

   - **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

     Kaspersky Embedded Systems Security 2.1 использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы, папки на компьютерах локальной сети.

Вы можете сформировать список источников, которые содержат актуальный набор обновлений, нажав на ссылку **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:

   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

      i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.
      ii. Нажмите на кнопку **ОК**.

   b. В блоке **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:

   Выполните следующие действия:

   - Снимите или установите флажок **Использовать пассивный режим FTP, если возможно**.

     Флажок включает или выключает функцию, которая позволяет загружать обновления с FTP-серверов в пассивном режиме соединения.

Если флажок установлен, соединение выполняется в пассивном режиме.

Если флажок снят, соединение выполняется в стандартном режиме.

По умолчанию флажок установлен.

- Если требуется, укажите период тайм-аута (сек.).

В блоке **Параметры соединения с источниками обновлений**:

- Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений «Лаборатории Касперского».**

  Флажок включает / выключает использование параметров прокси-сервера, если обновление производится с серверов «Лаборатории Касперского», или установлен флажок **Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны**.

  Если флажок установлен, параметры прокси-сервера используются.

  Если флажок снят, параметры прокси-сервера не используются.

  По умолчанию флажок снят.

- Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

  Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

  Если флажок установлен, параметры прокси-сервера используются.

  По умолчанию флажок снят.

7. Нажмите на кнопку **ОК**.

Настроенные параметры источника обновлений Kaspersky Embedded Systems Security 2.1 будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Embedded Systems Security 2.1.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.
5. Выполните следующие действия:

   - Чтобы добавить новый пользовательский источник обновления, в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере; укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

     По умолчанию добавленная папка используется в качестве источника обновлений.

   - Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.

   - Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.

   - Чтобы изменить очередность обращения Kaspersky Embedded Systems Security 2.1 к пользовательским источникам, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, хотите вы использовать его раньше или позже.

   - Чтобы изменить путь к пользовательскому источнику, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.

   - Чтобы удалить пользовательский источник, выберите его в списке и нажмите на кнопку **Удалить**.

Вы не можете удалить единственный пользовательский источник из списка.

6. Нажмите на кнопку **ОК**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Embedded Systems Security 2.1 размещает файлы обновлений на локальном диске компьютера. Вы можете снизить нагрузку на дисковую подсистему компьютера за счет размещения файлов обновлений на виртуальном диске в оперативной памяти в процессе выполнения задачи обновления.

► *Чтобы снизить нагрузку на дисковую подсистему компьютера при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.
4. Откроется окно **Параметры задачи** на закладке **Общие**.
5. В блоке **Оптимизация использования дисковой подсистемы** настройте следующие параметры:

   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

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

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.

- В поле **Объем оперативной памяти, используемый для оптимизации**, укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия*:

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений.**
3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел «Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security 2.1« на стр. 288).
5. На закладке **Общие** в блоке **Параметры копирования обновлений** выполните следующие действия:
   - Укажите условия копирования обновлений программы:
     - **Копировать обновления программы**.

       Kaspersky Embedded Systems Security 2.1 загружает только обновления баз Kaspersky Embedded Systems Security 2.1.

       Этот вариант выбран по умолчанию.

- **Копировать критические обновления модулей программы**.

  Kaspersky Embedded Systems Security 2.1 загружает только срочные обновления программных модулей Kaspersky Embedded Systems Security 2.1.

- **Копировать обновления баз программы и критические обновления модулей программы**.

  Kaspersky Embedded Systems Security 2.1 загружает обновления баз и срочные обновления программных модулей Kaspersky Embedded Systems Security 2.1.

- Укажите локальную или сетевую папку, в которую Kaspersky Embedded Systems Security 2.1 будет копировать полученные обновления.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел «Настройка параметров расписания запуска задач« на стр. 74).

7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80).

8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия*:

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.

2. Выберите вложенный узел **Обновление модулей программы**.

3. В панели результатов узла **Обновление модулей программы** перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи**.

4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел «Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security 2.1« на стр. 288).

5. На закладке **Общие** в блоке **Параметры обновления** настройте параметры обновления модулей программы:

   - **Только проверять наличие доступных критических обновлений модулей программы**.

     Kaspersky Embedded Systems Security 2.1 выполняет уведомление об имеющихся на источнике срочных обновлениях программных модулей без скачивания обновлений. Уведомление производится, если оповещение о событиях этого типа настроено.

     Этот вариант выбран по умолчанию.

   - **Копировать и устанавливать критические обновления модулей программы**.

     Kaspersky Embedded Systems Security 2.1 копирует и устанавливает срочные обновления программных модулей.

   - **Разрешать перезагрузку компьютера**.

     Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 обновлениях модулей программы**.

     Получение уведомлений обо всех имеющихся на источнике плановых обновлений программных модулях Kaspersky Embedded Systems

Security 2.1. Kaspersky Embedded Systems Security 2.1 выполняет уведомления в том случае, если настроено оповещение о событиях этого типа.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 выполняет уведомление обо всех имеющихся на источнике плановых обновлениях программных модулей.

По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел «Настройка параметров расписания запуска задач« на стр. 74). По умолчанию Kaspersky Embedded Systems Security 2.1 запускает задачу Обновление модулей программы еженедельно, по пятницам в 16:00 (время согласно региональным настройкам защищаемого компьютера).

7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80).

8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

«Лаборатория Касперского» не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта «Лаборатории Касперского». Вы можете настроить уведомление администратора о событии *Доступно плановое обновление модулей программы*, в котором будет содержаться адрес страницы веб-сайта, с которой вы можете загрузить плановые обновления.

Откат обновления баз Kaspersky Embedded Systems Security 2.1

Перед применением обновления баз Kaspersky Embedded Systems Security 2.1 создает резервные копии баз, которые использовались ранее. Если обновление прервалось или завершилось с ошибкой, Kaspersky Embedded Systems Security 2.1 автоматически возвращается к использованию баз с предыдущими установленными обновлениями.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз.

► *Чтобы запустить задачу Откат обновления баз,*

перейдите по ссылке **Запустить** в панели результатов узла **Откат обновления баз программы**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Embedded Systems Security 2.1 создает резервные копии модулей, используемых в текущий момент. Если обновление модулей прервалось или завершилось с ошибкой, Kaspersky Embedded Systems Security 2.1 автоматически возвращается к использованию модулей с последними установленными обновлениями.

Чтобы откатить программные модули, используйте компонент панели управления Microsoft Windows **Установка и удаление программ**.

Статистика задач обновления

Пока выполняется задача обновления, вы можете просматривать в реальном времени информацию об объеме данных, полученных с момента запуска задачи по текущий момент, а также другую информацию о выполнении задачи.

После завершения или остановки задачи вы можете просмотреть эту информацию в журнале выполнения задачи (см. раздел «Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач« на стр. 335).

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.

2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

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

Если вы просматриваете задачу Обновление баз программы или задачу Копирование обновлений, в блоке **Статистика** отображается объем данных, загруженных Kaspersky Embedded Systems Security 2.1 на текущий момент (**Полученные данные**).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Таблица 31. Информация о задаче Обновление модулей программы

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Вы можете просмотреть название обновления, при применении которого возникла ошибка, в журнале выполнения задачи (см. раздел «Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач« на стр. 335).

Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

В этом разделе

Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

В этом разделе

Об изолировании возможно зараженных объектов

Kaspersky Embedded Systems Security 2.1 помещает объекты, которые он признает возможно зараженными, на карантин, то есть переносит объекты из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли Kaspersky Embedded Systems Security 2.1.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 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. 302) или отфильтруйте их (см. раздел «Фильтрация объектов на карантине« на стр. 303).

Сортировка объектов на карантине

По умолчанию объекты в списке объектов на карантине отсортированы по дате помещения в обратном хронологическом порядке. Чтобы найти нужный объект, вы можете отсортировать объекты по содержимому столбцов с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль Kaspersky Embedded Systems Security 2.1 с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты в списке.

Объекты в списке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, вы можете отфильтровать объекты в списке – отобразить только те объекты, которые удовлетворяют заданным вами критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы покинете и снова откроете узел Карантин или если вы закроете Консоль Kaspersky Embedded Systems Security 2.1 с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать один или несколько фильтров, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню названия узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в списке **Название поля**.

   c. В поле **Значение поля** введите или выберите в списке значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите действия a-d для каждого фильтра, который вы хотите добавить. При работе с фильтрами придерживайтесь следующих правил:

   - 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 фильтр в списке в окне **Параметры фильтра**, затем измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить.**

5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы снова отобразить все объекты в списке объектов на карантине,*

в контекстном меню названия узла **Карантин** выберите пункт **Снять фильтр**.

Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Embedded Systems Security 2.1 выполняет системную задачу Проверка объектов на карантине. Параметры задачи приводятся в таблице ниже. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Вы можете настраивать расписание запуска задачи (см. раздел «Настройка параметров расписания запуска задач« на стр. 74), запускать ее вручную, а также изменять права учетной записи (см. раздел «Указание учетной записи для запуска задачи« на стр. 80), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Embedded Systems Security 2.1 может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Embedded Systems Security 2.1 может признать зараженными и выполнить над ними действия, указанные параметрами задачи проверки по требованию Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Таблица 32. Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки; их значения приводятся в следующей таблице.

Таблица 33. Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверка объектов	Все объекты области проверки
Оптимизация	Выключена
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Пропускать
Исключать объекты	Нет
Не обнаруживать	Нет
Останавливать проверку, если длится более (сек.)	Не задано
Не проверять составные объекты размером более (МБ)	Не задано
Альтернативные потоки NTFS	Включена
Загрузочные секторы дисков и MBR	Выключена
Использовать технологию iChecker	Выключено

Параметр безопасности	Значение
Использовать технологию iSwift	Выключено
Проверка составных объектов	• Архивы* • SFX-архивы* • упакованные объекты* • вложенные OLE-объекты* * Проверка только новых и измененных файлов выключена.
Проверка подписи Microsoft у файлов	Не выполняется
Использовать эвристический анализатор	Включено с уровнем анализа **Глубокий**
Доверенная зона (см. стр. 61)	Не применяется

Восстановление объекта из карантина

Kaspersky Embedded Systems Security 2.1 помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстановить любой объект из карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Embedded Systems Security 2.1 не изолировал этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать объекты** (по имени

файла) или **Не обнаруживать** в этих задачах или добавьте его в доверенную зону (см. раздел «Настройка доверенной зоны« на стр. 61).

При восстановлении объекта вы можете выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановления на защищаемом компьютере или в указанной вами папке на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, или другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению компьютера.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Embedded Systems Security 2.1 не включает его снова составной объект при восстановлении, а сохраняет отдельно, в указанной папке.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты из карантина, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выполните одно из следующих действий:
   - чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**;
   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **CTRL** или клавишу **SHIFT**, затем откройте контекстное меню на одном из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого из выбранных объектов укажите папку, в которой будет сохранен восстановленный объект (имя объекта отображается в поле **Объект** в верхней части окна; если вы выбрали несколько объектов, в этом поле отображается имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:

   - чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**;
   - чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления в параметрах карантина, выберите **Восстановить в папку, используемую по умолчанию**;
   - чтобы сохранить объект в другой папке на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

5. Если вы хотите сохранить копию объекта в папке карантина после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

6. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

7. Нажмите на кнопку **ОК**.

   Kaspersky Embedded Systems Security 2.1 начнет восстанавливать первый из выбранных вами объектов.

8. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

a. Выберите одно из следующих действий Kaspersky Embedded Systems Security 2.1:

- **Заменить**, чтобы сохранить восстановленный объект вместо существующего;
- **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
- **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

c. Нажмите на кнопку **ОК**.

Объект будет восстановлен; информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню названия узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **ОК**.

   Kaspersky Embedded Systems Security 2.1 поместит указанный файл на карантин.

Удаление объектов из карантина

Согласно параметрам задачи **Проверка объектов на карантине** (см. стр. 304), Kaspersky Embedded Systems Security 2.1 автоматически удаляет из папки карантина объекты, статус которых при проверке карантина с использованием обновленных баз изменился на *зараженный или обнаруживаемый* и которые Kaspersky Embedded Systems Security 2.1 не удалось вылечить. Остальные объекты Kaspersky Embedded Systems Security 2.1 не удаляет.

Вы можете вручную удалить из карантина один или несколько объектов.

► *Чтобы удалить из карантина один или несколько объектов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.

2. Выберите вложенный узел **Карантин**.

3. Выполните одно из следующих действий:

   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**;

   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт **Удалить**.

4. В открывшемся окне нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены из карантина.

Отправка возможно зараженных объектов на исследование в »Лабораторию Касперского»

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Embedded Systems Security 2.1 признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в »Лабораторию Касперского». Вирусные аналитики «Лаборатории Касперского» проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись и алгоритм лечения в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Embedded Systems Security 2.1 признает его зараженным и ему удастся его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы из карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Вы не можете отправлять объекты из карантина на исследование в »Лабораторию Касперского» после окончания срока действия лицензии.

► *Чтобы отправить файл на исследование в »Лабораторию Касперского», выполните следующие действия:*

1. Если файл не находится на карантине, предварительно поместите его на карантин (см. стр. 309).

2. В узле **Карантин**, в списке объектов на карантине, откройте контекстное меню файла, который вы хотите отправить на исследование в »Лабораторию Касперского», и выберите пункт **Отправить объект на исследование**.

3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.

4. Если на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, настроен почтовый клиент, будет создано новое сообщение электроной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

Поле **Получатель** сообщения содержит адрес электронной почты «Лаборатории Касперского» newvirus@kaspersky.com. Поле **Тема** содержит текст «Объект карантина».

Тело сообщения содержит текст «Файл будет отправлен в »Лабораторию Касперского» для исследования». В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

В сообщение вложен архив <имя объекта>.cab. Он содержит файл <uuid>.klq с зашифрованным объектом (где uuid – уникальный идентификатор объекта в Kaspersky Embedded Systems Security 2.1), файл <uuid>.txt с информацией, полученной Kaspersky Embedded Systems Security 2.1 об объекте, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Embedded Systems Security 2.1 и операционной системе на компьютере:

- название и версию операционной системы;
- название и версию Kaspersky Embedded Systems Security 2.1;
- дата выпуска последних установленных обновлений баз;
- номер активного ключа.

Эта информация нужна вирусным аналитикам «Лаборатории Касперского», чтобы быстрее и эффективнее проанализировать файл. Однако если вы не хотите передавать ее, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл вы можете переслать в »Лабораторию Касперского» самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **Да**.
2. Выберите папку на диске защищаемого компьютера или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые значения параметров карантина применяются сразу после их сохранения.

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

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Откройте контекстное меню названия вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Параметры хранилища** настройте нужные параметры карантина в соответствии с вашими требованиями:

   В блоке **Параметры карантина**:

   - **Папка карантина**.

     Путь к папке карантина в формате UNC (Universal Naming Convention).

     По умолчанию установлен путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Quarantine\.

   - **Максимальный размер карантина**.

     Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security 2.1 фиксирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отслеживает суммарный размер размещенных в карантине объектов.

     Если флажок снят, Kaspersky Embedded Systems Security 2.1 не отслеживает суммарный размер объектов в карантине.

     По умолчанию флажок снят.

- **Порог доступного пространства**.

  Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Embedded Systems Security 2.1 фиксирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отслеживает размер свободного места в резервном хранилище.

  Флажок **Порог доступного пространства (МБ)** активен, если установлен флажок **Максимальный размер резервного хранилища (МБ)**.

  По умолчанию флажок установлен.

> Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Embedded Systems Security 2.1 уведомит вас об этом, не переставая помещать объекты на карантин.

В блоке **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**.

  Путь к папке, в которую восстанавливаются объекты в формате UNC (Universal Naming Convention).

  По умолчанию установлен путь C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Restored\.

5. Нажмите на кнопку **ОК**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в контекстном меню названия узла **Карантин** в дереве Консоли Kaspersky Embedded Systems Security 2.1 выберите пункт **Статистика**.

В окне **Статистика** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

Таблица 34. Информация об объектах на карантине в окне Статистика карантина

Поле	Описание
Возможно зараженных объектов	Количество объектов, которые Kaspersky Embedded Systems Security 2.1 признал возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которые получили статус *Ложное срабатывание*, так как при проверке карантина с применением обновленных баз были признаны незараженными.
Вылечено объектов	Количество объектов, которые после проверки карантина получили статус *Вылеченный*.
Всего объектов	Общее количество объектов на карантине.

Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

В этом разделе

О резервном копировании объектов перед лечением или удалением

Kaspersky Embedded Systems Security 2.1 сохраняет зашифрованные копии объектов со статусами *зараженный* или *обнаруживаемый* и *возможно зараженный* в *резервном хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Embedded Systems Security 2.1 сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Embedded Systems Security 2.1 признал зараженным один из объектов в составе почтовой базы, он резервирует всю почтовую базу.

Если объект, который Kaspersky Embedded Systems Security 2.1 копирует в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске вашего компьютера.

Вы можете восстанавливать файлы из резервного хранилища, как в исходную папку, так и в другую папку на защищаемом компьютере или другом компьютере в локальной сети организации. Вы можете восстановить файл из резервного хранилища, например, если исходный зараженный или возможно зараженный файл содержал важную информацию, но при лечении этого файла Kaspersky Embedded Systems Security 2.1 не удалось сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только через Консоль Kaspersky Embedded Systems Security 2.1, в узле **Резервное хранилище**. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище,*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

   Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов в резервном хранилище,*

отсортируйте объекты или отфильтруйте их.

В этом разделе

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их сохранения в обратном хронологическом порядке. Чтобы найти нужный файл, вы можете отсортировать файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы покинете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль Kaspersky Embedded Systems Security 2.1 с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В списке файлов в резервном хранилище выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат фильтрации сохранится, если вы покинете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль Kaspersky Embedded Systems Security 2.1 с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

2. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, со значениями которого будет сравниваться указанное вами значение фильтра при отборе.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.

   c. В поле **Значение поля** введите или выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого фильтра, который вы хотите добавить. Вы можете использовать следующие правила работы с фильтрами:

   - Чтобы объединить несколько фильтров по логическому «И», выберите вариант **При выполнении всех условий**.

   - Чтобы объединить несколько фильтров по логическому «ИЛИ», выберите вариант **При выполнении любого условия**.

   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.

   - Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► *Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,*

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

Восстановление файлов из резервного хранилища

Kaspersky Embedded Systems Security 2.1 хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный файл, который оказался зараженным, содержал важную информацию, при лечении файла Kaspersky Embedded Systems Security 2.1 не удалось сохранить его целостность, и в результате информация в файле стала недоступной;
- если вы считаете файл безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Embedded Systems Security 2.1 не признавал файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и задачах проверки по требованию. Для этого укажите файл в качестве параметра **Исключать объекты** или параметра **Не обнаруживать** этих задач.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходную папку (по умолчанию), в специальную папку для восстановленных объектов на защищаемом компьютере или в указанную вами папку на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, или другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел «Настройка параметров резервного хранилища« на стр. 324).

По умолчанию, когда Kaspersky Embedded Systems Security 2.1 восстанавливает файл, он сохраняет его копию в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.

2. Выберите вложенный узел **Резервное хранилище**.

3. Выполните одно из следующих действий:

   - чтобы восстановить один файл, в списке файлов в резервном хранилище откройте контекстное меню на файле, который вы хотите восстановить, и выберите пункт **Восстановить**.

   - чтобы восстановить несколько файлов, выберите нужные файлы в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на одном из выбранных файлов и выберите пункт **Восстановить**.

4. В окне **Восстановление объекта** укажите папку, в которой будет сохранен восстановленный файл.

   Название файла отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько файлов, в этом поле отображается имя первого файла в списке выбранных.

   Выполните одно из следующих действий:

   - Чтобы сохранить восстановленный файл на защищаемом компьютере, выберите один из следующих вариантов:

     - **Восстановить в исходную папку**, если вы хотите восстановить файл в исходную папку.

- **Восстановить в папку, используемую по умолчанию**, если вы хотите восстановить файл в папку, которую вы указали в качестве папки для восстановления в параметрах резервного хранилища.

- Чтобы сохранить восстановленный файл в другую папку, выберите пункт **Восстановить в папку на локальном компьютере или сетевом ресурсе** и выберите нужную папку (на компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, или в сети) или укажите путь к ней.

5. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалять объекты из хранилища после восстановления** (по умолчанию флажок снят).

6. Если вы выбрали несколько файлов для восстановления, то, чтобы применить указанные условия сохранения к остальным выбранным файлам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные файлы будут восстановлены и сохранены в указанную вами папку: если вы выбрали вариант **Восстановить в исходную папку**, каждый из файлов будет сохранен в свою исходную папку; если вы выбрали вариант **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все файлы будут сохранены в одну указанную папку.

7. Нажмите на кнопку **ОК**.

   Kaspersky Embedded Systems Security 2.1 начнет восстанавливать первый из выбранных вами файлов.

   Если файл с таким именем уже существует в указанной папке, откроется окно **Объект с таким именем существует**.

8. Выполните следующие действия:

   a. Выберите одно из следующих условий сохранения восстановленного файла:

   - **Заменить**, чтобы сохранить восстановленный файл вместо существующего.
   - **Переименовать**, чтобы сохранить восстановленный файл под другим именем. В поле ввода введите новое имя файла и полный путь к нему

- **Переименовать, добавив суффикс**, чтобы переименовать файл, добавив к его имени суффикс. Введите суффикс в поле ввода.

b. Если вы хотите применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным файлам, установите флажок **Применить ко всем объектам**.

Если вы выбрали вариант **Переименовать**, флажок **Применить ко всем объектам** будет недоступен.

c. Нажмите на кнопку **ОК**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы выбрали несколько файлов для восстановления и не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать папку, в которой будет сохранен при восстановлении следующий выбранный файл (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

► *Чтобы удалить из резервного хранилища один или несколько файлов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.

2. Выберите вложенный узел **Резервное хранилище**.

3. Выполните одно из следующих действий:

   - чтобы удалить один файл, в списке объектов откройте контекстное меню на файле, который вы хотите удалить, и выберите команду **Удалить**;

   - чтобы удалить несколько файлов, выберите нужные файлы в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных файлов и выберите команду **Удалить**.

4. В окне **Подтверждение** нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Хранилища**.

2. Откройте контекстное меню названия вложенного узла **Резервное хранилище**.

3. Выберите пункт **Свойства**.

4. В окне **Параметры хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

   В блоке **Параметры резервного хранилища**:

   - **Папка резервного хранилища**.

     Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

     По умолчанию установлен путь C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Backup\.

   - **Максимальный размер резервного хранилища (МБ)**.

     Флажок включает или выключает функцию, которая отслеживает суммарный размер размещенных в резервном хранилище объектов. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security 2.1 фиксирует 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 2.1 отслеживает суммарный размер размещенных в резервном хранилище объектов.

По умолчанию флажок снят.

- **Порог доступного пространства (МБ)**.

  Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Embedded Systems Security 2.1 фиксирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 2.1 уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В блоке **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**.

  Путь к папке, в которую восстанавливаются объекты в формате UNC (Universal Naming Convention).

  По умолчанию установлен путь C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Restored\.

5. Нажмите на кнопку **ОК**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Вы можете просматривать информацию о состоянии резервного хранилища в текущий момент – статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли откройте контекстное меню на узле **Резервное хранилище** и выберите команду **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о состоянии резервного хранилища в текущий момент (см. таблицу ниже).

Таблица 35. 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

Запись событий. Журналы Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о работе с журналами Kaspersky Embedded Systems Security 2.1: журналом системного аудита, журналами выполнения задач Kaspersky Embedded Systems Security 2.1 и журналом событий Kaspersky Embedded Systems Security 2.1.

В этом разделе

Способы записи событий Kaspersky Embedded Systems Security 2.1

События Kaspersky Embedded Systems Security 2.1 делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Embedded Systems Security 2.1;
- события, связанные с управлением Kaspersky Embedded Systems Security 2.1, например, запуск программы, создание или удаление задач, запуск задач, изменение параметров задач.

Kaspersky Embedded Systems Security 2.1 использует следующие способы для записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о параметрах задачи, текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Embedded Systems Security 2.1.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security 2.1. Журнал событий доступен в консоли Просмотр событий Microsoft Windows.
- **Журнал событий безопасности**. Журнал событий безопасности содержит информацию о событиях, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере.

Если в работе Kaspersky Embedded Systems Security 2.1 возникла проблема (например, Kaspersky Embedded Systems Security 2.1 или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать файл трассировки и файл дампа процессов Kaspersky Embedded Systems Security 2.1 и отправить файлы с этой информацией на анализ в Службу технической поддержки «Лаборатории Касперского».

Kaspersky Embedded Systems Security 2.1 записывает информацию в файлы трассировки и файл дампа в незашифрованном виде.

Журнал системного аудита

Kaspersky Embedded Systems Security 2.1 ведет системный аудит событий, связанных с управлением Kaspersky Embedded Systems Security 2.1. Программа сохраняет информацию о, например, запуске программы, запуске и остановке задач Kaspersky Embedded Systems Security 2.1, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли Kaspersky Embedded Systems Security 2.1.

По умолчанию Kaspersky Embedded Systems Security 2.1 хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которой Kaspersky Embedded Systems Security 2.1 сохраняет файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

В этом разделе

Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
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 только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.

2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

3. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.

   c. В списке **Значение поля** выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:

   - Если вы хотите объединить несколько фильтров по логическому «И», выберите вариант **При выполнении всех условий**.

   - Если вы хотите объединить несколько фильтров по логическому «ИЛИ», выберите вариант **При выполнении любого условия**.

5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
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 2.1 хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► *Чтобы удалить события из журнала системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
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 2.1 и инструкции по работе с ними.

В этом разделе

О журналах выполнения задач

Информация о выполнении задач Kaspersky Embedded Systems Security 2.1 отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли Kaspersky Embedded Systems Security 2.1.

В журнале выполнения каждой задачи вы можете просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи по текущий момент, а также параметры задачи.

По умолчанию Kaspersky Embedded Systems Security 2.1 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 2.1 сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Также вы можете выбрать события, записи о которых Kaspersky Embedded Systems Security 2.1 сохраняет в журналах выполнения задач.

Просмотр списка событий в журналах выполнения задач

► *Чтобы просмотреть список событий в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.

Список событий, сохраненных в журналах выполнения задач Kaspersky Embedded Systems Security 2.1, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

Сортировка событий в журналах выполнения задач

По умолчанию события отображаются в журналах выполнения задач в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.

3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в журналах выполнения задач Kaspersky Embedded Systems Security 2.1.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация событий в журналах выполнения задач

Вы можете отобразить в списке событий журналов выполнения задач только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.

2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

3. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.

   c. В списке **Значение поля** выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:

   - Если вы хотите объединить несколько фильтров по логическому «И», выберите вариант **При выполнении всех условий**.

- Если вы хотите объединить несколько фильтров по логическому «ИЛИ», выберите вариант **При выполнении любого условия**.

5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в списке событий журналов выполнения задач.

В списке событий журналов выполнения задач отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.

2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке событий журналов выполнения задач отобразятся все события.

Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска по текущий момент, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.

2. Выберите вложенный узел **Журналы выполнения задач**.

3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:

- двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
- откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.

4. В открывшемся окне отображается следующая информация:
   - на закладке **Статистика** отображается время запуска и завершения задачи и ее статистика;
   - на закладке **События** отображается список событий, зафиксированных при выполнении задачи;
   - на закладке **Параметры** отображаются параметры задачи.
5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.
6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.
7. Нажмите на кнопку **Закрыть**.

Окно **Журнал выполнения** будет закрыто.

Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.
2. Выберите вложенный узел **Журналы выполнения задач**.

3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:

   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.

4. В нижней части окна **Журнал выполнения** нажмите на кнопку **Экспорт**.

   Откроется окно **Сохранить как**.

5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.

6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

Удаление событий из журналов выполнения задач

По умолчанию Kaspersky Embedded Systems Security 2.1 хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете вручную удалить все события из журналов выполнения задач, завершившихся на данный момент.

> События из журналов задач, выполняющих в данный момент и журналов, используемых другими пользователями, удалены не будут.

► *Чтобы удалить события из журналов выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Журналы**.

2. Выберите вложенный узел **Журналы выполнения задач**.

3. Выполните одно из следующих действий:

   - Если вы хотите удалить события из всех журналов выполнения задач, завершившихся на данный момент, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.

   - Если вы хотите очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню события, которое возникло в задаче, журнал выполнения которой вы хотите очистить, и выберите пункт **Удалить**.

   - Если вы хотите очистить журналы выполнения нескольких задач, выполните следующие действия:

     a. В панели результатов с помощью клавишей **Ctrl** или **Shift**, выберите события, которые возникли в задачах, журналы выполнения которых вы хотите очистить.

     b. Откройте контекстное меню любого выбранного события и выберите пункт **Удалить**.

4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление.

Выбранные журналы выполнения задач будут очищены. Удаление событий из журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал событий безопасности

Kaspersky Embedded Systems Security 2.1 ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.

- Критические события компонента Анализ журналов.

- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить Журнал событий безопасности, так же, как и Журнал системного аудита (см. раздел «Удаление событий из журнала системного аудита« на стр. 331). При этом Kaspersky Embedded Systems Security 2.1 фиксирует событие системного аудита об очистке Журнала событий безопасности.

Просмотр журнала событий Kaspersky Embedded Systems Security 2.1 в консоли Просмотр событий

С помощью оснастки **Просмотр событий** для Microsoft Management Console вы можете просматривать журнал событий Kaspersky Embedded Systems Security 2.1. В нем Kaspersky Embedded Systems Security 2.1 регистрирует события, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security 2.1.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий**;
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень **Информационные события**, при котором регистрируются события всех уровней важности; наименее подробным является уровень **Критические события**, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента **Обновление** установлен уровень детализации **Важные события** (регистрируются только важные и критические события); для компонента **Обновление** установлен уровень **Информационные события**.

► *Чтобы просмотреть журнал событий Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется окно Microsoft Management Console.

2. Выберите **Файл → Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите компьютер, на котором установлен Kaspersky Embedded Systems Security 2.1, и нажмите на кнопку **OK**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **OK**.

   В дереве Консоли появится узел **Просмотр событий**.

6. В дереве Консоли раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб → Kaspersky Embedded Systems Security 2.1**.

Откроется журнал событий Kaspersky Embedded Systems Security 2.1.

Настройка параметров журналов в Консоли Kaspersky Embedded Systems Security 2.1

Вы можете настраивать следующие параметры журналов Kaspersky Embedded Systems Security 2.1:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Embedded Systems Security 2.1 сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*;
- события, которые Kaspersky Embedded Systems Security 2.1 сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security 2.1 в консоли Просмотр событий;
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов**.

2. В окне **Параметры журналов** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, выберите события, которые Kaspersky Embedded Systems Security 2.1 сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security 2.1 в консоли Просмотр событий. Для этого выполните следующие действия:

- В списке **Компонент** выберите функциональный компонент Kaspersky Embedded Systems Security 2.1, уровень детализации событий которого вы хотите настроить.

  > Для компонентов Постоянная защита файлов, Проверка по требованию и Обновление предусмотрена запись событий в журналы выполнения задач и журнал событий. Для этих компонентов таблица списка событий содержит графы **Журналы** и **Журнал событий**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица списка событий содержит графы **Аудит** и **Журнал событий**.

- В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного функционального компонента.

  В таблице списка событий ниже установлены флажки рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

- Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:

  a. В списке **Уровень важности** выберите **Другой**.

  b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

- На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий о статусе защиты компьютера:

- В блоке **Хранение журналов**:
  - **Папка с журналами**.

    Путь к папке с журналами в формате UNC (Universal Naming Convention).

    По умолчанию установлен путь C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Reports\.

  - **Удалять журналы выполнения задач и событий старше, чем (дни)**.

    Флажок включает / выключает функцию, которая удаляет журналы о результатах выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода (по умолчанию 30 дней).

    Если флажок установлен, Kaspersky Embedded Systems Security 2.1 удаляет журналы о результатах выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода.

    По умолчанию флажок установлен.

  - **Удалять события журнала аудита старше, чем (дни)**.

    Флажок включает / выключает функцию, которая удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода (по умолчанию 60 дней).

    Если флажок установлен, Kaspersky Embedded Systems Security 2.1 удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода.

    По умолчанию флажок установлен.

- В блоке **Пороги формирования событий**:
  - количество дней, после которого будут возникать события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*;

Таблица 36. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих трех типов: • *Базы программы устарели* и *Базы программы сильно устарели*. Событие возникает, если базы Kaspersky Embedded Systems Security 2.1 не обновляются в течение указанного параметром количества дней с момента создания последних установленных обновлений баз. Вы можете настроить уведомление администратора по этим событиям. • *Проверка важных областей давно не выполнялась*. Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком **Считать выполнение задачи проверкой важных областей**.
Возможные значения	Количество дней от 1 до 365.
Значение по умолчанию	Базы программы устарели – 7 дней; Базы программы сильно устарели – 14 дней; Проверка важных областей давно не выполнялась – 30 дней.

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач (см. раздел «Настройка параметров интеграции с SIEM« на стр. 346) на syslog-сервер.

3. Нажмите на кнопку **ОК**.

Внесенные изменения будут сохранены.

Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и снизить риск деградации системы в результате увеличения объемов журналов программы, вы можете настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер агрегации событий (SIEM), выполняющий сбор и анализ полученных событий, а также другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: этот режим предполагает, что все события выполнения задач, публикация которых настроенная в параметрах журналов, а также все события системного аудита продолжают храниться на локальном компьютере даже после отправки в SIEM.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: этот режим предполагает, что все события, зарегистрированные в ходе работы программы и опубликованные в SIEM, будут удалены с локального компьютера.

  > Программа никогда не удаляет локальные версии журнала нарушений безопасности

Kaspersky Embedded Systems Security 2.1 может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемой SIEM.

Параметры надежности

Вы можете снизить риск неудачной отправки событий в SIEM задав параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если подключение к основному syslog-серверу или его использование недоступны.

Также Kaspersky Embedded Systems Security 2.1 уведомляет вас о неудачной попытке подключения к SIEM и об ошибках отправки событий в SIEM с помощью событий системного аудита.

Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и отключать интеграцию с SIEM, а также настраивать параметры функциональности (см. таблицу ниже).

Таблица 37. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.

Параметр	Значение по умолчанию	Описание
Протокол подключения	UDP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UPD или TCP с помощью выпадающего списка.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Журналы и уведомления**.

2. Выберите пункт **Параметры**.

   Откроется окно **Параметры журналов**.

3. Выберите закладку **Интеграция с SIEM**.

4. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий в SIEM в соответствии с настроенными параметрами интеграции с SIEM.

   Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

   По умолчанию флажок снят.

5. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Флажок включает или отключает удаление локальных копий журналов по их отправке в SIEM.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы в SIEM. Рекомендуется использовать этот режим на маломощных компьютерах.

   Если флажок снят, программа только отправляет события в SIEM. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

6. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события по работе программы для их отправки в SIEM.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В блоке **Параметры принимающего syslog-сервера** выполните следующие действия:

   - Укажите протокол подключения к SIEM.
   - Укажите параметры соединения с основным syslog-сервером.

     Вы можете указать IP-адрес только в формате IPv4.

   - Если требуется, установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер недоступна. Укажите параметры подключения к зеркальному syslog-серверу.лажка.

     Поля **IP-адрес** и **Порт** для зеркального syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

     Вы можете указать IP-адрес только в формате IPv4.

8. Нажмите на кнопку **ОК**.

   Настроенные параметры интеграции с SIEM будут применены.

Лицензирование

Подробная информация о лицензировании Kaspersky Embedded Systems Security 2.1 содержится в *Руководстве Администратора Kaspersky Embedded Systems Security 2.1 2.1* в разделе Лицензирование программы.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Embedded Systems Security 2.1 о событиях программы и состоянии защиты компьютера, а также инструкцию по настройке уведомлений.

В этом разделе

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Embedded Systems Security 2.1 и состоянием антивирусной защиты компьютера.

Программа обеспечивает выполнение следующих задач:

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

В Консоли Kaspersky Embedded Systems Security 2.1 вы можете активировать уведомления администратора или пользователей несколькими способами:

- способы уведомления пользователей:

    a. Средства службы терминалов.

    Вы можете применять этот способ для оповещения терминальных пользователей, если защищаемый компьютер является терминальным.

    b. Средства службы сообщений.

    Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

- способы уведомления администраторов:

    a. Средства службы сообщений.

    Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

    b. Запуск исполняемого файла.

    Этот способ запускает по событию исполняемый файл, который хранится на локальном диске защищаемого компьютера.

    c. Отправка по электронной почте.

    Этот способ использует для передачи сообщений электронную почту.

Вы можете создавать текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется предустановленный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► *Чтобы настроить уведомления о событиях, выполните следующие действия:*

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Журналы** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов**.

2. На закладке **Уведомления** укажите способы уведомлений:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Вы можете настроить уведомления пользователей только для события **Обнаружен объект**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**. В окне **Текст сообщения** введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после того как вы выбрали способ уведомлений для одного типа событий, выберите, используя клавишу **CTRL** или клавишу **SHIFT**, остальные типы событий, для которых вы хотите составить такой же текст сообщения, перед тем как нажать на кнопку **Текст сообщения**.

b. 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.

c. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Если вы хотите настроить параметры для способов уведомлений уведомлений администраторов о выбранном событии, в окне **Уведомления** нажмите на кнопку **Настройка** и в окне **Дополнительные параметры** выполните настройку выбранных способов. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте откройте закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса символом «точка с запятой»), имя или сетевой адрес SMTP-сервера, а также его порт. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** вы также можете включать переменные с информацией о событии (см. таблицу ниже).

   Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

   b. Для уведомлений средствами службы сообщений на закладке **Служба сообщений**, составьте список компьютеров-получателей уведомлений: для каждого компьютера, который вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

   c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите на локальном диске защищаемого компьютера файл, который будет выполняться на компьютере по событию, или введите полный путь к нему. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Если вы хотите ограничить количество уведомлений по событиям одного типа в единицу времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите нужное количество раз и единицу времени.

5. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

Таблица 38. 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 и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя обнаруженного объекта согласно классификации Вирусной энциклопедии (http://www.securelist.ru). Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security 2.1 возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел «Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач« на стр. 335).

Переменная	Описание
%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 2.1 возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи (см. раздел «Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security 2.1 в журналах выполнения задач« на стр. 335).
%USER_COMPUTER%	В задаче Постоянная защита файлов имя компьютера пользователя, который обратился к объекту на компьютере.
%USER_NAME%	В задаче Постоянная защита файлов имя пользователя, который обратился к объекту на компьютере.
%FROM_COMPUTER%	Имя защищаемого компьютера, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (применяется только для события «внутренняя ошибка задачи»).
%TASK_NAME%	Имя задачи (имеется только у событий, связанных с выполнением задач).

Глоссарий

O

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы «Лаборатории Касперского» позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать 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.

В

Возможно зараженный файл

Файл, внутри которого содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Д

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

З

Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

К

Карантин

Папка, в которую программа «Лаборатории Касперского» перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный из-за того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- ***** – символ, заменяющий нуль или более нуля любых символов;
- **?** – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Объекты автозапуска

Набор программ, необходимых для запуска и 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

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

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 файлов, создаваемых перед их первым лечением или удалением.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах «Лаборатории Касперского» и управления ими.

У

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ «Лаборатории Касперского». Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Файлам, в которых во время эвристического анализа обнаружен вредоносный код, присваивается статус *зараженный*.

Эвристический анализатор

Модуль Kaspersky Embedded Systems Security 2.1, выполняющий эвристический анализ.

АО «Лаборатория Касперского»

«Лаборатория Касперского» – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). В России, по данным IDC, «Лаборатория Касперского» – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей («IDC Endpoint Tracker 2014»).

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами «Лаборатории Касперского».

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Предметный указатель

D

F

H

I

K

A

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

Р

С

Т