KASPERSKY lab

Kaspersky Security для виртуальных сред 4.0 Легкий агент для Windows

Руководство пользователя для Windows

Версия программы: 4.0

Уважаемый пользователь!

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

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

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

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

Документ может быть изменен без предварительного уведомления.

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

Дата редакции документа: 20.01.2017

© АО «Лаборатория Касперского», 2017.

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

Содержание

Об этом руководстве

Руководство пользователя Kaspersky Security для виртуальных сред 4.0 Легкий агент (далее также «Kaspersky Security») адресовано специалистам, которые осуществляют настройку Легкого агента, установленного на виртуальной машине с операционной системой Microsoft® Windows® (далее «Легкий агент для Windows»).

Для использования Kaspersky Security пользователю нужно быть знакомым с интерфейсом операционной системы Microsoft Windows, владеть основными приемами работы в ней, уметь работать с электронной почтой и интернетом.

В этом разделе

В этом документе

Этот документ содержит следующие разделы:

Kaspersky Security для виртуальных сред 4.0 Легкий агент (см. стр. 17)

Этот раздел содержит информацию о назначении, ключевых возможностях, составе программы, а также краткое описание функций и компонентов программы.

Интерфейс программы (см. стр. 21)

Этот раздел содержит информацию об основных элементах интерфейса программы.

Запуск и остановка программы (см. стр. 26)

Этот раздел содержит информацию о том, как запустить программу и как завершить работу с ней.

Состояние защиты виртуальной машины (см. стр. 30)

Этот раздел содержит информацию о том, как определить наличие угроз безопасности и настроить защиту от этих угроз.

Подключение защищенной виртуальной машины к SVM (см. стр. 34)

Этот раздел содержит информацию об особенностях и настройке подключения защищенной виртуальной машины к SVM.

Защита файловой системы виртуальной машины. Файловый Антивирус (см. стр. 38)

Этот раздел содержит информацию о Файловом Антивирусе и инструкции о том, как настроить параметры компонента.

Защита почты. Почтовый Антивирус (см. стр. 54)

Этот раздел содержит информацию о Почтовом Антивирусе и инструкции о том, как настроить параметры компонента.

Защита интернет-трафика виртуальной машины. Веб-Антивирус (см. стр. 68)

Этот раздел содержит информацию о Веб-Антивирусе и инструкции о том, как настроить параметры компонента.

Защита трафика IM-клиентов. IM-Антивирус (см. стр. 80)

Этот раздел содержит информацию об IM-Антивирусе и инструкции о том, как настроить параметры компонента.

Сетевая защита (см. стр. 86)

Этот раздел содержит информацию о принципах работы и настройке компонентов Сетевой экран, Защита от сетевых атак и Мониторинг сети, а также о контроле сетевого трафика.

Мониторинг системы (см. стр. 133)

Этот раздел содержит информацию о Мониторинге системы и инструкции о том, как настроить параметры компонента.

Контроль запуска программ (см. стр. 138)

Этот раздел содержит информацию о Контроле запуска программ и инструкции о том, как настроить параметры компонента.

Контроль активности программ (см. стр. 154)

Этот раздел содержит информацию о Контроле активности программ и инструкции о том, как настроить параметры компонента.

Контроль устройств (см. стр. 174)

Этот раздел содержит информацию о Контроле устройств и инструкции о том, как настроить параметры компонента.

Веб-Контроль (см. стр. 190)

Этот раздел содержит информацию о Веб-Контроле и инструкции о том, как настроить параметры компонента.

Проверка виртуальной машины (см. стр. 210)

Этот раздел содержит информацию об особенностях и настройке задач проверки, уровнях безопасности, методах и технологиях проверки, а также инструкции по работе с файлами, которые программа Kaspersky Security не обработала в процессе проверки виртуальной машины на вирусы и другие вредоносные программы.

Обновление баз и модулей программы (см. стр. 237)

Этот раздел содержит информацию об обновлении баз и модулей программы (далее также «обновления») и инструкции о том, как настроить параметры обновления.

Доверенная зона (см. стр. 243)

Этот раздел содержит информацию о доверенной зоне и инструкции о том, как настроить исключения и сформировать список доверенных программ.

Резервное хранилище (см. стр. 255)

Этот раздел содержит инструкции о том, как настроить параметры резервного хранилища и как работать с резервным хранилищем.

Работа с отчетами (см. стр. 262)

Этот раздел содержит инструкции о том, как настроить параметры отчетов и как работать с отчетами.

Уведомления (см. стр. 272)

Этот раздел содержит информацию об уведомлениях, оповещающих о событиях в работе Kaspersky Security, а также инструкции о том, как настроить уведомления о событиях.

Производительность Kaspersky Security и совместимость с другими программами (см. стр. 277)

Этот раздел содержит информацию о производительности Kaspersky Security и совместимости с другими программами, а также инструкции о том, как выбрать тип обнаруживаемых объектов и режим работы Kaspersky Security.

Самозащита Kaspersky Security (см. стр. 281)

Этот раздел содержит информацию о механизмах самозащиты программы Kaspersky Security и защиты от внешнего управления программой и инструкции о том, как настроить параметры этих механизмов.

Защита паролем (см. стр. 285)

Этот раздел содержит информацию об ограничении доступа к программе Kaspersky Security с помощью пароля.

Управление параметрами программы Kaspersky Security (см. стр. 289)

Этот раздел содержит инструкции о том, как перенести настроенные параметры программы в программу Kaspersky Security, установленную на другой виртуальной машине, а также как восстановить стандартные параметры работы программы.

Участие в Kaspersky Security Network (см. стр. 293)

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как проверить подключение к Kaspersky Security Network.

Глоссарий (см. стр. 296)

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

АО «Лаборатория Касперского» (см. стр. 301)

Этот раздел содержит информацию об АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 303)

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

Уведомления о товарных знаках (см. стр. 304)

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: ...	Примеры приведены в блоках на голубом фоне под заголовком «Пример».

Пример текста	Описание условного обозначения
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.

Kaspersky Security для виртуальных сред 4.0 Легкий агент

Kaspersky Security для виртуальных сред 4.0 Легкий агент представляет собой интегрированное решение, обеспечивающее комплексную защиту виртуальных машин под управлением гипервизоров Microsoft® Windows Server® с установленной ролью Hyper-V® (далее также «Microsoft Windows Server (Hyper-V)»), Citrix® XenServer, VMware ESXi™ или KVM (Kernel-based Virtual Machine), от различных видов информационных угроз, сетевых и мошеннических атак.

Программа Kaspersky Security оптимизирована для обеспечения максимальной производительности виртуальных машин, которые вы хотите защищать.

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

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

Компоненты программы

К компонентам контроля относятся следующие компоненты программы:

- **Контроль запуска программ**. Компонент отслеживает ваши попытки запуска программ и регулирует запуск программ.
- **Контроль активности программ**. Компонент регистрирует действия, совершаемые программами в операционной системе, установленной на защищенной виртуальной машине, и регулирует деятельность программ, исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к вашим персональным данным и ресурсам операционной системы. К персональным данным пользователя относятся

папка «Мои документы», файлы cookie, данные об активности в операционной системе, а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

- **Контроль устройств**. Компонент позволяет установить гибкие ограничения доступа к устройствам хранения данных (например, жесткие диски, съемные диски, CD/DVD-диски), сетевым устройствам (например, модемы), устройствам печати (например, принтеры) или интерфейсам, с помощью которых устройства подключаются к защищенной виртуальной машине (например, USB, Bluetooth, FireWire®).

- **Веб-Контроль**. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

Работа компонентов контроля основана на правилах:

- Контроль запуска программ использует правила контроля запуска программ.

- Контроль активности программ использует правила контроля программ.

- Контроль устройств использует правила доступа к устройствам и правила доступа к шинам подключения.

- Веб-Контроль использует правила доступа к веб-ресурсам.

К компонентам защиты относятся следующие компоненты программы:

- **Файловый Антивирус**. Компонент позволяет избежать заражения файловой системы операционной системы защищенной виртуальной машины. Компонент запускается при старте Kaspersky Security, постоянно находится в оперативной памяти и проверяет все открываемые, сохраняемые и запускаемые файлы в операционной системе защищенной виртуальной машины. Файловый Антивирус перехватывает каждое обращение к файлу и проверяет этот файл на вирусы и другие вредоносные программы.

- **Мониторинг системы**. Компонент собирает данные о действиях программ в операционной системе защищенной виртуальной машины и предоставляет эту информацию другим компонентам для более эффективной защиты.

- **Почтовый Антивирус**. Компонент проверяет входящие и исходящие сообщения электронной почты на вирусы и другие вредоносные программы.

- **Веб-Антивирус**. Компонент проверяет трафик, поступающий на защищенную виртуальную машину по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

- **IM-Антивирус**. Компонент проверяет входящий и исходящий трафик защищенной виртуальной машины, передающийся по протоколам IM-клиентов. Компонент обеспечивает безопасную работу со многими IM-клиентами.

- **Сетевой экран**. Компонент обеспечивает защиту персональных данных, хранящихся в операционной системе защищенной виртуальной машины пользователя, блокируя все возможные для операционной системы угрозы в то время, когда защищенная виртуальная машина подключена к интернету или к локальной сети. Компонент фильтрует всю сетевую активность согласно правилам двух типов: сетевым правилам программ и сетевым пакетным правилам (см. раздел «О сетевых правилах» на стр. 90).

- **Мониторинг сети**. Компонент предназначен для просмотра в режиме реального времени информации о сетевой активности защищенной виртуальной машины.

- **Защита от сетевых атак**. Компонент отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на защищенную виртуальную машину, Kaspersky Security блокирует сетевую активность атакующего компьютера.

Задачи и функции программы

В программе Kaspersky Security предусмотрены следующие задачи:

- **Полная проверка**. Программа Kaspersky Security выполняет тщательную проверку операционной системы защищенной виртуальной машины, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.

- **Выборочная проверка**. Программа Kaspersky Security проверяет объекты, выбранные пользователем.

- **Проверка важных областей**. Программа Kaspersky Security проверяет объекты, загрузка которых осуществляется при старте операционной системы защищенной виртуальной машины, системную память и объекты заражения руткитами.
- **Обновление**. Программа Kaspersky Security загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты операционной системы защищенной виртуальной машины от новых вирусов и других вредоносных программ.

Kaspersky Security включает ряд служебных функций, предназначенных для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе:

- **Отчеты**. В процессе работы программы для каждого компонента и задачи программы формируется отчет. Отчет содержит список событий, произошедших во время работы Kaspersky Security, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в «Лабораторию Касперского», чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.
- **Хранилище данных**. Если в ходе проверки операционной системы защищенной виртуальной машины на вирусы и другие вредоносные программы, программа Kaspersky Security обнаруживает зараженные файлы, она блокирует эти файлы. Копии вылеченных и удаленных файлов Kaspersky Security сохраняет в *резервном хранилище*. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Security помещает в список необработанных файлов. Вы можете восстанавливать файлы в папку их исходного размещения, а также очищать хранилище данных.
- **Уведомления**. Уведомления позволяют вам быть в курсе событий о текущем состоянии защиты операционной системы защищенной виртуальной машины и о работе Kaspersky Security. Уведомления могут отображаться на экране или доставляться по электронной почте.
- **Поддержка**. Все зарегистрированные пользователи программы Kaspersky Security могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос через портал Kaspersky CompanyAccount на веб-сайте Службы технической поддержки или получить консультацию по телефону (подробнее см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

Интерфейс программы

Этот раздел содержит информацию об основных элементах интерфейса программы.

В этом разделе

Значок программы в области уведомлений

Сразу после запуска Kaspersky Security значок программы появляется в области уведомлений панели задач Microsoft Windows®.

Значок программы выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню значка программы и главному окну программы.

Значок программы отражает состояние защиты виртуальной машины, а также показывает действия, которые программа выполняет в текущий момент:

- Значок  означает, что работа всех компонентов защиты программы включена.
- Значок  означает, что Kaspersky Security проверяет сообщение электронной почты.
- Значок  означает, что Kaspersky Security проверяет входящий или исходящий сетевой трафик.

- Значок  означает, что Kaspersky Security обновляет базы и модули программы.
- Значок  означает, что в работе Kaspersky Security произошли важные события, на которые нужно обратить внимание. Например, выключен Файловый Антивирус, базы и модули программы устарели.
- Значок  означает, что в работе Kaspersky Security произошли события критической важности. Например, сбой в работе компонента(ов), повреждение баз и модулей программы.

По умолчанию анимация значка программы выключена. Вы можете включить анимацию значка программы (см. раздел «Включение и выключение анимации значка программы» на стр. 22).

Включение и выключение анимации значка программы

► *Чтобы включить или выключить анимацию значка программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса программы.
3. Выполните одно из следующих действий:
   - Установите флажок **Использовать анимацию значка при выполнении задач**, если вы хотите включить анимацию значка программы.
   - Снимите флажок **Использовать анимацию значка при выполнении задач**, если вы хотите выключить анимацию значка программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контекстное меню значка программы

Вы можете открыть контекстное меню значка программы наведением курсора мыши на значок программы в области уведомлений панели задач Microsoft Windows и нажатием на правую клавишу мыши.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Security для виртуальных сред 4.0 Легкий агент**. Открывает закладку **Центр управления** главного окна программы. На закладке **Центр управления** вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и обнаруженных угрозах.
- **Настройка**. Открывает закладку **Настройка** главного окна программы. На закладке **Настройка** вы можете изменить параметры программы, установленные по умолчанию.
- **Приостановка защиты и контроля / Возобновление защиты и контроля**. Временно выключает / включает работу компонентов защиты и компонентов контроля. Этот пункт контекстного меню не влияет на выполнение задачи обновления и задач проверки и доступен только при выключенной политике Kaspersky Security Center.
- **Выключение политики / Включение политики**. Выключает / включает политику Kaspersky Security Center. Этот пункт доступен, если Kaspersky Security работает под политикой Kaspersky Security Center и в параметрах политики установлен пароль на выключение политики.
- **О программе**. Открывает информационное окно со сведениями о программе.
- **Выход**. Завершает работу Kaspersky Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти виртуальной машины.

Главное окно программы

В главном окне Kaspersky Security находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

► *Чтобы открыть главное окно Kaspersky Security, выполните одно из следующих действий:*

- наведите курсор на значок программы в области уведомлений панели задач Microsoft Windows и нажмите на левую клавишу мыши;
- в контекстном меню значка программы (см. раздел «Контекстное меню значка программы» на стр. 23) выберите пункт **Kaspersky Security для виртуальных сред 4.0 Легкий агент**;
- в меню **Пуск** выберите пункт **Программы** → **Kaspersky Security для виртуальных сред 4.0 Легкий агент**.

Главное окно программы можно условно разделить на три части:

- В верхней части окна расположены элементы интерфейса, с помощью которых вы можете просмотреть следующую информацию:
  - сведения о программе;
  - статистику репутационных баз;
  - список необработанных файлов;
  - хранилище резервных копий зараженных файлов, которые были удалены или изменены в ходе работы программы;
  - отчеты о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.
- В центральной части окна находятся закладки **Центр управления** и **Настройка**:
  - Закладка **Центр управления** позволяет регулировать работу компонентов и задач программы. Когда вы открываете главное окно программы, в нем отображается закладка **Центр управления**.
  - Закладка **Настройка** позволяет изменять параметры программы, установленные по умолчанию.

- В нижней части окна расположены ссылки:
  - **Справка**. По ссылке осуществляется переход к справочной системе Kaspersky Security.
  - **Поддержка**. По ссылке открывается окно **Поддержка** с информацией об операционной системе, текущей версии Kaspersky Security и ссылками на информационные ресурсы «Лаборатории Касперского».
  - **Лицензия**. По ссылке открывается окно **Лицензирование** с информацией о действующей лицензии.

Окно настройки параметров программы

Окно настройки параметров Kaspersky Security предназначено для настройки параметров работы программы в целом, отдельных ее компонентов, отчетов и хранилищ, задач проверки и задачи обновления.

► *Чтобы открыть окно настройки параметров программы, выполните одно из следующих действий:*

- выберите закладку **Настройка** в главном окне программы (см. раздел «Главное окно программы» на стр. 23);
- выберите пункт **Настройка** в контекстном меню значка программы (см. раздел «Контекстное меню значка программы» на стр. 23).

Окно настройки параметров программы состоит из двух частей:

- В левой части окна содержатся компоненты программы, задачи и другие составляющие, предназначенные для настройки.
- В правой части окна содержатся элементы управления, с помощью которых вы можете настроить работу составляющей, выбранной в левой части окна.

Запуск и остановка программы

Этот раздел содержит информацию о том, как запустить программу и как завершить работу с ней.

В этом разделе

Включение и выключение автоматического запуска программы

Под автоматическим запуском программы подразумевается запуск Kaspersky Security, который выполняется без вашего участия после старта операционной системы. Этот вариант запуска программы установлен по умолчанию.

В первый раз Kaspersky Security запускается автоматически после своей установки. В дальнейшем программа запускается автоматически после старта операционной системы.

► *Чтобы включить или выключить автоматический запуск программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. Выполните одно из следующих действий:

   - Установите флажок **Запускать Kaspersky Security для виртуальных сред 4.0 Легкий агент при включении виртуальной машины**, если вы хотите включить автоматический запуск программы.

- Снимите флажок **Запускать Kaspersky Security для виртуальных сред 4.0 Легкий агент при включении виртуальной машины**, если вы хотите выключить автоматический запуск программы.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и завершение работы программы вручную

Специалисты «Лаборатории Касперского» рекомендуют не завершать работу Kaspersky Security, поскольку в этом случае защита вашей виртуальной машины и ваших персональных данных окажется под угрозой. Если требуется, вы можете приостановить защиту (см. раздел «Приостановка и возобновление защиты и контроля виртуальной машины» на стр. 28) виртуальной машины на необходимый срок, не завершая работу программы.

► *Чтобы завершить работу программы вручную, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы (на стр. 23), который расположен в области уведомлений панели задач.

2. В контекстном меню выберите пункт **Выход**.

Запускать Kaspersky Security вручную требуется в том случае, если вы выключили автоматический запуск программы (см. раздел «Включение и выключение автоматического запуска программы» на стр. 26).

► *Чтобы запустить программу вручную,*

в меню **Пуск** выберите пункт **Программы → Kaspersky Security для виртуальных сред 4.0 Легкий агент**.

Приостановка и возобновление защиты и контроля виртуальной машины

Приостановка защиты и контроля виртуальной машины означает выключение на некоторое время всех компонентов защиты и компонентов контроля Kaspersky Security.

Индикатором работы программы служит значок программы в области уведомлений панели задач (см. раздел «Значок программы в области уведомлений» на стр. 21):

- Значок  свидетельствует о приостановке защиты и контроля виртуальной машины.
- Значок  свидетельствует о возобновлении защиты и контроля виртуальной машины.

Приостановка и возобновление защиты и контроля виртуальной машины не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля виртуальной машины были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

► *Чтобы приостановить или возобновить защиту и контроль виртуальной машины, выполните следующие действия:*

1. Если вы хотите приостановить защиту и контроль виртуальной машины, выполните следующие действия:

   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.

   b. В контекстном меню выберите пункт **Приостановка защиты и контроля**.

      Откроется окно **Приостановка защиты**.

   c. Выберите один из следующих вариантов:

      - **Приостановить на указанное время** – защита и контроль виртуальной машины включатся через интервал времени, указанный в раскрывающемся списке ниже. Вы можете выбрать нужный интервал в раскрывающемся списке.

- **Приостановить до перезагрузки** – защита и контроль виртуальной машины включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
- **Приостановить** – защита и контроль виртуальной машины включатся тогда, когда вы решите возобновить ее.

2. Если вы хотите возобновить защиту и контроль виртуальной машины, то вы можете это сделать в любой момент, независимо от того, какой вариант приостановки защиты и контроля виртуальной машины вы выбрали ранее. Чтобы возобновить защиту и контроль виртуальной машины, выполните следующие действия:

   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.

   b. В контекстном меню выберите пункт **Возобновление защиты и контроля**.

Состояние защиты виртуальной машины

Этот раздел содержит информацию о том, как определить наличие угроз безопасности и настроить защиту от этих угроз.

В этом разделе

Индикация состояния защиты виртуальной машины

Kaspersky Security информирует вас о событиях, определяющих текущее состояние защиты виртуальной машины, с помощью различных способов индикации в главном окне программы.

Kaspersky Security использует следующие способы индикации состояния защиты виртуальной машины:

- Индикация с помощью значков статуса работы компонентов и состояний работы компонентов Kaspersky Security. Возможны следующие варианты индикации:
  - В строке включенного компонента отображается зеленый значок статуса работы компонента. Справа отображается статистика о количестве проверенных этим компонентом объектов, найденных угроз и действиях компонента по устранению угроз.
  - В строке выключенного компонента отображается желтый значок статуса работы компонента. Статистика о работе компонента в этом случае не отображается.
  - Если все компоненты контроля или компоненты защиты выключены, в заголовке блока **Контроль рабочего места** или **Управление защитой** отображается состояние *выключен(о)*.

- Если один или несколько компонентов контроля или компонентов защиты выключен, в заголовке блока **Контроль рабочего места** или **Управление защитой** отображается состояние *частично включен(о) (работающих компонентов: <количество включенных компонентов блока> из <общее количество компонентов в блоке>)*.

- Индикация наличия угроз, обнаруженных компонентами Kaspersky Security (например, *разрешено запусков программ, запрещено запусков программ, проверено объектов, найдено угроз*):

  - Если блок **Контроль рабочего места** или **Управление защитой** свернут, индикация наличия угроз отображается в строке с общей статистикой о работе компонентов под заголовком блока.

  - Если блок **Контроль рабочего места** или **Управление защитой** развернут, индикация наличия угроз отображается в строке со статистикой о работе каждого компонента.

  В зависимости от угрозы информация об угрозе и ее уровне важности фиксируется в виде события и отображается на одной из закладок окна **Отчеты и Хранилища**:

  - **Отчеты**.
  - **Резервное хранилище**.
  - **Необработанные файлы**.

- Индикация с помощью сообщений о событиях в работе компонентов защиты Kaspersky Security, связанных с состоянием защищенной виртуальной машины (например, *Требуется перезагрузка виртуальной машины* или *Нет подключения к SVM*). Сообщения отображаются следующим образом:

  - Если блок **Управление защитой** свернут, то сообщение отображается вместо строки со статистикой под заголовком блока.

  - Если блок **Управление защитой** развернут, то сообщение отображается вместо строки со статистикой компонента Файловый Антивирус.

- Индикация с помощью сообщений о событиях, связанных с выполнением задач Kaspersky Security или отклонениями от оптимальной работы программы (например, базы и модули программы сильно устарели). Сообщения отображаются следующим образом:

  - Если блок **Управление задачами** свернут, то сообщения отображаются в информационной области под заголовком блока.

  - Если блок **Управление задачами** развернут, то сообщения отображаются вместо строки со статистикой и расписанием задачи обновления.

- Индикация с помощью сообщений о проблемах с лицензией.

  Если есть проблемы с лицензией (например, срок действия лицензии истек), то индикация в виде сообщений, выделенных красным цветом, отображается в окне **Лицензирование**, которое открывается по ссылке **Лицензия**, расположенной внизу главного окна программы.

Устранение проблем в защите виртуальной машины

Для устранения проблем в защите виртуальной машины вы можете выбрать следующие варианты действий:

- Немедленно устранить проблему. Обнаружив информацию о критических и важных событиях в состоянии защиты виртуальной машины, вы можете перейти к непосредственному устранению проблемы:

  - Если компонентом программы обнаружены проблемы в защите виртуальной машины, то с помощью пункта **Отчеты** контекстного меню компонента вы можете просмотреть информацию о файлах, в которых программа Kaspersky Security обнаружила угрозу, и выбрать действие над этими файлами (например, удалить файл или восстановить файл в папку исходного размещения).

  - Если требуется перезагрузка виртуальной машины, то вы можете закрыть все программы и перезагрузить виртуальную машину.

- Если базы и модули программы устарели, то вы можете запустить задачу обновления.

- Если есть проблемы с лицензией, то сообщение об этом отображается в окне **Лицензирование**, которое открывается по ссылке **Лицензия**, расположенной внизу главного окна программы. Для устранения проблемы с лицензией обратитесь к администратору.

- Отложить устранение проблемы. Если по какой-либо причине немедленное устранение проблемы невозможно, вы можете отложить это действие и вернуться к нему позже.

  Для серьезных проблем возможность отложить устранение не предусмотрена. К числу таких проблем относятся, например, сбой в работе одного или нескольких компонентов программы, повреждение файлов программы, окончание срока действия лицензии.

Подключение защищенной виртуальной машины к SVM

Этот раздел содержит информацию об особенностях подключения защищенной виртуальной машины к SVM.

В этом разделе

О подключении защищенной виртуальной машины к SVM

Для функционирования программы требуется подключение защищенной виртуальной машины к SVM с установленным Сервером защиты.

Если защищенная виртуальная машина не подключена ни к одной SVM, программа не проверяет файлы на защищенной виртуальной машине. Файлы, которые требуется проверять в соответствии с параметрами защиты, передаются на проверку после подключения к SVM.

Чтобы выбрать SVM для подключения, защищенная виртуальная машина должна получить информацию о SVM, работающих в сети. Защищенная виртуальная машина выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM. Подробнее о подключении защищенной виртуальной машины к SVM см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*.

Вы можете настроить параметры обнаружения SVM, которые использует защищенная виртуальная машина (см. раздел «Настройка параметров обнаружения SVM» на стр. 35).

Настройка параметров обнаружения SVM

► *Чтобы настроить параметры обнаружения SVM, работающих в сети, и получения о них информации, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Параметры обнаружения SVM**.

   В правой части окна отобразятся параметры обнаружения SVM.

3. Выберите способ, который защищенная виртуальная машина будет использовать для обнаружения SVM и получения информации о них:

   - **Использовать многоадресную рассылку (Multicast)**.

     Если выбран этот вариант, компонент Легкий агент получает информацию об SVM с помощью многоадресной рассылки (Multicast).

     Этот вариант выбран по умолчанию.

   - **Использовать Сервер интеграции**.

     Если выбран этот вариант, защищенная виртуальная машина подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам требуется указать параметры подключения защищенной виртуальной машины к Серверу интеграции.

   - **Использовать список адресов SVM, заданный вручную**.

     Если выбран этот вариант, вы можете указать список SVM, к которым может подключаться защищенная виртуальная машина.

4. Если вы выбрали вариант **Использовать Сервер интеграции**, укажите параметры подключения защищенной виртуальной машины к Серверу интеграции. Для этого выполните следующие действия:

   a. По умолчанию в поле **Адрес** указывается доменное имя компьютера, на котором установлена Консоль администрирования Kaspersky Security Center. Если этот

компьютер не входит в домен или Сервер интеграции установлен на другом компьютере и в поле указан неверный адрес, укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера интеграции.

b. Если порт для подключения к Серверу интеграции отличается от используемого по умолчанию (7271), укажите номер порта в поле **Порт**.

c. Если компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен, или ваша учетная запись не входит в группу KLAdmins или в группу локальных администраторов, откроется окно **Подключение к Серверу интеграции**. Укажите пароль администратора Сервера интеграции (пароль учетной записи admin). Подключение к Серверу интеграции с правами администратора требуется для получения от Сервера интеграции параметров учетной записи, которая используется для подключения защищенной виртуальной машины к Серверу интеграции.

   При сохранении параметров получения информации об SVM выполняется проверка возможности подключения к Серверу интеграции. Если проверка подключения закончилась неудачно или не удалось установить соединение с Сервером интеграции, проверьте введенные параметры подключения. Информация об ошибках подключения к Серверу интеграции записывается в журнал работы Сервера интеграции. Вы можете посмотреть журнал работы Сервера интеграции в Консоли управления Сервера интеграции (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент)*.

5. Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную**, сформируйте список SVM. Для этого выполните следующие действия:

   a. Нажмите на кнопку **Добавить**, расположенную над списком адресов SVM.

      Откроется окно **Адреса SVM**.

   b. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) той SVM, к которой может подключаться защищенная виртуальная машина. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе программы.

c. Нажмите на кнопку **ОК** в окне **Адреса SVM**.

   Выполняется проверка введенных адресов и полных доменных имен SVM. Если некоторые адреса или имена не распознаны, сообщение об этом и количество нераспознанных адресов или имен отображается в отдельном окне. Распознанные адреса и полные доменные имена отображаются в списке адресов SVM.

d. Если вы хотите удалить IP-адрес или полное доменное имя SVM из списка, выберите его в списке и нажмите на кнопку **Удалить**, расположенную над списком.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита файловой системы виртуальной машины. Файловый Антивирус

Этот раздел содержит информацию о Файловом Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Файловом Антивирусе

Файловый Антивирус позволяет избежать заражения файловой системы защищенной виртуальной машины. По умолчанию Файловый Антивирус запускается при старте Kaspersky Security, постоянно находится в оперативной памяти виртуальной машины и проверяет все открываемые, сохраняемые и запускаемые файлы на защищенной виртуальной машине на наличие в них вирусов и других вредоносных программ.

Файловый Антивирус использует методы сигнатурного и эвристического анализа, а также технологию iSwift. Перед проверкой файла Файловый Антивирус проверяет наличие информации об этом файле в базах iSwift и на основании полученных сведений принимает решение о необходимости проверки файла. Если при проверке в файле не обнаружены вирусы или другие вредоносные программы, Kaspersky Security разрешает доступ к этому файлу.

Если в результате проверки Файловый Антивирус обнаруживает угрозу в файле, Kaspersky Security присваивает файлу статус, обозначающий тип обнаруженного объекта (например, *вирус*, *троянская программа*).

После этого программа выводит на экран уведомление об обнаруженной в файле угрозе (если это указано в параметрах уведомлений) и выполняет над файлом действие, заданное в параметрах Файлового Антивируса.

Включение и выключение Файлового Антивируса

По умолчанию Файловый Антивирус включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Файловый Антивирус при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Файловый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши откройте контекстное меню строки **Файловый Антивирус** с информацией о компоненте Файловый Антивирус.

   Откроется меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Файловый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .

   - Выберите в меню пункт **Выключить**, если вы хотите выключить Файловый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Файловый Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

    - Установите флажок **Включить Файловый Антивирус**, если вы хотите включить Файловый Антивирус.

    - Снимите флажок **Включить Файловый Антивирус**, если вы хотите выключить Файловый Антивирус.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Файлового Антивируса

Вы можете выполнить следующие действия для настройки работы Файлового Антивируса:

- Настроить автоматическую приостановку работы Файлового Антивируса по расписанию или при запуске программ.

- Изменить уровень безопасности файлов.

  Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. После того как вы изменили параметры уровня безопасности файлов, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности файлов.

- Изменить действие, которое Файловый Антивирус выполняет при обнаружении зараженного файла.

- Сформировать область защиты Файлового Антивируса.

  Вы можете расширить или сузить область защиты, добавив или удалив объекты проверки или изменив тип проверяемых файлов.

- Настроить использование эвристического анализа.

  Во время своей работы Файловый Антивирус использует сигнатурный анализ. В процессе сигнатурного анализа Файловый Антивирус сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов «Лаборатории Касперского» сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Файловый Антивирус анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

- Настроить использование технологии проверки iSwift.

  Вы можете включить использование технологии iSwift, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки. Включение технологии iSwift также подразумевает использование технологии SharedCache, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, уже проверенных на другой виртуальной машине.

- Оптимизировать проверку.

  Вы можете оптимизировать проверку файлов Файловым Антивирусом: сократить время проверки и увеличить скорость работы Kaspersky Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

- Настроить проверку составных файлов.

- Изменить режим проверки файлов.

В этом разделе

Автоматическая приостановка работы Файлового Антивируса

Вы можете настроить автоматическую приостановку работы компонента Файловый Антивирус в указанное время или во время работы с определенными программами.

Приостановка работы Файлового Антивируса при конфликте с определенными программами является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, обратитесь в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/#s_tab4).

► *Чтобы настроить автоматическую приостановку работы Файлового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** выберите закладку **Дополнительно**.
5. В блоке **Приостановка работы** выполните следующие действия:

   - Установите флажок **По расписанию** и нажмите на кнопку **Расписание**, если вы хотите настроить автоматическую приостановку работы Файлового Антивируса в указанное время.

     Откроется окно **Приостановка работы**.

- Установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**, если вы хотите настроить автоматическую приостановку работы Файлового Антивируса при запуске указанных программ.

  Откроется окно **Программы**.

6. Выполните одно из следующих действий:

   - Если вы настраиваете автоматическую приостановку работы Файлового Антивируса в указанное время, то в окне **Приостановка работы** в полях **Приостановить в** и **Возобновить в** укажите время (в формате ЧЧ:ММ), в течение которого работу Файлового Антивируса следует приостанавливать. Далее нажмите на кнопку **OK**.

   - Если вы настраиваете автоматическую приостановку работы Файлового Антивируса при запуске указанных программ, то в окне **Программы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список программ, во время работы которых работу Файлового Антивируса следует приостанавливать. Далее нажмите на кнопку **OK**.

7. В окне **Файловый Антивирус** нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение уровня безопасности файлов

Для защиты файловой системы виртуальной машины Файловый Антивирус применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности файлов*. Предусмотрено три уровня безопасности файлов: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности файлов **Рекомендуемый** считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского».

► *Чтобы изменить уровень безопасности файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите установить один из предустановленных уровней безопасности файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.

   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Файловый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.

   - Если вы хотите изменить уровень безопасности файлов на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия Файлового Антивируса над зараженными файлами

► *Чтобы изменить действие Файлового Антивируса над зараженными файлами, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:

   - **Выбирать действие автоматически**.

     Этот вариант выбран по умолчанию. При обнаружении угрозы программа выполняет действие **Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.

- **Выполнять действие: Лечить**.

  В отношении файлов, являющихся частью приложения Windows Store, Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

- **Выполнять действие: Удалять**.
- **Выполнять действие: Блокировать**.

При удалении или лечении копии файлов сохраняются в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области защиты Файлового Антивируса

Областью защиты называются объекты, которые компонент проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Файлового Антивируса являются местоположение и тип проверяемых файлов. По умолчанию Файловый Антивирус проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков виртуальной машины.

► *Чтобы сформировать область защиты Файлового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Общие**.

5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять Файловым Антивирусом:

   - Выберите **Все файлы**, если вы хотите проверять все файлы.
   - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
   - Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

   Выбирая тип проверяемых файлов, нужно помнить следующее:

   - Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
   - Злоумышленник может отправить вирус или другую вредоносную программу на вашу виртуальную машину в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие вредоносные программы.

6. В блоке **Область защиты** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите удалить объект из области защиты, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.

7. В окне **Выбор объекта** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта**, отобразятся в списке **Область защиты** в окне **Файловый Антивирус**.

     Нажмите на кнопку **OK**.

   - Если вы хотите изменить путь к объекту из списка объектов, укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **OK**.

   - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.

8. При необходимости повторите пункты 6 и 7 для добавления объектов, изменения пути к ним или удаления объектов из области защиты.

9. Если вы хотите исключить объект из области защиты, в списке **Область защиты** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но исключается из проверки Файловым Антивирусом.

10. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования эвристического анализа в работе Файлового Антивируса

► *Чтобы настроить использование эвристического анализа в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Производительность**.

5. В блоке **Методы проверки** выполните одно из следующих действий:

   - Если вы хотите, чтобы Файловый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   - Если вы хотите, чтобы Файловый Антивирус не использовал эвристический анализ, снимите флажок **Эвристический анализ**.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования технологии iSwift в работе Файлового Антивируса

► *Чтобы настроить использование технологии iSwift в работе Файлового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Дополнительно**.

5. В блоке **Технология проверки** выполните одно из следующих действий:

   - Установите флажок **Технология iSwift**, если вы хотите использовать эту технологию в работе Файлового Антивируса.
   - Снимите флажок **Технология iSwift**, если вы не хотите использовать эту технологию в работе Файлового Антивируса.

   Включение технологии iSwift включает использование технологии SharedCache.

6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов Файловым Антивирусом

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.

4. Выберите закладку **Производительность**.
5. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов Файловым Антивирусом

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** на закладке **Производительность** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты или вложенные OLE-объекты, установив соответствующие флажки.
5. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение после нажатия на нее левой клавишей мыши.

   Если флажок **Проверять только новые и измененные файлы** установлен, то проверяются только новые файлы.
6. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.

7. В блоке **Фоновая проверка** выполните одно из следующих действий:

   - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.

   - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера в фоновом режиме, установите флажок **Распаковывать составные файлы в фоновом режиме** и в поле **Минимальный размер файла** укажите нужное значение.

8. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

   - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

     Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

   > Файловый Антивирус проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

9. Нажмите на кнопку **OK** в окне **Составные файлы**.

10. Нажмите на кнопку **OK** в окне **Файловый Антивирус**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять файлы. По умолчанию Kaspersky Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, Файловый Антивирус принимает решение о проверке файлов на основании анализа операций, которые вы, программа от вашего имени или имени другого пользователя (на основании учетных данных, с которыми был осуществлен вход в операционную систему) или операционная система выполняют над файлами. Например, работая с документом Microsoft Office Word, Kaspersky Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** выберите закладку **Дополнительно**.
5. В блоке **Режим проверки** выберите нужный режим:
   - **Интеллектуальный**.
   - **При доступе и изменении**.
   - **При доступе**.
   - **При выполнении**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита почты. Почтовый Антивирус

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows.

Этот раздел содержит информацию о Почтовом Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Почтовом Антивирусе

Почтовый Антивирус проверяет входящие и исходящие сообщения электронной почты (далее также «сообщения» и «почта») на наличие в них вирусов и других вредоносных программ. Почтовый Антивирус запускается при старте Kaspersky Security, постоянно находится в оперативной памяти виртуальной машины и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP и NNTP.

Почтовый Антивирус не поддерживает протоколы, которые обеспечивают защищенную передачу данных.

Индикатором работы Почтового Антивируса служит значок программы в области уведомлений панели задач (см. раздел «Значок программы в области уведомлений» на стр. 21). Значок программы принимает вид  каждый раз при проверке сообщения, если включена анимация значка программы (см. раздел «Включение и выключение анимации значка программы» на стр. 22).

Почтовый Антивирус перехватывает и проверяет каждое сообщение электронной почты, которое вы принимаете или отправляете. Если угрозы в сообщении не обнаружены, сообщение становится доступным для вас.

Если в результате проверки Почтовый Антивирус обнаруживает угрозу в сообщении, Kaspersky Security присваивает сообщению статус, обозначающий тип обнаруженного объекта (например, *вирус*, *троянская программа*).

После этого программа блокирует сообщение, выводит на экран уведомление (если это указано в параметрах уведомлений) об обнаруженной угрозе и выполняет заданное в параметрах Почтового Антивируса действие (см. раздел «Изменение действия над зараженными сообщениями электронной почты» на стр. 59).

Для программы Microsoft Office Outlook® предусмотрен плагин, позволяющий производить более тонкую настройку параметров проверки сообщений. Плагин Почтового Антивируса встраивается в программу Microsoft Office Outlook во время установки Kaspersky Security.

Включение и выключение Почтового Антивируса

По умолчанию Почтовый Антивирус включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Почтовый Антивирус при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Почтовый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.

4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Почтовый Антивирус.

   Откроется меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Почтовый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .

   - Выберите в меню пункт **Выключить**, если вы хотите выключить Почтовый Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Почтовый Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

- Установите флажок **Включить Почтовый Антивирус**, если вы хотите включить Почтовый Антивирус.
- Снимите флажок **Включить Почтовый Антивирус**, если вы хотите выключить Почтовый Антивирус.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Почтового Антивируса

Вы можете выполнить следующие действия для настройки работы Почтового Антивируса:

- Изменить уровень безопасности почты.

  Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно.

  После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

- Изменить действие, которое Kaspersky Security выполняет над зараженными сообщениями электронной почты.
- Сформировать область защиты Почтового Антивируса.
- Настроить проверку вложенных в сообщения объектов.

  Вы можете включить или выключить проверку вложенных в сообщения архивов, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки вложенных в сообщения объектов.

- Настроить фильтрацию по типу вложений в сообщениях электронной почты.

  Фильтрация по типу вложений в сообщениях позволяет автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Security может защитить вашу виртуальную машину от автоматического запуска вредоносной программы.

- Настроить использование эвристического анализа.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать в сообщениях новые вредоносные объекты, записей о которых еще нет в базах Kaspersky Security.

- Настроить параметры проверки почты в программе Microsoft Office Outlook.

  Для программы Microsoft Office Outlook предусмотрен встраиваемый плагин, позволяющий настраивать параметры проверки почты.

  Работая с остальными программами (в том числе с Microsoft Outlook Express, Windows Mail и Mozilla™ Thunderbird™), Почтовый Антивирус проверяет почту на трафике по протоколам SMTP, POP3, IMAP и NNTP.

  > Работая с программой Mozilla Thunderbird, Почтовый Антивирус не проверяет сообщения, передаваемые по протоколу IMAP на вирусы и другие вредоносные программы в случае, если используются фильтры, перемещающие сообщения из папки «Входящие».

В этом разделе

Изменение уровня безопасности почты

Для защиты почты Почтовый Антивирус применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности почты*. Предусмотрено три

уровня безопасности почты: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами «Лаборатории Касперского».

► *Чтобы изменить уровень безопасности почты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите установить один из предустановленных уровней безопасности почты (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Почтовый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить настроенный самостоятельно уровень безопасности почты на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над зараженными сообщениями электронной почты

► *Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое программа Kaspersky Security выполняет при обнаружении зараженного сообщения электронной почты:

   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно.**
   - **Выполнять действие: Лечить.**
   - **Выполнять действие: Удалять.**
   - **Выполнять действие: Блокировать.**

   По умолчанию выбран вариант **Выполнять действие: Лечить. Удалять, если лечение невозможно**.

   > При удалении или лечении сообщений копии сообщений сохраняются в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области защиты Почтового Антивируса

Под областью защиты подразумеваются объекты, которые компонент проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Почтового Антивируса являются параметры интеграции Почтового Антивируса в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет Почтовый Антивирус. По умолчанию Kaspersky Security проверяет входящие и исходящие сообщения, трафик почтовых

протоколов POP3, SMTP, IMAP и NNTP, а также интегрируется в программу Microsoft Office Outlook.

► *Чтобы сформировать область защиты Почтового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
4. В окне **Почтовый Антивирус** выберите закладку **Общие**.
5. В блоке **Область защиты** выполните одно из следующих действий:

   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял все входящие и исходящие сообщения на вашей виртуальной машине.
   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял только входящие сообщения на вашей виртуальной машине.

   > Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашей виртуальной машине есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать неприятностей, связанных с неконтролируемой рассылкой зараженных сообщений с вашей виртуальной машины.
6. В блоке **Встраивание в систему** выполните следующие действия:

- Установите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы Почтовый Антивирус проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на вашей виртуальной машине.

  Снимите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы Почтовый Антивирус не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на вашей виртуальной машине. В этом случае сообщения проверяет плагин Почтового Антивируса, встроенный в программу Microsoft Office Outlook, после их получения на вашей виртуальной машине.

  > Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Трафик POP3 / SMTP / NNTP / IMAP** Почтовый Антивирус не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

  > Если флажок **Дополнительно: плагин в Microsoft Office Outlook** снят, то Почтовый Антивирус также не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок **Дополнительно: плагин в Microsoft Office Outlook**, если вы хотите открыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP и IMAP, после их получения на вашей виртуальной машине на стороне плагина, интегрированного в программу Microsoft Office Outlook.

  Снимите флажок **Дополнительно: плагин в Microsoft Office Outlook**, если вы хотите закрыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP и IMAP, после их получения на вашей виртуальной машине на стороне плагина, интегрированного в программу Microsoft Office Outlook.

Плагин Почтового Антивируса встраивается в программу Microsoft Office Outlook во время установки Kaspersky Security.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

► *Чтобы настроить проверку вложенных в сообщения объектов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

4. В окне **Почтовый Антивирус** выберите закладку **Общие**.

5. В блоке **Проверка составных файлов** выполните следующие действия:

   - Снимите флажок **Проверять вложенные архивы**, если вы хотите, чтобы Почтовый Антивирус не выполнял проверку вложенных в сообщения архивов.

   - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы Почтовый Антивирус не проверял вложенные в сообщения архивы размером более N мегабайт. Если вы установили этот флажок, укажите максимальный размер архивов в поле рядом с названием флажка.

   - Установите флажок **Не проверять архивы более N с**, если вы хотите, чтобы Почтовый Антивирус не проверял вложенные в сообщения архивы, если на их проверку затрачивается более N секунд. Если вы установили этот флажок, укажите максимальное время проверки архивов в поле рядом с названием флажка.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Фильтрация вложений в сообщениях

Вредоносные программы могут распространяться через почту в виде вложений в сообщениях. Вы можете настроить фильтрацию по типу вложений в сообщениях электронной почты, которая позволяет автоматически переименовывать или удалять файлы указанных типов.

► *Чтобы настроить фильтрацию вложений, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
4. В окне **Почтовый Антивирус** выберите закладку **Фильтр вложений**.
5. Выполните одно из следующих действий:

   - Выберите вариант **Не применять фильтр**, если вы хотите, чтобы Почтовый Антивирус не фильтровал вложения в сообщениях.
   - Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус изменял названия вложенных в сообщения файлов указанных типов.
   - Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус удалял вложенные в сообщения файлы указанных типов.
6. Если в пункте 5 инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, становится активным список типов файлов. Установите флажки напротив нужных типов файлов.

Вы можете изменить список типов файлов с помощью кнопок **Добавить**, **Изменить**, **Удалить**.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе Почтового Антивируса

► *Чтобы настроить использование эвристического анализа в работе Почтового Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

4. В окне **Почтовый Антивирус** выберите закладку **Дополнительно**.

5. В блоке **Метод проверки** выполните следующие действия:

   - Если вы хотите, чтобы Почтовый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   - Если вы хотите, чтобы Почтовый Антивирус не использовал эвристический анализ, снимите флажок **Эвристический анализ**.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка почты в Microsoft Office Outlook

Во время установки Kaspersky Security в программу Microsoft Office Outlook встраивается специальный плагин. Он позволяет перейти к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других вредоносных программ.

Почтовый плагин программы Microsoft Office Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP и IMAP.

> Настройка параметров Почтового Антивируса из программы Microsoft Office Outlook доступна в том случае, если в интерфейсе программы Kaspersky Security установлен флажок **Дополнительно: плагин в Microsoft Office Outlook**.

В программе Microsoft Office Outlook входящие сообщения сначала проверяет Почтовый Антивирус (если в интерфейсе программы Kaspersky Security установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), а затем проверяет почтовый плагин программы Microsoft Office Outlook. Если Почтовый Антивирус обнаруживает в сообщении электронной почты вредоносный объект, он уведомляет вас об этом.

Исходящие сообщения сначала проверяет почтовый плагин программы Microsoft Office Outlook, а затем проверяет Почтовый Антивирус.

От выбора действия в окне уведомления зависит, кто устраняет угрозу в сообщении: Почтовый Антивирус или почтовый плагин программы Microsoft Office Outlook:

- Если в окне уведомления Почтового Антивируса вы выбираете действие **Лечить** или **Удалить**, то действие по устранению угрозы выполняет Почтовый Антивирус.
- Если в окне уведомления Почтового Антивируса вы выбираете действие **Пропустить**, то действие по устранению угрозы выполняет почтовый плагин программы Microsoft Office Outlook.

► *Чтобы перейти к настройке параметров проверки почты в программе Microsoft Office Outlook, выполните следующие действия:*

1. Откройте главное окно Microsoft Office Outlook.
2. В меню программы выберите пункт **Сервис** → **Параметры**.

Откроется окно **Параметры**.

3. В окне **Параметры** выберите закладку **Защита почты**.

Защита интернет-трафика виртуальной машины. Веб-Антивирус

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows.

Этот раздел содержит информацию о Веб-Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Веб-Антивирусе

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на виртуальной машине, риску заражения вирусами и другими программами, представляющими угрозу. Они могут проникать на виртуальную машину, когда вы скачиваете бесплатные программы или просматриваете информацию на веб-сайтах, которые до вашего посещения подверглись атаке хакеров. Сетевые черви могут проникнуть на вашу виртуальную машину до открытия веб-страницы или скачивания файла, непосредственно в момент установки соединения с интернетом.

Веб-Антивирус защищает информацию, поступающую на вашу виртуальную машину и отправляемую с нее по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

Каждую веб-страницу или файл, к которому вы или некоторая программа обращаетесь по протоколу HTTP или FTP, Веб-Антивирус перехватывает и анализирует на присутствие вирусов и других программ, представляющих угрозу. Далее происходит следующее:

- если на веб-странице или в файле не обнаружен вредоносный код, они сразу же становятся доступными для вас;
- если веб-страница или файл содержат вредоносный код, программа выполняет заданное в параметрах Веб-Антивируса действие (см. раздел «Изменения действия над вредоносными объектами веб-трафика» на стр. 74).

Веб-Антивирус не поддерживает протоколы, которые обеспечивают защищенную передачу данных.

Включение и выключение Веб-Антивируса

По умолчанию Веб-Антивирус включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Веб-Антивирус при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Веб-Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.

4. По правой клавише мыши откройте контекстное меню строки **Веб-Антивирус** с информацией о компоненте Веб-Антивирус.

   Откроется меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .

   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Веб-Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Веб-Антивирус**, если вы хотите включить Веб-Антивирус.
   - Снимите флажок **Включить Веб-Антивирус**, если вы хотите выключить Веб-Антивирус.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Веб-Антивируса

Вы можете выполнить следующие действия для настройки работы Веб-Антивируса:

- Изменить уровень безопасности веб-трафика.

  Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно.

  После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

- Изменить действие, которое Kaspersky Security выполняет над вредоносными объектами веб-трафика.

  Если в результате проверки Веб-Антивирусом объекта веб-трафика выясняется, что объект содержит вредоносный код, дальнейшие операции Веб-Антивируса с этим объектом зависят от указанного вами действия.

- Настроить проверку Веб-Антивирусом ссылок по базам фишинговых и вредоносных веб-адресов.

- Настроить использование эвристического анализа при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу.

  Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах Kaspersky Security.

- Настроить использование эвристического анализа при проверке веб-страниц на наличие фишинговых ссылок.
- Оптимизировать проверку Веб-Антивирусом веб-трафика.

  Для оптимизации проверки веб-трафика вы можете настроить продолжительность кеширования Веб-Антивирусом веб-трафика, исходящего и поступающего по протоколам HTTP и FTP.
- Сформировать список доверенных веб-адресов.

  Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Веб-Антивирус не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других программ, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если Веб-Антивирус препятствует загрузке файла с известного вам веб-сайта.

  > Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

В этом разделе

Изменение уровня безопасности веб-трафика

Для защиты данных, получаемых и передаваемых по протоколам HTTP и FTP, Веб-Антивирус применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности веб-трафика*. Предусмотрено три уровня безопасности веб-трафика: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами «Лаборатории Касперского».

► *Чтобы изменить уровень безопасности веб-трафика, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. В блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.

   - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Веб-Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке **Уровень безопасности** изменится на **Другой**.

   - Если вы хотите изменить уровень безопасности веб-трафика на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменения действия над вредоносными объектами веб-трафика

► *Чтобы изменить действие над вредоносными объектами веб-трафика, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Security выполняет над вредоносными объектами веб-трафика:

   - **Выбирать действие автоматически**.
   - **Запрещать загрузку**.
   - **Разрешать загрузку**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка Веб-Антивирусом ссылок по базам фишинговых и вредоносных веб-адресов

Проверка ссылок на принадлежность к фишинговым веб-адресам позволяет избежать *фишинг-атак*. Частным примером фишинг-атаки может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадете на точную копию веб-сайта банка, адрес которого, на первый взгляд, не будет отличаться от адреса оригинального веб-сайта. Однако вы будете находиться на фиктивном веб-сайте. Все ваши дальнейшие действия будут отслеживаться и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в тексте ICQ-сообщения, Веб-Антивирус отслеживает попытки перейти на фишинговый веб-сайт во время проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Security и обновляются при наличии обновления списков в базах программы.

► *Чтобы настроить проверку Веб-Антивирусом ссылок по базам фишинговых и вредоносных веб-адресов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. В окне **Веб-Антивирус** выберите закладку **Общие**.
5. Выполните следующие действия:

   - В блоке **Методы проверки** установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите, чтобы Веб-Антивирус проверял ссылки по базам вредоносных веб-адресов.
   - В блоке **Параметры антифишинга** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите, чтобы Веб-Антивирус проверял ссылки по базам фишинговых веб-адресов.

   > Для проверки ссылок по базам фишинговых и вредоносных веб-адресов вы также можете использовать репутационные базы Kaspersky Security Network.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе Веб-Антивируса

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

4. В окне **Веб-Антивирус** выберите закладку **Общие**.

5. Выполните следующие действия:

   - Если вы хотите, чтобы Веб-Антивирус использовал эвристический анализ при проверке веб-трафика на наличие вирусов и других вредоносных программ, в блоке **Методы проверки** установите флажок **Эвристический анализ для обнаружения вирусов** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   - Если вы хотите, чтобы Веб-Антивирус использовал эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок, в блоке **Параметры антифишинга** установите флажок **Эвристический анализ для обнаружения фишинговых ссылок** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка продолжительности кеширования веб-трафика

Для повышения эффективности обнаружения вредоносного кода Веб-Антивирус применяет кеширование фрагментов объектов, поступающих из интернета. Используя кеширование, Веб-Антивирус проверяет объекты только после того, как они полностью получены на защищенную виртуальную машину.

Кеширование увеличивает продолжительность обработки объектов и передачи их вам для работы. Кроме того, кеширование может вызывать проблемы при загрузке и обработке больших объектов, связанные с истечением времени ожидания на соединение HTTP-клиента.

Для решения этой проблемы предусмотрена возможность ограничивать продолжительность кеширования фрагментов объектов, поступающих из интернета. По истечении определенного времени каждая полученная часть объекта передается вам непроверенной, а по завершении копирования объект проверяется целиком. Это позволяет уменьшить продолжительность передачи вам объектов и решить проблему разрыва соединения. Уровень безопасности работы в интернете при этом не снижается.

Снятие ограничения на продолжительность кеширования веб-трафика повышает эффективность антивирусной проверки, но одновременно замедляет доступ к объектам.

► *Чтобы настроить продолжительность кеширования веб-трафика, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. В окне **Веб-Антивирус** выберите закладку **Общие**.

5. В блоке **Действия** выполните одно из следующих действий:

   - Установите флажок **Ограничивать продолжительность кеширования веб-трафика**, если вы хотите ограничить продолжительность кеширования веб-трафика и ускорить его проверку.

   - Снимите флажок **Ограничивать продолжительность кеширования веб-трафика**, если вы хотите отменить ограничение на продолжительность кеширования веб-трафика.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка доверенных веб-адресов

► *Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

4. Выберите закладку **Доверенные веб-адреса**.

5. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.

6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для этого выполните следующие действия:

    a. Нажмите на кнопку **Добавить**.

       Откроется окно **Адрес / Маска адреса**.

    b. Введите адрес веб-сайта (или веб-страницы) или маску адреса веб-сайта (или веб-страницы).

    c. Нажмите на кнопку **OK**.

       В списке доверенных веб-адресов появится новая запись.

    d. Повторите пункты a-c инструкции, если это требуется.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита трафика IM-клиентов. IM-Антивирус

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows.

Этот раздел содержит информацию об IM-Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

Об IM-Антивирусе

IM-Антивирус предназначен для проверки трафика, передаваемого IM-клиентами.

Сообщения, переданные через IM-клиенты, могут содержать следующие виды угроз безопасности виртуальной машины:

- Ссылки, при активации которых на вашу виртуальную машину пытается загрузиться вредоносная программа.
- Ссылки на вредоносные программы и веб-страницы, которые злоумышленники используют для фишинг-атак.

  Целью фишинг-атак является хищение персональных данных пользователей, например: номеров банковских карт, паспортных данных, паролей к платежным системам банков или другим интернет-сервисам (например, социальным сетям или почтовым сервисам).

Через IM-клиенты можно передавать файлы. Во время попытки сохранения этих файлов их проверяет компонент Файловый Антивирус (см. раздел «О Файловом Антивирусе» на стр. 38).

IM-Антивирус перехватывает каждое сообщение, которое вы принимаете или отправляете с помощью IM-клиента, и проверяет сообщение на наличие в нем ссылок, представляющих угрозу безопасности виртуальной машины.

Далее происходит следующее:

- если в сообщении не обнаружены ссылки, представляющие угрозу, сообщение становится доступным для вас;
- если в сообщении обнаружены ссылки, представляющие угрозу, IM-Антивирус заменяет это сообщение информацией об обнаруженной угрозе в окне переписки используемого IM-клиента.

Включение и выключение IM-Антивируса

По умолчанию IM-Антивирус включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить IM-Антивирус при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить IM-Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.

4. По правой клавише мыши на строке **IM-Антивирус** откройте контекстное меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить IM-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **IM-Антивирус**, изменится на значок .

   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить IM-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **IM-Антивирус**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить IM-Антивирус из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить IM-Антивирус**, если вы хотите включить IM-Антивирус.
   - Снимите флажок **Включить IM-Антивирус**, если вы хотите выключить IM-Антивирус.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка IM-Антивируса

Вы можете выполнить следующие действия для настройки работы IM-Антивируса:

- Сформировать область защиты.

  Вы можете расширить или сузить область защиты, изменив тип проверяемых сообщений, поступающих через IM-клиенты.

- Настроить проверку IM-Антивирусом ссылок в сообщениях IM-клиентов по базам вредоносных и фишинговых веб-адресов.

- Настроить использование эвристического анализа.

  Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать в сообщениях IM-клиентов угрозы, записей о которых еще нет в базах Kaspersky Security.

В этом разделе

Формирование области защиты IM-Антивируса

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойством области защиты IM-Антивируса является тип проверяемых сообщений, поступающих и отправляемых через IM-клиенты. По умолчанию IM-Антивирус проверяет как входящие, так и исходящие сообщения. Вы можете отказаться от проверки исходящих сообщений.

► *Чтобы сформировать область защиты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.
3. В блоке **Область защиты** выполните одно из следующих действий:
   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы IM-Антивирус проверял все входящие и исходящие сообщения IM-клиентов.
   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы IM-Антивирус проверял только входящие сообщения IM-клиентов.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка IM-Антивирусом ссылок по базам вредоносных и фишинговых веб-адресов

► *Чтобы настроить проверку IM-Антивирусом ссылок по базам вредоносных и фишинговых веб-адресов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.
3. В блоке **Методы проверки** установите флажки около названий тех методов, которые вы хотите использовать в работе IM-Антивируса:

- Установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите проверять ссылки в сообщениях IM-клиентов на их принадлежность к базе вредоносных веб-адресов.

- Установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите проверять ссылки в сообщениях IM-клиентов на их принадлежность к базе фишинговых веб-адресов.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе IM-Антивируса

► *Чтобы настроить использование эвристического анализа в работе IM-Антивируса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.

3. В блоке **Методы проверки** выполните следующие действия:

   a. Установите флажок **Эвристический анализ**.

   b. При помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Сетевая защита

Этот раздел содержит информацию о принципах работы и настройке компонентов Сетевой экран, Защита от сетевых атак и Мониторинг сети, а также о контроле сетевого трафика.

В этом разделе

Сетевой экран

Этот раздел содержит информацию о Сетевом экране и инструкции о том, как настроить параметры компонента.

В этом разделе

О Сетевом экране

Во время работы в локальных сетях и интернете ваша виртуальная машина подвержена не только заражению вирусами и другими программами, представляющими угрозу, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения.

Сетевой экран обеспечивает защиту персональных данных, хранящихся на вашей защищенной виртуальной машине, блокируя сетевые угрозы в то время, когда виртуальная машина подсоединена к сети Интернет или к локальной сети. Сетевой экран позволяет обнаружить все сетевые соединения на вашей виртуальной машине и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

При удаленном подключении к защищенной виртуальной машине после установки программы по умолчанию включается Сетевой экран, который блокирует RDP-сессию. Чтобы избежать блокировки, измените действие Сетевого экрана (см. раздел «Изменение действия Сетевого экрана для сетевого пакетного правила» на стр. 100) для сетевого пакетного правила «Сетевая активность для работы удаленного рабочего стола» на **Разрешать**.

Компонент Сетевой экран фильтрует всю сетевую активность в соответствии с сетевыми правилами (см. раздел «О сетевых правилах» на стр. 90). Настройка сетевых правил позволяет вам задать нужный уровень защиты виртуальной машины, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

При работе с Сетевым экраном обратите внимание на следующие особенности:

- Сетевая активность на прикладном уровне по протоколам TCP и UDP не блокируется, если IP-адрес отправителя и адрес получателя совпадают, при условии, что пакет был отправлен через RAW-сокет.
- Сетевой экран не выполняет проверку правил программ и разрешает сетевую активность, если IP-адрес удаленного компьютера имеет значение:
  - для IPv4: 127.0.0.1
  - для IPv6: ::1

  при условии, что пакет был отправлен через RAW-сокет.

- В следующих случаях локальный адрес, с которого / на который выполняется отправка данных, может быть не определен:
  - программа, инициировавшая сетевую активность по протоколам TCP или UDP, не указала локальный IP-адрес;
  - программа инициировала сетевую активность по протоколу ICMP;
  - программа получает входящий пакет по протоколу UDP.
- Сетевой экран не выполняет фильтрацию loopback-трафика на сетевом уровне. Принятие решения по loopback-пакетам происходит на прикладном уровне.
- При фильтрации сетевой активности на прикладном уровне по протоколу ICMP Сетевой экран поддерживает только исходящий запрос ICMP Echo-Request.
- Фильтрация входящих ICMP-пакетов на прикладном уровне не выполняется.
- Для исходящей сетевой активности через RAW-сокет фильтрация по пакетным правилами на прикладном уровне не выполняется.
- Пакеты, отфильтрованные компонентом Защита от сетевых атак, не проверяются Сетевым экраном.
- При наличии на виртуальной машине туннелирующих сетевых интерфейсов фильтрация туннелированного трафика пакетными правилами повторяется для одного и того же пакета по мере продвижения пакета между интерфейсами.

Включение и выключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме. При необходимости вы можете выключить Сетевой экран.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Сетевой экран на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши на строке **Сетевой экран** откройте контекстное меню действий с компонентом Сетевой экран.
5. Выполните одно из следующих действий:
   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить Сетевой экран.

     Значок статуса работы компонента  , отображающийся слева в строке **Сетевой экран**, изменится на значок  .
   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить Сетевой экран.

     Значок статуса работы компонента  , отображающийся слева в строке **Сетевой экран**, изменится на значок  .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Сетевой экран из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

   > Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Сетевой экран**, если вы хотите включить Сетевой экран.
   - Снимите флажок **Включить Сетевой экран**, если вы хотите выключить Сетевой экран.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения

О сетевых правилах

Сетевое правило представляет собой разрешающее или запрещающее действие, которое Сетевой экран совершает, обнаружив попытку сетевого соединения.

Защиту от сетевых атак различного рода Сетевой экран осуществляет на двух уровнях: сетевом и прикладном. Защита на сетевом уровне обеспечивается за счет применения правил для сетевых пакетов. Защита на прикладном уровне обеспечивается за счет применения правил использования сетевых ресурсов программами, установленными на вашей виртуальной машине.

Исходя из двух уровней защиты Сетевого экрана, вы можете сформировать:

- *Сетевые пакетные правила*. Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Сетевой экран задает по умолчанию некоторые сетевые пакетные правила.

- *Сетевые правила программ*. Используются для ограничения сетевой активности конкретной программы. При этом учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета. Такие правила позволяют тонко настраивать фильтрацию сетевой активности, например, когда определенный тип сетевых соединений запрещен для одних программ, но разрешен для других.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Правила контроля сетевой активности программ не учитывают следующие параметры фильтрации, заданные на сетевом уровне:

- идентификатор сетевого адаптера;
- список MAC-адресов локального адаптера;
- список локальных MAC-адресов;
- список удаленных MAC-адресов;
- тип Ethernet-фрейма (IP, IPv6, ARP);
- время жизни (TTL) IP-пакета.

В результате совместного использования правил сетевого и прикладного уровней сетевой трафик может быть заблокирован на прикладном уровне, несмотря на то, что на сетевом уровне он разрешен.

Вы можете установить свой приоритет выполнения для каждого сетевого пакетного правила (см. раздел «Изменение приоритета сетевого пакетного правила» на стр. 101) и сетевого правила программы (см. раздел «Изменение приоритета сетевого правила программы» на стр. 121).

О статусах сетевого соединения

Сетевой экран контролирует все сетевые соединения на вашей виртуальной машине и автоматически присваивает статус каждому из обнаруженных сетевых соединений.

Выделены следующие статусы сетевого соединения:

- **Публичная сеть**. Этот статус разработан для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами (например, для сети интернет-кафе). Пользователю виртуальной машины, подключенной к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этой виртуальной машины. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этой виртуальной машины. Сетевой экран фильтрует сетевую активность каждой программы в соответствии с сетевыми правилами этой программы.

  Сетевой экран по умолчанию присваивает статус *Публичная сеть* сети Интернет. Вы не можете изменить статус сети Интернет.

- **Локальная сеть**. Этот статус разработан для сетей, пользователям которых вы доверяете доступ к файлам и принтерам вашей виртуальной машины (например, для локальной сети организации или для домашней сети).

- **Доверенная сеть**. Этот статус разработан для безопасной сети, во время работы в которой виртуальная машина не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Изменение статуса сетевого соединения

► *Чтобы изменить статус сетевого соединения, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Доступные сети**.

   Откроется окно **Сетевой экран**.
4. Выберите закладку **Сети**.
5. Выберите сетевое соединение, статус которого вы хотите изменить.
6. По правой клавише мыши откройте контекстное меню сетевого соединения.
7. В контекстном меню выберите статус сетевого соединения (см. раздел «О статусах сетевого соединения» на стр. 92):
   - **Публичная сеть**.
   - **Локальная сеть**.
   - **Доверенная сеть**.
8. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с сетевыми пакетными правилами

Вы можете выполнить следующие действия в процессе работы с сетевыми пакетными правилами:

- Создать новое сетевое пакетное правило.

  Вы можете создать новое сетевое пакетное правило, сформировав набор условий и действий над сетевыми пакетами и потоками данных.

- Включить и выключить сетевое пакетное правило.

  Все сетевые пакетные правила, созданные Сетевым экраном по умолчанию, имеют статус *Включено*. Если сетевое пакетное правило включено, Сетевой экран применяет это правило.

  Вы можете выключить любое сетевое пакетное правило, выбранное в списке сетевых пакетных правил. Если сетевое пакетное правило выключено, Сетевой экран временно не применяет это правило.

  > Новое сетевое пакетное правило, созданное пользователем, по умолчанию добавляется в список сетевых пакетных правил со статусом *Включено*.

- Изменить параметры существующего сетевого пакетного правила.

  После того как вы создали новое сетевое пакетное правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого пакетного правила.

  В списке сетевых пакетных правил вы можете изменить действие, которое Сетевой экран выполняет, обнаружив сетевую активность указанного сетевого пакетного правила.

- Изменить приоритет сетевого пакетного правила.

  Вы можете повысить или понизить приоритет выбранного в списке сетевого пакетного правила.

- Удалить сетевое пакетное правило.

  Вы можете удалить сетевое пакетное правило, если вы не хотите, чтобы Сетевой экран применял это правило при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых пакетных правил со статусом *Выключено*.

В этом разделе

Создание и изменение сетевого пакетного правила

Создавая сетевые пакетные правила, нужно помнить, что они имеют приоритет над сетевыми правилами программ.

► *Чтобы создать или изменить сетевое пакетное правило, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

На этой закладке представлен список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.

4. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое пакетное правило, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое пакетное правило, выберите его в списке сетевых пакетных правил и нажмите на кнопку **Изменить**.

5. Откроется окно **Сетевое правило**.

6. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.
   - **Запрещать**.
   - **По правилам программы**.

7. В поле **Название** укажите имя сетевого сервиса одним из следующих способов:

   - Нажмите на значок  , расположенный справа от поля **Название**, и выберите имя сетевого сервиса в раскрывающемся списке.

     В состав Kaspersky Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.

   - В поле **Название** введите имя сетевого сервиса вручную.

     > *Сетевой сервис* – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.

8. Укажите протокол передачи данных:

   a. Установите флажок **Протокол**.

b. В раскрывающемся списке выберите тип протокола, по которому Сетевой экран должен контролировать сетевую активность.

   Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE.

   По умолчанию флажок **Протокол** снят.

   Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.

9. В раскрывающемся списке **Направление** выберите направление контролируемой сетевой активности.

   Сетевой экран контролирует сетевые соединения со следующими направлениями:

   - **Входящее (пакет)**.
   - **Входящее**.
   - **Входящее / Исходящее**.
   - **Исходящее (пакет)**.
   - **Исходящее**.

10. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

    a. Установите флажок **ICMP-тип** и в раскрывающемся списке выберите тип ICMP-пакета.

    b. Установите флажок **ICMP-код** и в раскрывающемся списке выберите код ICMP-пакета.

11. Если в качестве протокола выбран протокол TCP или UDP, вы можете задать порты вашей виртуальной машины и удаленного компьютера, соединение между которыми контролируется:

    a. В поле **Удаленные порты** введите порты удаленного компьютера.

    b. В поле **Локальные порты** введите порты вашей виртуальной машины.

12. В таблице **Сетевые адаптеры** укажите параметры сетевых адаптеров, с которых могут быть отправлены или которыми могут быть приняты сетевые пакеты. Для этого воспользуйтесь кнопками **Добавить**, **Изменить** и **Удалить**.

13. В поле **Максимальное значение времени жизни пакета** укажите диапазон значений времени жизни передаваемых и / или получаемых сетевых пакетов. Сетевое правило контролирует передачу сетевых пакетов, значение времени жизни которых входит в диапазон от единицы до указанного значения.

14. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Удаленные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

    - **Адреса подсети**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: **Доверенные сети**, **Локальные сети**, **Публичные сети**.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

15. Укажите сетевые адреса виртуальных машин с установленной программой Kaspersky Security, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Локальные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и любым IP-адресом.

- **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

> Для приложений не всегда возможно получить локальный адрес. В этом случае параметр правила **Локальные адреса** игнорируется.

16. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого пакетного правила было отражено в отчете.

17. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое пакетное правило, оно отобразится на закладке **Сетевые пакетные правила** окна **Сетевой экран**. По умолчанию новое сетевое правило помещается в конец списка сетевых пакетных правил.

18. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

19. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение сетевого пакетного правила

► *Чтобы включить или выключить сетевое пакетное правило, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

4. В списке сетевых пакетных правил выберите нужное вам сетевое пакетное правило.

5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого пакетного правила, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого пакетного правила, если вы хотите выключить правило.

6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия Сетевого экрана для сетевого пакетного правила

► *Чтобы изменить действие Сетевого экрана для сетевого пакетного правила, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

4. В списке сетевых пакетных правил выберите сетевое пакетное правило, для которого вы хотите изменить действие.
5. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Разрешать**.
   - **Запрещать**.
   - **По правилу программы**.
   - **Записывать в отчет**.

6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения

Изменение приоритета сетевого пакетного правила

Приоритет выполнения сетевого пакетного правила определяется его положением в списке сетевых пакетных правил. Первое сетевое пакетное правило в списке сетевых пакетных правил обладает самым высоким приоритетом.

Каждое сетевое пакетное правило, которое вы создали вручную, добавляется в конец списка сетевых пакетных правил и имеет самый низкий приоритет.

Сетевой экран выполняет правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Согласно каждому обрабатываемому сетевому пакетному правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

► *Чтобы изменить приоритет сетевого пакетного правила, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.
4. В списке сетевых пакетных правил выберите сетевое пакетное правило, приоритет которого вы хотите изменить.
5. С помощью кнопок **Вверх** и **Вниз** переместите сетевое пакетное правило на нужную позицию в списке сетевых пакетных правил.
6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с сетевыми правилами группы программ

Программа Kaspersky Security по умолчанию группирует все программы, установленные в операционной системе защищенной виртуальной машины, по названию производителей программного обеспечения, файловую и сетевую активность которого контролирует. Группы программ, в свою очередь, сгруппированы в *группы доверия*. Все программы и группы программ наследуют свойства своей родительской группы: правила контроля программ, сетевые правила программы, а также приоритет их выполнения.

Как и компонент Контроль активности программ (см. раздел «О Контроле активности программ» на стр. 154), компонент Сетевой экран по умолчанию применяет сетевые правила группы программ для фильтрации сетевой активности всех помещенных в группу программ. Сетевые правила группы программ определяют, какими правами доступа к различным сетевым соединениям обладают программы, входящие в эту группу.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые программа Kaspersky Security обнаружила на виртуальной машине. Вы можете изменить действие Сетевого экрана для сетевых правил группы программ, созданных по умолчанию. Вы не можете изменить, удалить или выключить сетевые правила группы программ, созданные по умолчанию, а также изменить их приоритет.

Вы можете выполнить следующие действия в процессе работы с сетевыми правилами группы программ:

- Создать новое сетевое правило группы программ.

  Вы можете создать новое сетевое правило группы программ, в соответствии с которым Сетевой экран должен регулировать сетевую активность программ, входящих в выбранную группу программ.

- Включить и выключить сетевое правило группы программ.

  Все сетевые правила группы программ добавляются в список сетевых правил группы программ со статусом *Включено*. Если сетевое правило группы программ включено, Сетевой экран применяет это правило.

Вы можете выключить сетевое правило группы программ, созданное вручную. Если сетевое правило группы программ выключено, Сетевой экран временно не применяет это правило.

- Изменить параметры сетевого правила группы программ.

  После того как вы создали новое сетевое правило группы программ, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого правила группы программ.

  В списке сетевых правил группы программ вы можете изменить действие для сетевого правила группы программ, которое Сетевой экран выполняет, обнаружив сетевую активность этой группы программ.

- Изменить приоритет сетевого правила группы программ.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила группы программ.

- Удалить сетевое правило группы программ.

  Вы можете удалить созданное вручную сетевое правило группы программ, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной группе программ при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых правил группы программ.

В этом разделе

Создание и изменение сетевого правила группы программ

► *Чтобы создать или изменить сетевое правило группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите группу программ, для которой вы хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. Выберите закладку **Сетевые правила**.
7. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое правило группы программ, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое правило группы программ, выберите его в списке сетевых правил и нажмите на кнопку **Изменить**.
8. Откроется окно **Сетевое правило**.
9. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.
   - **Запрещать**.

10. В поле **Название** укажите имя сетевого сервиса одним из следующих способов:

    - Нажмите на значок  , расположенный справа от поля **Название**, и выберите имя сетевого сервиса в раскрывающемся списке.

      В состав Kaspersky Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.

    - В поле **Название** введите имя сетевого сервиса вручную.

      > *Сетевой сервис* – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.

11. Укажите протокол передачи данных:

    a. Установите флажок **Протокол**.

    b. В раскрывающемся списке выберите тип протокола, по которому Сетевой экран должен контролировать сетевую активность.

       Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE.

       По умолчанию флажок **Протокол** снят.

       Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.

12. В раскрывающемся списке **Направление** выберите направление контролируемой сетевой активности.

    Сетевой экран контролирует сетевые соединения со следующими направлениями:

    - **Входящее**.
    - **Входящее / Исходящее**.
    - **Исходящее**.

13. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

    a. Установите флажок **ICMP-тип** и в раскрывающемся списке выберите тип ICMP-пакета.

    b. Установите флажок **ICMP-код** и в раскрывающемся списке выберите код ICMP-пакета.

14. Если в качестве протокола выбран протокол TCP или UDP, вы можете задать порты вашей виртуальной машины и удаленного компьютера, соединение между которыми следует контролировать:

    a. В поле **Удаленные порты** введите порты удаленного компьютера.

    b. В поле **Локальные порты** введите порты вашей виртуальной машины.

15. В поле **Максимальное значение времени жизни пакета** укажите диапазон значений времени жизни передаваемых и / или получаемых сетевых пакетов. Сетевое правило контролирует передачу сетевых пакетов, значение времени жизни которых входит в диапазон от единицы до указанного значения.

16. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Удаленные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

    - **Адреса подсети**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: **Доверенные сети**, **Локальные сети**, **Публичные сети**.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

17. Укажите сетевые адреса виртуальных машин с установленной программой Kaspersky Security, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Локальные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и любым IP-адресом.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

    > Для приложений не всегда возможно получить локальный адрес. В этом случае параметр правила **Локальные адреса** игнорируется.

18. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого правила группы программ было отражено в отчете.

19. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое правило группы программ, оно отобразится на закладке **Сетевые правила** окна **Правила контроля группы программ**.

20. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.

21. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

22. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение сетевого правила группы программ

► *Чтобы включить или выключить сетевое правило группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную группу программ.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил группы программ выберите нужное вам сетевое правило группы программ.
8. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого правила группы программ, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого правила группы программ, если вы хотите выключить правило.

     Вы не можете выключить сетевое правило группы программ, если оно создано Сетевым экраном по умолчанию.

9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия Сетевого экрана для сетевого правила группы программ

Вы можете изменить действие Сетевого экрана для сетевых правил всей группы программ, которые были созданы по умолчанию, а также изменить действие Сетевого экрана для одного сетевого правила группы программ, которое было создано вручную.

► *Чтобы изменить действие Сетевого экрана для сетевых правил всей группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке программ выберите группу программ, если вы хотите изменить действие Сетевого экрана для всех сетевых правил группы программ, созданных по умолчанию. Сетевые правила группы программ, созданные вручную, останутся без изменений.

5. В графе **Сеть** по левой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

► *Чтобы изменить действие Сетевого экрана для одного сетевого правила группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную группу программ.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил группы программ выберите сетевое правило группы программ, для которого вы хотите изменить действие Сетевого экрана.
8. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.
9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.
10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение приоритета сетевого правила группы программ

Приоритет выполнения сетевого правила группы программ определяется его положением в списке сетевых правил. Сетевой экран выполняет правила в порядке их расположения в списке сетевых правил, сверху вниз. Согласно каждому обрабатываемому сетевому правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Созданные вручную сетевые правила группы программ имеют более высокий приоритет, чем сетевые правила группы программ, созданные по умолчанию.

Вы не можете изменить приоритет сетевых правил группы программ, созданных по умолчанию.

► *Чтобы изменить приоритет сетевого правила группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную группу программ.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил группы программ выберите сетевое правило группы программ, приоритет которого вы хотите изменить.

8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило группы программ на нужную позицию в списке сетевых правил группы программ.

9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с сетевыми правилами программы

В соответствии с сетевыми правилами программы Сетевой экран регулирует доступ этой программы к различным сетевым соединениям.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые программа Kaspersky Security обнаружила на виртуальной машине. Программы, входящие в эту группу программ, наследуют эти сетевые правила. Вы можете изменить действия Сетевого экрана для унаследованных сетевых правил программы. Вы не можете изменить, удалить или выключить сетевые правила программ, унаследованные от родительской группы программ, а также изменить их приоритет.

Вы можете выполнить следующие действия в процессе работы с сетевыми правилами программы:

- Создать новое сетевое правило программы.

  Вы можете создать новое сетевое правило программы, в соответствии с которым Сетевой экран должен регулировать сетевую активность этой программы.

- Включить и выключить сетевое правило программы.

  Все сетевые правила программы добавляются в список сетевых правил программы со статусом *Включено*. Если правило программы включено, Сетевой экран применяет это правило.

  Вы можете выключить любое сетевое правило программы, созданное вручную. Если правило программы выключено, Сетевой экран временно не применяет это правило.

- Изменить параметры сетевого правила программы.

  После того как вы создали новое сетевое правило программы, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого правила программы.

  В списке правил программы вы можете изменить действие для сетевого правила программы, которое Сетевой экран выполняет, обнаружив сетевую активность этой программы.

- Изменить приоритет сетевого правила программы.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила программы.

- Удалить сетевое правило программы.

  Вы можете удалить созданное вручную сетевое правило программы, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной программе при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых правил программы.

В этом разделе

Создание и изменение сетевого правила программы

► *Чтобы создать или изменить сетевое правило программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите программу, для которой вы хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Сетевые правила**.
7. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое правило программы, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое правило программы, выберите его в списке сетевых правил программы и нажмите на кнопку **Изменить**.
8. Откроется окно **Сетевое правило**.
9. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.
   - **Запрещать**.

10. В поле **Название** укажите имя сетевого сервиса одним из следующих способов:

    - Нажмите на значок  , расположенный справа от поля **Название**, и выберите имя сетевого сервиса в раскрывающемся списке.

      В состав Kaspersky Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.

    - В поле **Название** введите имя сетевого сервиса вручную.

      > *Сетевой сервис* – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.

11. Укажите протокол передачи данных:

    a. Установите флажок **Протокол**.

    b. В раскрывающемся списке выберите тип протокола, по которому Сетевой экран должен контролировать сетевую активность.

       Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE.

       По умолчанию флажок **Протокол** снят.

       Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.

12. В раскрывающемся списке **Направление** выберите направление контролируемой сетевой активности.

    Сетевой экран контролирует сетевые соединения со следующими направлениями:

    - **Входящее**.
    - **Входящее / Исходящее**.
    - **Исходящее**.

13. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

    a. Установите флажок **ICMP-тип** и в раскрывающемся списке выберите тип ICMP-пакета.

    b. Установите флажок **ICMP-код** и в раскрывающемся списке выберите код ICMP-пакета.

14. Если в качестве протокола выбран протокол TCP или UDP, вы можете задать порты виртуальной машины и удаленного компьютера, соединение между которыми будет контролироваться:

    a. В поле **Удаленные порты** введите порты удаленного компьютера.

    b. В поле **Локальные порты** введите порты виртуальной машины.

15. В поле **Максимальное значение времени жизни пакета** укажите диапазон значений времени жизни передаваемых и / или получаемых сетевых пакетов. Сетевое правило контролирует передачу сетевых пакетов, значение времени жизни которых входит в диапазон от единицы до указанного значения.

16. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Удаленные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

    - **Адреса подсети**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: **Доверенные сети**, **Локальные сети**, **Публичные сети**.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

17. Укажите сетевые адреса виртуальных машин с установленной программой Kaspersky Security, которые могут передавать и / или получать сетевые пакеты.
    Для этого в раскрывающемся списке **Локальные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и любым IP-адресом.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов виртуальными машинами с установленной программой Kaspersky Security и с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

    > Для приложений не всегда возможно получить локальный адрес. В этом случае параметр правила **Локальные адреса** игнорируется.

18. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого правила программы было отражено в отчете.

19. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое правило программы, оно отобразится на закладке **Сетевые правила** окна **Правила программы**.

20. Нажмите на кнопку **ОК** в окне **Правила контроля программы**.

21. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

22. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение сетевого правила программы

► *Чтобы включить или выключить сетевое правило программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил программы выберите нужное вам сетевое правило программы.
8. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого правила программы, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого правила программы, если вы хотите выключить правило.

   > Вы не можете выключить сетевое правило программы, если оно создано Сетевым экраном по умолчанию.
9. Нажмите на кнопку **ОК** в окне **Правила контроля программы**.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия Сетевого экрана для сетевого правила программы

Вы можете изменить действие Сетевого экрана для всех сетевых правил программы, которые были созданы по умолчанию, а также вы можете изменить действие Сетевого экрана для одного сетевого правила программы, которое было создано вручную.

► *Чтобы изменить действие Сетевого экрана для всех сетевых правил программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке программ выберите программу, если хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию.

   Сетевые правила программы, созданные вручную, останутся без изменений.

5. В графе **Сеть** по левой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.

6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

► *Чтобы изменить действие Сетевого экрана для одного сетевого правила программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонентов Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил программы выберите сетевое правило программы, для которого вы хотите изменить действие Сетевого экрана.
8. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.
9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.
10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение приоритета сетевого правила программы

Приоритет выполнения сетевого правила программы определяется его положением в списке сетевых правил. Сетевой экран выполняет правила в порядке их расположения в списке сетевых правил, сверху вниз. Согласно каждому обрабатываемому сетевому правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Сетевые правила программы (как унаследованные, так и созданные вручную) имеют более высокий приоритет, чем сетевые правила, унаследованные от родительской группы программ. То есть в группе все программы автоматически наследуют сетевые правила этой группы, но если для отдельной программы изменить какое-либо правило или создать новое, то оно обрабатывается прежде, чем все унаследованные.

Вы не можете изменить приоритет унаследованных сетевых правил программы.

► *Чтобы изменить приоритет сетевого правила программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.

6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил программы выберите сетевое правило программы, приоритет которого вы хотите изменить.
8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило программы на нужную позицию в списке сетевых правил программы.
9. Нажмите на кнопку **ОК** в окне **Правила контроля программы**.
10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита от сетевых атак

Этот раздел содержит информацию о Защите от сетевых атак и инструкции о том, как настроить параметры компонента.

В этом разделе

О Защите от сетевых атак

Компонент Защита от сетевых атак отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на защищенную виртуальную машину, Kaspersky Security блокирует сетевую активность атакующего компьютера. После этого на экран выводится уведомление о том, что была попытка сетевой атаки с указанием информации об атакующем компьютере.

Сетевая активность атакующего компьютера блокируется на один час. Вы можете изменить параметры блокирования атакующего компьютера (см. раздел «Изменение параметров блокирования атакующего компьютера» на стр. 125).

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними приведены в базах Kaspersky Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых атак, пополняется в процессе обновления баз программы (см. раздел «Об обновлении баз и модулей программы» на стр. 237).

Включение и выключение Защиты от сетевых атак

По умолчанию компонент Защита от сетевых атак включен и работает в оптимальном режиме. При необходимости вы можете выключить Защиту от сетевых атак.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Защиту от сетевых атак на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши на строке **Защита от сетевых атак** откройте контекстное меню действий с компонентом Защита от сетевых атак.

5. Выполните одно из следующих действий:

   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить Защиту от сетевых атак.

     Значок статуса работы компонента  , отображающийся слева в строке **Защита от сетевых атак**, изменится на значок  .

   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить Защиту от сетевых атак.

     Значок статуса работы компонента  , отображающийся слева в строке **Защита от сетевых атак**, изменится на значок  .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Защиту от сетевых атак из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Защита от сетевых атак**.

   В правой части окна отобразятся параметры компонента Защита от сетевых атак.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните следующие действия:

   - Установите флажок **Включить Защиту от сетевых атак**, если вы хотите включить Защиту от сетевых атак.
   - Снимите флажок **Включить Защиту от сетевых атак**, если вы хотите выключить Защиту от сетевых атак.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение параметров блокирования атакующего компьютера

► *Чтобы изменить параметры блокирования атакующего компьютера, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите раздел **Защита от сетевых атак**.

   В правой части окна отобразятся параметры компонента Защита от сетевых атак.

3. Установите флажок **Добавить атакующий компьютер в список блокирования на N минут**.

   Если этот флажок установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых атак блокирует сетевую активность атакующего компьютера в течение заданного времени, чтобы автоматически защитить виртуальную машину от возможных будущих сетевых атак с этого адреса.

   Если этот флажок не установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых атак не включает автоматическую защиту от возможных будущих сетевых атак с этого адреса.

4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Добавить атакующий компьютер в список блокирования на N минут**.

   По умолчанию сетевая активность атакующего компьютера блокируется на один час.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль сетевого трафика

Этот раздел содержит информацию о контроле сетевого трафика и инструкции о том, как настроить параметры контролируемых сетевых портов.

В этом разделе

О контроле сетевого трафика

Во время работы Kaspersky Security компоненты Почтовый Антивирус (см. раздел «О Почтовом Антивирусе» на стр. 54), Веб-Антивирус (см. раздел «О Веб-Антивирусе» на стр. 68) и IM-Антивирус (см. раздел «Об IM-Антивирусе» на стр. 80) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты защищенной виртуальной машины. Так, например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, а Веб-Антивирус анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Security подразделяет TCP- и UDP-порты операционной системы на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для служб, которые могут быть уязвимыми, следует контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список программ, запрашивающих сетевой доступ, на которые компоненты Почтовый Антивирус, Веб-Антивирус и IM-Антивирус должны обращать особое внимание во время слежения за сетевым трафиком.

Настройка параметров контроля сетевого трафика

Вы можете выполнить следующие действия для настройки параметров контроля сетевого трафика:

- Включить контроль всех сетевых портов.
- Сформировать список контролируемых сетевых портов.
- Сформировать список программ, для которых контролируются все сетевые порты.

В этом разделе

Включение контроля всех сетевых портов

► *Чтобы включить контроль всех сетевых портов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка контролируемых сетевых портов

► *Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.

4. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**. Окно **Сетевые порты** содержит список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Security.

5. В списке сетевых портов выполните следующие действия:

   - Установите флажки напротив названий тех сетевых портов, которые вы хотите включить в список контролируемых сетевых портов.

     По умолчанию флажки установлены для всех сетевых портов, представленных в окне **Сетевые порты**.

   - Снимите флажки напротив названий тех сетевых портов, которые вы хотите исключить из списка контролируемых сетевых портов.

6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:

   a. По ссылке **Добавить**, расположенной под списком сетевых портов, откройте окно **Сетевой порт**.

   b. В поле **Порт** введите номер сетевого порта.

c. В поле **Описание** введите название сетевого порта.

d. Нажмите кнопку **ОК**.

Окно **Сетевой порт** закроется. Добавленный вами сетевой порт отобразится в конце списка сетевых портов.

7. Нажмите на кнопку **ОК** в окне **Сетевые порты**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Во время работы протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, нужно включить контроль для всех сетевых портов (см. раздел «Включение контроля всех сетевых портов» на стр. 127) или настроить контроль всех сетевых портов для программ (см. раздел «Формирование списка программ, для которых контролируются все сетевые порты» на стр. 129), с помощью которых устанавливается FTP-соединение.

Формирование списка программ, для которых контролируются все сетевые порты

Вы можете сформировать список программ, для которых Kaspersky Security контролирует все сетевые порты.

В список программ, для которых Kaspersky Security контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

► *Чтобы сформировать список программ, для которых контролируются все сетевые порты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна выберите раздел **Антивирусная защита**.

В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.

4. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**.

5. Установите флажок **Контролировать все порты для указанных программ**.

6. В списке программ, расположенном под флажком **Контролировать все порты для указанных программ**, выполните следующие действия:

   - Установите флажки напротив названий программ, для которых нужно контролировать все сетевые порты.

     По умолчанию флажки установлены для всех программ, представленных в окне **Сетевые порты**.

   - Снимите флажки напротив названий программ, для которых не нужно контролировать все сетевые порты.

7. Если программа отсутствует в списке программ, добавьте ее следующим образом:

   a. По ссылке **Добавить**, расположенной под списком программ, откройте контекстное меню.

   b. Выберите в контекстном меню способ добавления программы в список программ:

      - Выберите пункт **Программы**, если вы хотите выбрать программу из списка программ, установленных на защищенной виртуальной машине. Откроется окно **Выбор программы**, с помощью которого вы можете указать название программы.

      - Выберите пункт **Обзор**, если вы хотите указать местонахождение исполняемого файла программы. Откроется стандартное окно Microsoft Windows **Открыть**, с помощью которого вы можете указать название исполняемого файла программы.

   c. После выбора программы откроется окно **Программа**.

d. В поле **Название** введите название для выбранной программы.

e. Нажмите кнопку **ОК**.

Окно **Программа** закроется. Добавленная вами программа отобразится в конце списка программ.

8. Нажмите на кнопку **ОК** в окне **Сетевые порты**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Мониторинг сети

Этот раздел содержит информацию о мониторинге сети и инструкцию о том, как его запустить.

В этом разделе

О мониторинге сети

Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности вашей виртуальной машины в реальном времени.

Запуск мониторинга сети

► *Чтобы запустить мониторинг сети, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. Выберите закладку **Центр управления**.

3. Раскройте блок **Управление защитой**.

4. По правой клавише мыши на строке **Сетевой экран** откройте контекстное меню действий с компонентом Сетевой экран.

5. В контекстном меню выберите пункт **Мониторинг сети**.

   Откроется окно **Мониторинг сети**. В этом окне информация о сетевой активности защищенной виртуальной машины представлена на четырех закладках:

   - На закладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения вашей защищенной виртуальной машины. Приводятся как сетевые соединения, инициированные защищенной виртуальной машиной, так и входящие сетевые соединения.

   - На закладке **Открытые порты** перечислены все открытые сетевые порты на защищенной виртуальной машине.

   - На закладке **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между защищенной виртуальной машиной и другими компьютерами сети, в которой вы работаете в текущий момент.

   - На закладке **Заблокированные компьютеры** представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых атак заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Мониторинг системы

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows.

Этот раздел содержит информацию о Мониторинге системы и инструкции о том, как настроить параметры компонента.

В этом разделе

О Мониторинге системы

Мониторинг системы собирает данные о действиях программ на вашей виртуальной машине и предоставляет эту информацию другим компонентам для более эффективной защиты.

Шаблоны опасного поведения программ

Шаблоны опасного поведения программ BSS (Behavior Stream Signatures) (далее также «шаблоны опасного поведения» и «шаблоны опасного поведения программ») содержат последовательности действий программ, которые Kaspersky Security классифицирует как опасные. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Security выполняет заданное действие. Функциональность Kaspersky Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту виртуальной машины.

Откат действий, произведенных вредоносными программами

На основе информации, собранной Мониторингом системы, Kaspersky Security при лечении вредоносных программ может выполнять откат действий, произведенных вредоносными программами в операционной системе.

Откат действий вредоносной программы может быть инициирован проактивной защитой, Файловым Антивирусом (см. раздел «Защита файловой системы виртуальной машины. Файловый Антивирус» на стр. 38) и программой Kaspersky Security при антивирусной проверке.

Откат действий вредоносной программы не оказывает негативного влияния на работу операционной системы и целостность информации на вашей виртуальной машине.

Включение и выключение Мониторинга системы

По умолчанию Мониторинг системы включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Мониторинг системы при необходимости.

Не рекомендуется выключать Мониторинг системы без необходимости, так как это снижает эффективность работы компонентов защиты, которые могут запрашивать данные, собранные Мониторингом системы, для уточнения обнаруженной угрозы.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Мониторинг системы на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление защитой**.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Мониторинг системы.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Мониторинг системы.

     Значок статуса работы компонента , отображающийся слева в строке **Мониторинг системы**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Мониторинг системы.

     Значок статуса работы компонента , отображающийся слева в строке **Мониторинг системы**, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Мониторинг системы из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Мониторинг системы**, если вы хотите включить Мониторинг системы.
   - Снимите флажок **Включить Мониторинг системы**, если вы хотите выключить Мониторинг системы.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование шаблонов опасного поведения программ

► *Чтобы использовать шаблоны опасного поведения программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

3. В блоке **Проактивная защита** установите флажок **Использовать обновляемые шаблоны опасного поведения (BSS)**.
4. В раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:

   - **Выбирать действие автоматически**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Security выполняет действие, установленное специалистами «Лаборатории Касперского» по умолчанию.

- **Завершать работу вредоносной программы**. Если выбран этот элемент, то обнаружив вредоносную активность программы, Kaspersky Security завершает работу этой программы.

- **Пропускать**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Security не выполняет действий над исполняемым файлом этой программы.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Откат действий вредоносных программ при лечении

► *Чтобы включить или выключить откат действий вредоносных программ при лечении, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

3. Выполните одно из следующих действий:

   - Установите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы при лечении вредоносных программ программа Kaspersky Security выполняла откат действий, которые эти программы совершили в операционной системе.

   - Снимите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы при лечении вредоносных программ программа Kaspersky Security не выполняла откат действий, которые эти программы совершили в операционной системе.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль запуска программ

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows и во время установки выбрали тип «Установка компонентов защиты и контроля».

Этот раздел содержит информацию о Контроле запуска программ и инструкции о том, как настроить параметры компонента.

В этом разделе

О Контроле запуска программ

Компонент Контроль запуска программ отслеживает попытки запуска программ на виртуальной машине и регулирует запуск программ с помощью *правил контроля запуска программ* (см. раздел «*О правилах контроля запуска программ*» на стр. 141).

Запуск программ, параметры которых не удовлетворяют ни одному из правил контроля запуска программ, регулируются созданным по умолчанию правилом «Разрешить все». Правило «Разрешить все» разрешает любым пользователям запускать любые программы.

Все попытки запуска программ на виртуальной машине фиксируются в отчетах.

Включение и выключение Контроля запуска программ

По умолчанию Контроль запуска программ включен, вы можете выключить Контроль запуска программ при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Контроль запуска программ на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль запуска программ.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль запуска программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль запуска программ**, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль запуска программ.

     Значок статуса работы компонента , отображающийся слева в строке **Контроль запуска программ**, изменится на значок .

Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Контроль запуска программ из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел Контроль запуска программ.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.
3. В блоке **Контроль программ** выполните одно из следующих действий:
   - Установите флажок **Включить Контроль запуска программ**, если вы хотите включить Контроль запуска программ.
   - Снимите флажок **Включить Контроль запуска программ**, если вы хотите выключить Контроль запуска программ.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О правилах контроля запуска программ

Правило контроля запуска программ представляет собой набор параметров, которые определяют следующие функции компонента Контроль запуска программ:

- Классификация программ с помощью *условий срабатывания правила* (далее также «условий»). Условие срабатывания правила представляет собой соответствие: критерий условия – значение условия – тип условия.

  Критерием условия срабатывания правила может быть:

  - Путь к папке с исполняемым файлом программы или путь к исполняемому файлу программы.
  - Метаданные: исходное название исполняемого файла программы, название исполняемого файла программы на диске, версия исполняемого файла программы, название программы, производитель программы.
  - MD5-хеш исполняемого файла программы.
  - Принадлежность программы к KL-категории. KL-категория – это сформированный специалистами «Лаборатории Касперского» список программ, обладающих общими тематическими признаками.

    Например, KL-категория «Офисные программы» включает в себя программы из пакета Microsoft Office, Adobe® Acrobat® и другие.

  Тип условия срабатывания правила определяет порядок отнесения программы к правилу:

  - *Включающие условия*. Программа удовлетворяет правилу, если ее параметры удовлетворяют хотя бы одному включающему условию срабатывания правила.
  - *Исключающие условия*. Программа не удовлетворяет правилу, если ее параметры удовлетворяют хотя бы одному исключающему условию срабатывания правила или не удовлетворяют ни одному включающему условию срабатывания правила. Правило не контролирует запуск таких программ.

- Разрешение запускать программы выбранным пользователям и / или группам пользователей.

  Вы можете выбрать пользователя и / или группу пользователей, которым разрешен запуск программ, удовлетворяющих правилу.

  Правило, в котором не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, называется *запрещающим*.

- Запрещение запускать программы выбранным пользователям и / или группам пользователей.

  Вы можете выбрать пользователя и / или группу пользователей, которым запрещен запуск программ, удовлетворяющих правилу контроля запуска программ.

  Правило, в котором не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, называется *разрешающим*.

  > Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей определено разрешающее правило контроля запуска программы, и для одного из пользователей этой группы определено запрещающее правило контроля запуска программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила контроля запуска программ

Правила контроля запуска программ могут иметь три статуса работы:

- *Вкл.* Статус работы правила означает, что правило включено.
- *Выкл*. Статус работы правила означает, что правило выключено.
- *Тест*. Статус работы правила означает, что Kaspersky Security не ограничивает запуск программ в соответствии с параметрами правила, а лишь фиксирует в отчетах информацию о запуске программ.

  Статус работы правила *Тест* удобно использовать для проверки работы сформированного правила контроля запуска программ. Пользователь не ограничен в запуске программ, удовлетворяющих правилу со статусом работы *Тест*. Разрешение или запрет на запуск программы формируются отдельно для тестовых и не тестовых правил.

Правила контроля запуска программ по умолчанию

По умолчанию созданы следующие правила контроля запуска программ:

- **Разрешить все**. Правило разрешает запуск всех программ всем пользователям. На этом правиле основана работа Контроля запуска программ в режиме «Черный список» (см. раздел «О режимах работы Контроля запуска программ» на стр. 144). По умолчанию правило включено.

- **Доверенные программы обновления**. Правило разрешает запуск программ, которые установлены или обновлены программами из KL-категории «Доверенные программы обновления», и для которых не определены запрещающие правила. В KL-категорию «Доверенные программы обновления» включены программы обновления наиболее известных производителей программного обеспечения. Правило создано по умолчанию только в плагине управления Kaspersky Security. По умолчанию правило выключено.

- **Операционная система и ее компоненты**. Правило разрешает всем пользователям запускать программы, принадлежащие к KL-категории «Золотая категория». В KL-категорию «Золотая категория» включены программы, необходимые для запуска и работы операционной системы. Разрешение запускать программы из этой KL-категории требуется для работы Контроля запуска программ в режиме «Белый список» (см. раздел «О режимах работы Контроля запуска программ» на стр. 144). Правило создано по умолчанию только в плагине управления Kaspersky Security. По умолчанию правило выключено.

О режимах работы Контроля запуска программ

Компонент Контроль запуска программ может работать в двух режимах:

- **Черный список**. Режим, при котором Контроль запуска программ разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в запрещающих правилах контроля запуска программ (см. раздел «О правилах контроля запуска программ» на стр. 141).

  Этот режим работы Контроля запуска программ настроен по умолчанию. Разрешение на запуск всех программ основано на правиле контроля запуска программ «Разрешено все», созданном по умолчанию.

- **Белый список**. Режим, при котором Контроль запуска программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в разрешающих правилах контроля запуска программ. Таким образом, если разрешающие правила контроля запуска программ сформированы максимально полно, Контроль запуска программ запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Настройка Контроля запуска программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Security, так и через Kaspersky Security Center. Так как Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Security, настройку режима работы компонента Контроль запуска программ рекомендуется выполнять через Kaspersky Security Center (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

Действия с правилами контроля запуска программ

Вы можете выполнить следующие действия с правилами контроля запуска программ:

- Добавить новое правило.
- Изменить правило.
- Изменить статус работы правила.

  Правило контроля запуска программ может быть включено (статус работы *Вкл*), выключено (статус работы *Выкл*) или работать в тестовом режиме (статус работы *Тест*). По умолчанию после создания правило контроля запуска программ включено (имеет статус работы *Вкл)*. Вы можете выключить правило контроля запуска программ или включить работу правила в тестовом режиме.

- Удалить правило.

В этом разделе

Добавление и изменение правила контроля запуска программ

► *Чтобы добавить или изменить правило контроля запуска программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Выполните одно из следующих действий:

   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило контроля запуска программ**.

4. Задайте или измените параметры правила. Для этого выполните следующие действия:

   a. В поле **Название** введите или измените название правила.

   b. В таблице **Включающие условия** сформируйте или измените список включающих условий срабатывания правила контроля запуска программ (см. раздел «Добавление условия срабатывания правила контроля запуска программ» на стр. 147). Для этого воспользуйтесь кнопками **Добавить**, **Изменить**, **Удалить**, **Сделать исключением**.

   c. В таблице **Исключающие условия** сформируйте или измените список исключающих условий срабатывания правила контроля запуска программ. Для этого воспользуйтесь кнопками **Добавить**, **Изменить**, **Удалить**, **Сделать вкл. условием**.

   d. Вы можете изменить тип условия срабатывания правила. Для этого выполните следующие действия:

      - Чтобы изменить тип условия с включающего на исключающее, выберите условие в таблице **Включающие условия** и нажмите на кнопку **Сделать исключением**.
      - Чтобы изменить тип условия с исключающего на включающее, выберите условие в таблице **Исключающие условия** и нажмите на кнопку **Сделать вкл. условием**.

   e. Задайте или измените список пользователей и / или групп пользователей, которым разрешено запускать программы, удовлетворяющие включающим условиям срабатывания правила. Для этого в поле **Пользователи и / или группы, получающие разрешение** введите имена пользователей и / или группы пользователей вручную или нажмите на кнопку **Выбрать**.

      Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

f. Задайте или измените список пользователей и / или групп пользователей, которым запрещено запускать программы, удовлетворяющие включающим условиям срабатывания правила. Для этого в поле **Пользователи и / или группы, получающие запрет** введите имена пользователей и / или группы пользователей вручную или нажмите на кнопку **Выбрать**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

5. Нажмите на кнопку **OK**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Добавление условия срабатывания правила контроля запуска программ

► *Чтобы добавить условие срабатывания правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Добавить**, если вы хотите добавить условие срабатывания нового правила контроля запуска программ.

   - Выберите из списка **Правила контроля запуска программ** нужное правило и нажмите на кнопку **Изменить**, если вы хотите добавить условие срабатывания уже существующего правила контроля запуска программ.

   Откроется окно **Правило контроля запуска программ**.

4. Выполните одно из следующих действий:

   - Если вы хотите добавить включающее условие, нажмите на кнопку **Добавить** в таблице **Включающие условия**.
   - Если вы хотите добавить исключающее условие, нажмите на кнопку **Добавить** в таблице **Исключающие условия**.

   Откроется контекстное меню кнопки **Добавить**.

5. Выполните следующие действия:

   - Выберите пункт **Условие из свойств файла**, если вы хотите сформировать условие срабатывания правила контроля запуска программ на основе свойств исполняемого файла программы. Для этого выполните следующие действия:

     a. В стандартном окне Microsoft Windows **Открыть** выберите исполняемый файл программы, на основе свойств которого вы хотите сформировать условие срабатывания правила контроля запуска программ.

     b. Нажмите на кнопку **Открыть**.

        Откроется окно **Условие из свойств файла**.

        Параметры окна **Условие из свойств файла** имеют значения, извлеченные из свойств выбранного исполняемого файла программы.

     c. В окне **Условие из свойств файла** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к файлу или папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы. Для этого выберите соответствующий параметр.

     d. Если требуется, измените значения параметров выбранного критерия условия.

     e. Нажмите на кнопку **OK**.

- Выберите пункт **Условие(я) из свойств файлов указанной папки**, если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ из свойств файлов указанной папки. Для этого выполните следующие действия:

  a. В окне **Выбор папки** выберите папку с исполняемыми файлами программ, на основе свойств которых вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ.

  b. Нажмите на кнопку **OK**.

     Откроется окно **Добавление условий**.

  c. В поле **Папка** измените при необходимости путь к папке с исполняемыми файлами программ. Для этого нажмите на кнопку **Выбрать**. Откроется окно **Выбор папки**. В этом окне вы можете выбрать нужную папку.

  d. В раскрывающемся списке **Добавить по критерию** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы.

     Если в раскрывающемся списке **Добавить по критерию** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

  e. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условие(я) срабатывания правила.

  f. Нажмите на кнопку **Далее**.

     Отобразится список сформированных условий срабатывания правила.

  g. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило контроля запуска программ.

  h. Нажмите на кнопку **Завершить**.

- Выберите пункт **Условие(я) из свойств запускавшихся программ**, если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ из свойств запускавшихся на виртуальной машине программ. Для этого выполните следующие действия:

  a. В окне **Добавление условий** в раскрывающемся списке **Добавить по критерию** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы.

     Если в раскрывающемся списке **Добавить по критерию** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

  b. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условие(я) срабатывания правила.

  c. Нажмите на кнопку **Далее**.

     Отобразится список сформированных условий срабатывания правила.

  d. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило контроля запуска программ.

  e. Нажмите на кнопку **Завершить**.

- Выберите пункт **Условие(я) «KL-категория»,** если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ по критерию «KL-категория». Для этого выполните следующие действия:

  a. В окне **Условие(я) «KL-категория»** установите флажки около названий тех KL-категорий, на основе которых вы хотите создать условия срабатывания правила.

  b. Нажмите на кнопку **OK**.

- Выберите пункт **Условие вручную**, если вы хотите сформировать условие срабатывания правила контроля запуска программ вручную. Для этого выполните следующие действия:

  a. В окне **Пользовательское условие** введите путь к исполняемому файлу программы. Для этого нажмите на кнопку **Выбрать**.

     Откроется окно Microsoft Windows **Открыть**. В этом окне вы можете выбрать исполняемый файл программы.

  b. Выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к файлу или папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы. Для этого выберите соответствующий параметр.

  c. Если требуется, измените значения параметров выбранного критерия условия.

  d. Нажмите на кнопку **OK**.

- Выберите пункт **Условие по носителю файла**, если вы хотите сформировать условие срабатывания правила контроля запуска, основанное на информации о носителе исполняемого файла программы. Для этого выполните следующие действия:

  a. В окне **Условие по носителю файла** в раскрывающемся списке **Носитель** выберите тип носителя, запуск программ с которого контролирует правило контроля запуска программ.

  b. Нажмите на кнопку **OK**.

Изменение статуса правила контроля запуска программ

► *Чтобы изменить статус работы правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
3. В списке правил выберите правило, статус работы которого вы хотите изменить.
4. В графе **Статус** по левой клавише мыши откройте контекстное меню графы и выберите нужный статус работы правила:
   - Если вы хотите включить использование правила, выберите значение *Вкл*.
   - Если вы хотите выключить использование правила, выберите значение *Выкл*.
   - Если вы хотите, чтобы правило работало в тестовом режиме, выберите значение *Тест*.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение шаблонов сообщений Контроля запуска программ

Когда вы пытаетесь запустить программу, запрещенную правилом контроля запуска программ, Kaspersky Security выводит сообщение о блокировке запуска программы. Если блокировка запуска программы, по вашему мнению, произошла ошибочно, по ссылке из текста сообщения о блокировке вы можете отправить жалобу администратору локальной сети организации.

Для сообщения о блокировке запуска программы и письма-жалобы предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.
4. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон письма-жалобы администратору локальной сети организации, выберите закладку **Жалоба**.
5. Измените шаблон сообщения о блокировке или письма-жалобы. Для этого используйте кнопки **По умолчанию** и **Переменные**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль активности программ

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows и во время установки выбрали тип «Установка компонентов защиты и контроля».

Этот раздел содержит информацию о Контроле активности программ и инструкции о том, как настроить параметры компонента.

В этом разделе

О Контроле активности программ

Компонент Контроль активности программ предотвращает выполнение программами опасных для операционной системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным.

Компонент контролирует работу программ на защищенной виртуальной машине, в том числе доступ программ к защищаемым ресурсам (например, к файлам и папкам, ключам реестра), с помощью *правил контроля программ*. Правила контроля программ представляют собой набор ограничений для различных действий программ в операционной системе и прав доступа к ресурсам защищенной виртуальной машины.

Сетевую активность программ контролирует компонент Сетевой экран (см. раздел «О Сетевом экране» на стр. 87).

Во время первого запуска программы на защищенной виртуальной машине компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из *групп доверия*. Группа доверия определяет правила контроля программ, которые Kaspersky Security применяет для контроля работы программ.

Для более эффективной работы Контроля активности программ вам рекомендуется принять участие в Kaspersky Security Network (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля программ.

Во время повторного запуска программы Контроль активности программ проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие правила контроля программ. Если программа была изменена, Контроль активности программ исследует программу как при первом запуске.

Включение и выключение Контроля активности программ

По умолчанию Контроль активности программ включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. При необходимости Вы можете выключить Контроль активности программ.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Контроль активности программ на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль активности программ.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль активности программ.

     Значок статуса работы компонента , отображающийся слева в строке Контроль активности программ, изменится на значок .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль активности программ.

     Значок статуса работы компонента , отображающийся слева в строке Контроль активности программ, изменится на значок .

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Контроль активности программ из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел Контроль активности программ.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

   > Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В правой части окна выполните одно из следующих действий:
   - Установите флажок **Включить Контроль активности программ**, если вы хотите включить Контроль активности программ.
   - Снимите флажок **Включить Контроль активности программ**, если вы хотите выключить Контроль активности программ.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Распределение программ по группам доверия

Во время первого запуска программы на защищенной виртуальной машине компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из групп доверия.

На первом этапе проверки программы Kaspersky Security ищет запись о программе во внутренней базе известных программ, а затем отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). Если запись о программе найдена в базе Kaspersky Security Network, то программа помещается в группу доверия, зарегистрированную в базе Kaspersky Security Network.

Чтобы распределять по группам доверия неизвестные программы (отсутствующие в базе Kaspersky Security Network и не имеющие цифровой подписи доверенного производителя), программа Kaspersky Security по умолчанию использует эвристический анализ. В процессе эвристического анализа Kaspersky Security определяет степень угрозы программы. На основании степени угрозы программы Kaspersky Security помещает программу в ту или иную группу доверия. Вместо использования эвристического анализа вы можете указать группу доверия, в которую программа Kaspersky Security должна автоматически помещать все неизвестные программы.

По умолчанию Kaspersky Security проверяет программу в течение 30 секунд. Если по истечении этого времени определение степени угрозы программы не завершено, Kaspersky Security помещает программу в группу доверия «Слабые ограничения» и продолжает определять степень угрозы программы в фоновом режиме. Затем Kaspersky Security помещает программу в окончательную группу доверия. Вы можете изменить время, которое отводится для проверки степени угрозы запускаемых программ. Если вы уверены, что все запускаемые на защищенной виртуальной машине программы не представляют угрозы для ее безопасности, то время, отведенное для определения степени угрозы программы, можно уменьшить. Если же вы устанавливаете на защищенную виртуальную машину программы, в безопасности которых вы не уверены, время определения степени угрозы программ рекомендуется увеличить.

Если степень угрозы программы высока, то Kaspersky Security уведомляет вас об этом и предлагает выбрать группу доверия, в которую следует поместить эту программу. Уведомление содержит статистику использования этой программы участниками Kaspersky Security Network. На основании этой статистики, а также зная историю появления программы на виртуальной машине, вы можете принять более объективное решение о том, в какую группу доверия следует поместить эту программу.

► *Чтобы настроить распределение программ по группам доверия, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия «Доверенные», установите флажок **Доверять программам, имеющим цифровую подпись**.
4. Выберите способ распределения неизвестных программ по группам доверия:
   - Если вы хотите использовать эвристический анализ для распределения неизвестных программ по группам доверия, выберите вариант **Использовать эвристический анализ для определения группы** и укажите время, которое отводится для проверки запускаемой программы, в поле **Максимальное время определения группы**.
   - Если вы хотите помещать все неизвестные программы в указанную группу доверия, выберите вариант **Автоматически помещать в группу** и выберите нужную группу доверия из раскрывающегося списка.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Перемещение программы в группу доверия

Во время первого запуска программы Kaspersky Security автоматически помещает программу в ту или иную группу доверия. При необходимости вы можете вручную переместить программу в другую группу доверия.

Специалисты «Лаборатории Касперского» не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости рекомендуется изменить правила контроля отдельной программы (см. раздел «Изменение правила контроля программы» на стр. 163).

► *Чтобы переместить программу в группу доверия, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы**.
4. Выберите закладку **Правила контроля программ**.
5. В списке программ выберите нужную программу.
6. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню программы. В контекстном меню программы выберите пункт **Переместить в группу** → **<название группы>**.
   - Откройте контекстное меню по ссылке **Доверенные** / **Слабые ограничения** / **Сильные ограничения** / **Недоверенные** в левом нижнем углу закладки **Правила контроля программ**. В контекстном меню выберите нужную группу доверия.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с правилами контроля программ

По умолчанию для контроля работы программы применяются правила контроля программ, определенные для той группы доверия, в которую Kaspersky Security поместил программу при первом ее запуске. При необходимости вы можете изменить правила контроля программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Правила контроля программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем правила контроля программ, определенные для группы доверия. То есть, если параметры правил контроля программ, определенные для отдельной программы или группы программ внутри группы доверия, отличны от параметров правил контроля программ, определенных для группы доверия, то Контроль активности программ контролирует работу программы или группы программ внутри группы доверия в соответствии с правилами контроля программ, определенными для программы или группы программ.

В этом разделе

Изменение правил контроля групп доверия и правил контроля групп программ

По умолчанию для разных групп доверия созданы оптимальные правила контроля программ. Параметры правил контроля групп программ, входящих в группу доверия, наследуют значения параметров правил контроля групп доверия. Вы можете изменить предустановленные правила контроля групп доверия и правила контроля групп программ.

► *Чтобы изменить правила контроля группы доверия или правила контроля группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы**.

4. Выберите закладку **Правила контроля программ**.

5. В списке программ выберите нужную группу доверия или группу программ.

6. По правой клавише мыши откройте контекстное меню группы доверия или группы программ и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.

7. Выполните одно из следующих действий:

   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на доступ к процессам и объектам операционной системы.

8. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.

9. В контекстном меню выберите нужный пункт:

   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.

   > Если вы изменяете правила контроля группы доверия, то пункт **Наследовать** недоступен для выбора.

10. Нажмите на кнопку **OK** в окне **Правила контроля группы программ**.

11. Нажмите на кнопку **OK** в окне **Программы**.

12. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение правила контроля программы

По умолчанию параметры правил контроля программ, входящих в группу программ или в группу доверия, наследуют значения параметров правил контроля группы доверия. Вы можете изменить параметры правил контроля программ.

► *Чтобы изменить правило контроля программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы**.

4. Выберите закладку **Правила контроля программ**.

5. В списке программ выберите нужную программу.

6. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   - Нажмите на кнопку **Дополнительно**, расположенную в правом нижнем углу закладки **Правила контроля программ**.

   Откроется окно **Правила контроля программы**.

7. Выполните одно из следующих действий:

    - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля программы, регулирующие права программы на операции с реестром операционной системы, файлами пользователя и параметрами программ.
    - Выберите закладку **Права**, если вы хотите изменить правила контроля программы, регулирующие права программы на доступ к процессам и объектам операционной системы.

8. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
9. В контекстном меню выберите нужный пункт:

    - **Наследовать**.
    - **Разрешать**.
    - **Запрещать**.
    - **Записывать в отчет**.

10. Нажмите на кнопку **OK** в окне **Правила контроля программы**.
11. Нажмите на кнопку **OK** в окне **Программы**.
12. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение загрузки и обновления правил контроля программ из базы Kaspersky Security Network

По умолчанию для программ, найденных в базе Kaspersky Security Network (KSN), применяются правила контроля программ, загруженные из этой базы.

Если на момент первого своего запуска программа отсутствовала в базе KSN, но затем информация о ней была добавлена в базу KSN, то по умолчанию Kaspersky Security автоматически обновляет правила контроля этой программы.

Вы можете выключить загрузку правил контроля программ из базы KSN и автоматическое обновление правил контроля для ранее неизвестных программ.

► *Чтобы выключить загрузку и обновление правил контроля программ из базы Kaspersky Security Network, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Снимите флажок **Обновлять правила контроля ранее неизвестных программ из базы KSN**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение наследования ограничений родительского процесса

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска программы является другая программа, образуется последовательность запуска, состоящая из родительских и дочерних процессов.

Когда программа пытается получить доступ к защищаемому ресурсу, Контроль активности программ анализирует права всех родительских процессов этой программы на доступ к защищаемому ресурсу. При этом выполняется правило минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы применяются права доступа с минимальным приоритетом.

Приоритет прав доступа следующий:

1. **Разрешать**. Это право доступа имеет высший приоритет.

2. **Запрещать**. Это право доступа имеет низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права (см. раздел «Изменение правила контроля программы» на стр. 163) или выключить наследование ограничений родительского процесса.

► *Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы**.
4. Выберите закладку **Правила контроля программ**.
5. В списке программ выберите нужную программу.
6. По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
7. Выберите закладку **Исключения**.
8. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.
9. Нажмите на кнопку **OK** в окне **Правила контроля программы**.
10. Нажмите на кнопку **OK** в окне **Программы**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Исключение некоторых действий программы из правил контроля программы

► *Чтобы исключить некоторые действия программы из правил контроля программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Программы**.

   Откроется окно **Программы**.
4. Выберите закладку **Правила контроля программ**.
5. В списке программ выберите нужную программу.
6. По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
7. Выберите закладку **Исключения**.
8. Установите флажки напротив действий программы, которые контролировать не нужно:
   - **Не проверять открываемые файлы**.
   - **Не контролировать активность программы**.
   - **Не наследовать ограничения родительского процесса (программы)**.
   - **Не контролировать активность дочерних программ**.
   - **Разрешать взаимодействие с интерфейсом программы**.
   - **Не проверять сетевой трафик**.

9. Нажмите на кнопку **OK** в окне **Правила контроля программы**.

10. Нажмите на кнопку **OK** в окне **Программы**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка параметров хранения правил контроля неиспользуемых программ

По умолчанию правила контроля программ, которые не запускались в течение 60 дней, автоматически удаляются. Вы можете изменить время хранения правил контроля неиспользуемых программ или выключить их автоматическое удаление.

► *Чтобы настроить параметры хранения правил контроля неиспользуемых программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Выполните одно из следующих действий:

   - Установите флажок **Удалять правила контроля программ, не запускавшихся более** и укажите нужное количество дней, если вы хотите, чтобы программа Kaspersky Security удаляла правила контроля неиспользуемых программ.

   - Снимите флажок **Удалять правила контроля программ, не запускавшихся более**, если вы хотите выключить автоматическое удаление правил контроля неиспользуемых программ.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита ресурсов операционной системы и персональных данных

Компонент Контроль активности программ управляет правами программ на операции над различными категориями ресурсов операционной системы и персональных данных.

Специалисты «Лаборатории Касперского» выделили предустановленные категории защищаемых ресурсов. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Вы можете выполнить следующие действия:

- добавить новую категорию защищаемых ресурсов;
- добавить новый защищаемый ресурс;
- выключить защиту ресурса.

В этом разделе

Добавление категории защищаемых ресурсов

► *Чтобы добавить новую категорию защищаемых ресурсов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы**.

4. Выберите закладку **Защищаемые ресурсы**.

5. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.

6. В верхней левой части закладки **Защищаемые ресурсы** по левой клавише мыши откройте контекстное меню кнопки **Добавить**.

7. В контекстном меню выберите пункт **Категорию**.

   Откроется окно **Категория защищаемых ресурсов**.

8. Введите название новой категории защищаемых ресурсов.

9. Нажмите на кнопку **ОК**.

   В списке категорий защищаемых ресурсов появится новый элемент.

10. Нажмите на кнопку **ОК** в окне **Программы**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Добавление защищаемого ресурса

► *Чтобы добавить защищаемый ресурс, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы**.

4. Выберите закладку **Защищаемые ресурсы**.

5. В левой части закладки **Защищаемые ресурсы** выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

6. В верхней левой части закладки **Защищаемые ресурсы** по левой клавише мыши откройте контекстное меню кнопки **Добавить**.

7. В контекстном меню выберите тип ресурса, который вы хотите добавить:

   - **Файл или папку**.
   - **Ключ реестра**.

   Откроется окно **Защищаемый ресурс**.

8. В поле **Название** введите название защищаемого ресурса.

9. Нажмите на кнопку **Обзор**.

10. В открывшемся окне задайте необходимые параметры в зависимости от типа добавляемого защищаемого ресурса и нажмите на кнопку **OK**.

11. В окне **Защищаемый ресурс** нажмите на кнопку **OK**.

    На закладке **Защищаемые ресурсы** в списке защищаемых ресурсов выбранной категории появится новый элемент.

12. Нажмите на кнопку **OK** в окне **Программы**.

13. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение защиты ресурса

► *Чтобы выключить защиту ресурса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Ресурсы**.

   Откроется окно **Программы**.
4. Выберите закладку **Защищаемые ресурсы**.
5. Выполните одно из следующих действий:

   - В левой части закладки в списке защищаемых ресурсов выберите ресурс, защиту которого вы хотите выключить, и снимите флажок рядом с его названием.
   - Добавьте ресурс в список исключений из защиты компонентом Контроль активности программ. Для этого выполните следующие действия:

     a. В верхней правой части закладки **Защищаемые ресурсы** нажмите на кнопку **Исключения**.

     b. В открывшемся окне **Исключения** по левой клавише мыши откройте контекстное меню кнопки **Добавить**.

     c. В контекстном меню выберите тип ресурса, который вы хотите добавить в список исключений из защиты компонента Контроль активности программ: **Файл или папку** или **Ключ реестра**.

        Откроется окно **Защищаемый ресурс**.

     d. В поле **Название** введите название защищаемого ресурса.

e. Нажмите на кнопку **Обзор**.

f. В открывшемся окне задайте необходимые параметры в зависимости от типа защищаемого ресурса, который вы хотите добавить в список исключений из защиты компонентом Контроль активности программ.

g. Нажмите на кнопку **OK**.

h. Нажмите на кнопку **OK** в окне **Защищаемый ресурс**.

   В списке ресурсов, исключенных из защиты компонента Контроль активности программ, появится новый элемент.

i. Нажмите на кнопку **OK** в окне **Исключения**.

6. Нажмите на кнопку **OK** в окне **Программы**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль устройств

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows и во время установки выбрали тип «Установка компонентов защиты и контроля».

Этот раздел содержит информацию о Контроле устройств и инструкции о том, как настроить параметры компонента.

В этом разделе

О Контроле устройств

Контроль устройств обеспечивает безопасность конфиденциальных данных путем ограничения доступа пользователей к устройствам, установленным или подключенным к защищенной виртуальной машине:

- устройствам хранения данных (жесткие диски, съемные диски, CD/DVD-диски);
- сетевым устройствам (модемы, внешние сетевые карты);
- устройствам печати (принтеры);
- шинам подключения (далее также «шинам») – интерфейсам, с помощью которых устройства подключаются к защищенной виртуальной машине (например, USB, FireWire).

Контроль устройств регулирует доступ пользователей к устройствам с помощью *правил доступа к устройствам* (см. раздел «*О правилах доступа к устройствам и шинам подключения*» на стр. 177) (далее также «правил доступа») и *правил доступа к шинам подключения* (далее также «правил доступа к шинам»).

По умолчанию доступ ко всем типам устройств и шинам подключения разрешен для всех пользователей в любое время, фиксация в отчетах программы запрещенных попыток доступа к устройствам и шинам подключения включена.

Включение и выключение Контроля устройств

По умолчанию Контроль устройств включен. Вы можете выключить Контроль устройств при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Контроль устройств на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль устройств.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль устройств.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль устройств.

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Контроль устройств из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

    - Установите флажок **Включить Контроль устройств**, если вы хотите включить Контроль устройств.

    - Снимите флажок **Включить Контроль устройств**, если вы хотите выключить Контроль устройств.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О правилах доступа к устройствам и шинам подключения

Правило доступа к устройствам представляет собой набор параметров, которые определяют следующие функции компонента Контроль устройств:

- Разрешение выбранным пользователям и / или группам пользователей доступа к типам устройств в определенные интервалы времени.

  Вы можете выбрать пользователя и / или группу пользователей и создать для них расписание доступа к устройствам.

- Установка права на чтение содержимого устройств памяти.

- Установка права на изменение содержимого устройств памяти.

По умолчанию для всех типов устройств из классификации компонента Контроль устройств созданы правила доступа, которые разрешают полный доступ к устройствам всем пользователям в любое время, если разрешен доступ к шинам подключения для соответствующих типов устройств.

Правило доступа к шине подключения представляет собой разрешение или запрет на доступ к шине подключения.

Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Вы не можете создавать и удалять правила доступа к устройствам и правила доступа к шинам подключения, но вы можете изменять их.

О доверенных устройствах

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Если устройство добавлено в список доверенных устройств, а для устройств этого типа создано правило доступа, запрещающее или ограничивающее доступ, то при принятии решения о доступе к устройству наличие устройства в списке доверенных устройств имеет более высокий приоритет, чем правило доступа.

Типовые решения о доступе к устройствам

Kaspersky Security принимает решение о доступе к устройству после того, как вы подключили это устройство к защищенной виртуальной машине.

Таблица 2. Типовые решения о доступе к устройствам

Исходные условия	**Промежуточные шаги до принятия решения о доступе к устройству**			**Решение о доступе к устройству**
	Проверка наличия устройства в списке доверенных устройств	**Проверка доступа к устройству на основании правила доступа**	**Проверка доступа к шине на основании правила доступа к шине**	
Устройства нет в классификации компонента Контроль устройств.	Нет в списке доверенных устройств.	Нет правила доступа.	Не проверяется.	Доступ разрешен.
Устройство является доверенным.	Есть в списке доверенных устройств.	Не проверяется.	Не проверяется.	Доступ разрешен.

Исходные условия	Промежуточные шаги до принятия решения о доступе к устройству			Решение о доступе к устройству
	Проверка наличия устройства в списке доверенных устройств	Проверка доступа к устройству на основании правила доступа	Проверка доступа к шине на основании правила доступа к шине	
Доступ к устройству разрешен.	Нет в списке доверенных устройств.	Доступ разрешен.	Не проверяется.	Доступ разрешен.
Доступ к устройству зависит от шины.	Нет в списке доверенных устройств.	Доступ зависит от шины.	Доступ разрешен.	Доступ разрешен.
Доступ к устройству зависит от шины.	Нет в списке доверенных устройств.	Доступ зависит от шины.	Доступ запрещен.	Доступ запрещен.
Доступ к устройству разрешен. Правило доступа к шине отсутствует.	Нет в списке доверенных устройств.	Доступ разрешен.	Нет правила доступа к шине.	Доступ разрешен.
Доступ к устройству запрещен.	Нет в списке доверенных устройств.	Доступ запрещен.	Не проверяется.	Доступ запрещен.
Правило доступа к устройству и правило доступа к шине отсутствуют.	Нет в списке доверенных устройств.	Нет правила доступа.	Нет правила доступа к шине.	Доступ разрешен.
Правило доступа к устройству отсутствует.	Нет в списке доверенных устройств.	Нет правила доступа.	Доступ разрешен.	Доступ разрешен.
Правило доступа к устройству отсутствует.	Нет в списке доверенных устройств.	Нет правила доступа.	Доступ запрещен.	Доступ запрещен.

Вы можете изменить правило доступа к устройству после подключения устройства. Если устройство было подключено и правило доступа разрешало доступ к устройству, а после вы изменили правило доступа и запретили доступ к устройству, то при очередном обращении к устройству за какой-либо файловой операцией (просмотр дерева каталогов, чтение, запись) Kaspersky Security блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Изменение правила доступа к устройствам

► *Чтобы изменить правило доступа к устройствам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. Выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Выберите правило доступа, которое хотите изменить.

5. Нажмите на кнопку **Изменить**. Кнопка доступна только для тех типов устройств, которые имеют файловую систему.

   Откроется окно **Настройка правила доступа к устройствам**.

   По умолчанию правило доступа к устройствам разрешает полный доступ к типу устройств всем пользователям в любое время. Такое правило доступа в списке **Пользователи и / или группы пользователей** содержит группу **Все**, а в таблице **Права выделенной группы пользователей по расписаниям доступа** содержит расписание доступа к устройствам в течение всего времени с установленными правами на все возможные операции с устройствами.

6. Измените параметры правила доступа к устройствам:

   a. Для изменения списка **Пользователи и / или группы пользователей** используйте кнопки **Добавить**, **Изменить**, **Удалить**.

   b. Для изменения списка расписаний доступа к устройствам используйте кнопки **Создать**, **Изменить**, **Копировать**, **Удалить** в таблице **Права выделенной группы пользователей по расписаниям доступа**.

   c. Выберите пользователя и / или группу пользователей в списке **Пользователи и / или группы пользователей**.

   d. В таблице **Права выделенной группы пользователей по расписаниям доступа** настройте расписание доступа к устройствам для выбранного пользователя и / или группы пользователей. Для этого установите флажки около названий тех расписаний доступа к устройствам, которые вы хотите использовать в изменяемом правиле доступа к устройствам.

   e. Для каждого используемого для выбранного пользователя и / или группы пользователей расписания доступа к устройствам задайте операции, которые разрешаются при работе с устройствами. Для этого в таблице **Права выделенной группы пользователей по расписаниям доступа** установите флажки в графах с названиями нужных операций.

   f. Повторите пункты c – e для остальных элементов списка **Пользователи и / или группы пользователей**.

   g. Нажмите на кнопку **ОК**.

   После того как вы изменили исходные значения параметров правила доступа к устройствам, параметр доступа к типу устройств принимает значение О*граничивать правилами*.

7. При необходимости на закладке **Типы устройств** окна настройки компонента Контроль устройств измените значения параметра доступа:

   - если вы хотите разрешить доступ к типу устройств, по левой кнопке мыши в графе **Доступ** вызовите контекстное меню и выберите пункт **Разрешать**;
   - если вы хотите запретить доступ к типу устройств, по левой кнопке мыши в графе **Доступ** вызовите контекстное меню и выберите пункт **Запрещать**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение правила доступа к шине подключения

► *Чтобы изменить правило доступа к шине подключения, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. Выберите закладку **Шины подключения**.

   На закладке **Шины подключения** находятся правила доступа для всех шин подключения, которые есть в классификации компонента Контроль устройств.

4. Выберите правило доступа к шине, которое хотите изменить.
5. Измените значение параметра доступа:

   - если вы хотите разрешить доступ к шине подключения, в графе **Доступ** вызовите контекстное меню и выберите пункт **Разрешать**;
   - если вы хотите запретить доступ к шине подключения, в графе **Доступ** вызовите контекстное меню и выберите пункт **Запрещать**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Действия с доверенными устройствами

Для работы с доверенными устройствами доступны следующие действия:

- добавление устройства в список доверенных устройств;
- изменение пользователя и / или группы пользователей, которым разрешен доступ к доверенному устройству;
- удаление устройства из списка доверенных устройств.

В этом разделе

Добавление устройства в список доверенных устройств

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»).

► *Чтобы добавить устройство в список доверенных устройств, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. Выберите закладку **Доверенные устройства**.

4. Нажмите на кнопку **Выбрать**.

   Откроется окно **Выбор доверенных устройств**.

5. Установите флажок напротив названия устройства, которое вы хотите добавить в список доверенных устройств.

   Список устройств в графе **Устройства** зависит от того, какое значение выбрано в раскрывающемся списке **Отображать подключенные устройства**.

6. Нажмите на кнопку **Выбрать**.

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

7. Задайте пользователей и / или группы пользователей, для которых Kaspersky Security должен распознавать выбранные устройства как доверенные.

   Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

8. Нажмите на кнопку **OK** в окне **Выбор доверенных устройств**.

   В таблице на закладке **Доверенные устройства** окна параметров компонента **Контроль устройств** появится строка с параметрами добавленного доверенного устройства.

9. Повторите пункты 4-8 для каждого устройства, которое вы хотите добавить в список доверенных устройств для определенных пользователей и / или групп пользователей.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение параметра Пользователи доверенного устройства

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»). Вы можете изменить параметр **Пользователи** доверенного устройства.

► *Чтобы изменить параметр Пользователи доверенного устройства, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. Выберите закладку **Доверенные устройства**.
4. В списке доверенных устройств выберите устройство, параметры которого вы хотите изменить.
5. Нажмите на кнопку **Изменить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
6. Измените список пользователей и / или групп пользователей, для которых устройство является доверенным.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление устройства из списка доверенных устройств

► *Чтобы удалить устройство из списка доверенных устройств, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. В правой части окна выберите закладку **Доверенные устройства**.

4. Выберите устройство, которое вы хотите удалить из списка доверенных устройств.

5. Нажмите на кнопку **Удалить**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Решение о доступе к устройству, которое вы удалили из списка доверенных устройств, Kaspersky Security принимает на основании правил доступа к устройствам и правил доступа к шинам подключения.

Изменение шаблонов сообщений Контроля устройств

Когда вы пытаетесь обратиться к заблокированному устройству, Kaspersky Security выводит сообщение о блокировке доступа к устройству или запрете операции над содержимым устройства. Если блокировка доступа к устройству или запрет операции с содержимым устройства, по вашему мнению, произошли ошибочно, по ссылке из текста сообщения о блокировке вы можете отправить жалобу администратору локальной сети организации.

Для сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства и письма-жалобы предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщений Контроля устройств, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.

4. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, выберите закладку **Блокировка**.

   - Если вы хотите изменить шаблон письма-жалобы администратору локальной сети организации, выберите закладку **Жалоба**.

5. Измените шаблон сообщения о блокировке или письма-жалобы. Для этого используйте кнопки **По умолчанию** и **Переменные**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Получение доступа к заблокированному устройству

Вы можете получить доступ к заблокированному устройству. Для этого нужно сделать запрос из окна настройки компонента Контроль устройств или по ссылке в сообщении о блокировке устройства.

> Функциональность Kaspersky Security для получения временного доступа к устройству доступна, только если Kaspersky Security работает под политикой Kaspersky Security Center и эта функциональность включена в параметрах политики (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

► *Чтобы получить доступ к заблокированному устройству из окна настройки компонента Контроль устройств, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. Выберите закладку **Центр управления**.

3. Раскройте блок **Контроль рабочего места**.

4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль устройств.

   Откроется меню действий с компонентом.

5. Выберите в меню пункт **Доступ к устройству**.

   Откроется окно **Запрос доступа к устройству**.

6. В списке подключенных устройств выберите то устройство, к которому вы хотите получить доступ.

7. Нажмите на кнопку **Получить ключ доступа**.

   Откроется окно **Получение ключа доступа к устройству**.

8. В поле **Длительность доступа** укажите, на какое время вы хотите получить доступ к устройству.

9. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.

10. Выберите папку, в которую вы хотите сохранить файл с ключом доступа к устройству, и нажмите на кнопку **Сохранить**.

11. Передайте файл с ключом доступа к устройству администратору локальной сети организации.

12. Получите от администратора локальной сети организации код доступа к устройству.

13. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать код доступа**.

    Откроется стандартное окно Microsoft Windows **Загрузка кода доступа**.

14. Выберите полученный от администратора локальной сети организации файл с кодом доступа к устройству и нажмите на кнопку **Открыть**.

    Откроется окно **Активация кода доступа к устройству** с информацией о предоставленном доступе.

15. В окне **Активация кода доступа к устройству** нажмите на кнопку **ОК**.

► *Чтобы получить доступ к заблокированному устройству по ссылке в сообщении о блокировке устройства, выполните следующие действия:*

1. Из окна сообщения о блокировке устройства или шины подключения перейдите по ссылке **Запросить доступ**.

   Откроется окно **Получение ключа доступа к устройству**.

2. В поле **Длительность доступа** укажите, на какое время вы хотите получить доступ к устройству.

3. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.

4. Выберите папку, в которую вы хотите сохранить файл с ключом доступа к устройству, и нажмите на кнопку **Сохранить**.

5. Передайте файл с ключом доступа к устройству администратору локальной сети организации.

6. Получите от администратора локальной сети организации код доступа к устройству.

7. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать код доступа**.

   Откроется стандартное окно Microsoft Windows **Загрузка кода доступа**.

8. Выберите полученный от администратора локальной сети организации файл с кодом доступа к устройству и нажмите на кнопку **Открыть**.

   Откроется окно **Активация кода доступа к устройству** с информацией о предоставленном доступе.

9. В окне **Активация кода доступа к устройству** нажмите на кнопку **ОК**.

Период времени, на который предоставляется доступ к устройству, может отличаться от запрашиваемого вами периода времени. Доступ к устройству предоставляется на период времени, которой администратор локальной сети организации указывает при формировании кода доступа к устройству.

Веб-Контроль

Этот компонент доступен, если вы установили программу Kaspersky Security на виртуальной машине с настольной операционной системой Windows и во время установки выбрали тип «Установка компонентов защиты и контроля».

Этот раздел содержит информацию о Веб-Контроле и инструкции о том, как настроить параметры компонента.

В этом разделе

О Веб-Контроле

Компонент Веб-Контроль позволяет контролировать действия пользователей локальной сети организации: ограничивать или запрещать доступ к веб-ресурсам. Под веб-ресурсом подразумевается как отдельная веб-страница или несколько веб-страниц, так и веб-сайт или несколько веб-сайтов, сгруппированных по общему признаку.

Веб-Контроль предоставляет следующие возможности:

- Экономия трафика.

  Расход трафика контролируется путем ограничения или запрета загрузок мультимедийных файлов и ограничения или запрета доступа на не связанные с работой веб-ресурсы.

- Разграничение доступа по категориям содержания веб-ресурсов.

  Для уменьшения расхода трафика и потенциальных потерь из-за нецелевого использования рабочего времени вы можете ограничить или запретить доступ к веб-ресурсам определенных категорий (например, запретить доступ к веб-ресурсам категории «Новостные ресурсы»). Более подробно категории содержания описаны Базе знаний (http://support.kaspersky.ru/13175).

- Централизованное управление доступом к веб-ресурсам.

  При использовании Kaspersky Security Center доступны персональные и групповые параметры доступа к веб-ресурсам.

Все ограничения и запреты на доступ к веб-ресурсам реализуются в виде правил доступа к веб-ресурсам (см. раздел «О правилах доступа к веб-ресурсам» на стр. 193).

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен. Вы можете выключить Веб-Контроль при необходимости.

Вы можете включить и выключить компонент двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23);

- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 25).

► *Чтобы включить или выключить Веб-Контроль на закладке Центр управления главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Контроль рабочего места**.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Веб-Контроль.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Контроль.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Контроль.

   Если пункт меню недоступен, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

► *Чтобы включить или выключить Веб-Контроль из окна настройки параметров программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

   Если параметры компонента недоступны, это означает, что вы не можете включить или выключить этот компонент, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Веб-Контроль**, если вы хотите включить компонент Веб-Контроль.
   - Снимите флажок **Включить Веб-Контроль**, если вы хотите выключить компонент Веб-Контроль.

   Если Веб-Контроль выключен, Kaspersky Security не контролирует доступ к веб-ресурсам.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О правилах доступа к веб-ресурсам

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию**. Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к веб-ресурсам определенных категорий содержания и / или категорий типа данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Security выполняет действие, указанное в правиле.
- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Security в компоненте Веб-Контроль предустановлены два правила:

- Правило **Сценарии и таблицы стилей**, которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css?mode=normal, http://www.example.com/style.css.

- **Правило по умолчанию**, которое разрешает всем пользователям в любое время доступ к любым веб-ресурсам.

Действия с правилами доступа к веб-ресурсам

Вы можете выполнить следующие действия с правилами доступа к веб-ресурсам:

- Добавить новое правило.

- Экспортировать и импортировать список адресов веб-ресурсов правила.

  Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

- Изменить правило.

- Изменить приоритет правила.

  Приоритет правила определяется положением строки с кратким описанием правила в таблице **Правила доступа в порядке приоритета** окна параметров компонента Веб-Контроль. То есть правило, расположенное выше других правил в таблице **Правила доступа в порядке приоритета**, имеет более высокий приоритет.

  Если веб-ресурс, к которому пользователь пытается получить доступ, соответствует параметрам нескольких правил, то действие Kaspersky Security определяет правило с более высоким приоритетом.

- Проверить работу правила.

  Вы можете проверить согласованность работы правил с помощью инструмента «Диагностика правил».

- Включить и выключить правило.

  Правило доступа к веб-ресурсам может быть включено (имеет статус работы *Вкл*) или выключено (имеет статус работы *Выкл*). По умолчанию после создания правило включено (имеет статус работы *Вкл)*. Вы можете выключить правило.

- Удалить правило.

В этом разделе

Добавление и изменение правила доступа к веб-ресурсам

► *Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

3. Выполните одно из следующих действий:

   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

4. Задайте или измените параметры правила. Для этого выполните следующие действия:

   a. В поле **Название** введите или измените название правила.

   b. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент:

      - **Любое содержание**.
      - **По категориям содержания**.
      - **По типам данных**.
      - **По категориям содержания и типам данных**.

      Если выбран элемент, отличный от **Любое содержание**, откроется блок для выбора категорий содержания и / или категорий типа данных. Установите флажки напротив названий желаемых категорий содержания и / или категорий типа данных.

Установка флажка напротив названия категории содержания и / или категории типа данных означает, что Kaspersky Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим выбранным категориям содержания и / или категориям типа данных.

c. В раскрывающемся списке **Применять к адресам** выберите нужный элемент:

- **Ко всем адресам**.
- **К отдельным адресам**.

Если выбран элемент **К отдельным адресам**, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете создавать или изменять список адресов веб-ресурсов, используя кнопки **Добавить**, **Изменить**, **Удалить**. Для создания списка адресов веб-ресурсов вы можете также использовать *маски адреса веб-ресурса* (далее также «маски адреса») (см. раздел «Правила формирования масок адреса веб-ресурса» на стр. 199).

После создания списка адресов веб-ресурсов вы можете экспортировать его в файл, чтобы впоследствии импортировать этот список из файла (см. раздел «Экспорт и импорт списка адресов веб-ресурсов» на стр. 202).

d. Установите флажок **Укажите пользователей и / или группы** и нажмите на кнопку **Выбрать**.

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

e. Задайте или измените список пользователей и / или групп пользователей, для которых разрешен или ограничен доступ к веб-ресурсам, описанным в правиле.

f. Из раскрывающегося списка **Действие** выберите нужный элемент:

- **Разрешать**. Если выбрано это значение, то Kaspersky Security разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
- **Запрещать**. Если выбрано это значение, то Kaspersky Security запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
- **Предупреждать**. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим параметрам правила, Kaspersky Security

выводит сообщение-предупреждение о возможной небезопасности веб-ресурса. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

g. Из раскрывающегося списка **Расписание работы правила** выберите название нужного расписания или на основе выбранного расписания работы правила сформируйте новое расписание. Для этого выполните следующие действия:

   1. Нажмите на кнопку **Настройка** напротив раскрывающегося списка **Расписание работы правила**.

      Откроется окно **Расписание работы правила**.

   2. Чтобы добавить в расписание работы правила интервал времени, в течение которого правило не работает, в таблице с изображением расписания работы правила левой клавишей мыши нажмите по ячейкам таблицы, соответствующим нужному вам времени и дню недели.

      Цвет ячеек изменится на серый.

   3. Чтобы в расписании работы правила изменить интервал времени, в течение которого правило работает, на интервал времени, в течение которого правило не работает, левой клавишей мыши нажмите по серым ячейкам таблицы, соответствующим нужному вам времени и дню недели.

      Цвет ячеек изменится на зеленый.

   4. Нажмите на кнопку **OK** или **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила «Всегда», сформированного по умолчанию. Нажмите на кнопку **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила, сформированного не по умолчанию.

      Откроется окно **Название расписания работы правила**.

   5. Введите название расписания работы правила или оставьте название, предложенное по умолчанию.

   6. Нажмите на кнопку **OK**.

5. Нажмите на кнопку **OK** в окне **Правило доступа к веб-ресурсам**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Правила формирования масок адреса веб-ресурса

Использование маски адреса веб-ресурса может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует иметь в виду следующие правила:

1. Символ * заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса *abc* правило доступа к веб-ресурсам применяется ко всем адресам веб-ресурсов, содержащим последовательность abc. Пример: http://www.example.com/page_0-9abcdef.html.

   Символ ? трактуется как символ знака вопроса, а не любой один символ, как это принято в правилах формирования масок адреса в компоненте Веб-Антивирус.

   Для включения символа * в состав маски адреса нужно вводить два символа *, а не последовательность *, как это принято в правилах формирования масок адреса в компоненте Веб-Антивирус.

2. Последовательность символов www. в начале маски адреса трактуется как последовательность *.

   Пример: маска адреса www.example.com трактуется как *.example.com.

3. Если маска адреса начинается не с символа *, то содержание маски адреса эквивалентно тому же содержанию с префиксом *.

4. Последовательность символов *. В начале маски трактуется как *. или пустая строка.

   Пример: под действие маски адреса http://www.*.example.com попадает адрес веб-ресурса http://www2.example.com.

5. Если маска адреса заканчивается символом, отличным от / или *, то содержание маски адреса эквивалентно тому же содержанию с постфиксом /*.

Пример: под действие маски адреса http://www.example.com попадают адреса вида http://www.example.com/abc, где a, b, c – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес веб-ресурса с любым сетевым протоколом.

     Пример: под действие маски адреса example.com попадают адреса веб-ресурса http://example.com и https://example.com.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса веб-ресурса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса http://*.example.com попадает адрес веб-ресурса http://www.example.com и не попадает адрес https://www.example.com.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. То есть для таких масок адреса не выполняются правила 5 и 7.

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 3. Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 1.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	”example.com”	http://www.example.com	Нет	См. правило 9.
15	”http://www.example.com”	http://www.example.com/abc	Нет	См. правило 9.
16	”*.example.com”	http://www.example.com	Да	См. правила 1, 9.
17	”http://www.example.com/*”	http://www.example.com/abc	Да	См. правила 1, 9.
18	”www.example.com”	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов

веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

► *Чтобы экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать.
4. Нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

   Под раскрывающимся списком **Применять к адресам** отобразится список адресов веб-ресурсов, к которым применяется правило.
5. Если вы хотите экспортировать не весь список адресов веб-ресурсов, а только его часть, выделите нужные вам адреса веб-ресурсов.
6. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Откроется окно подтверждения действия.
7. Выполните одно из следующих действий:

   - Если вы хотите экспортировать только выделенные элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Да**.
   - Если вы хотите экспортировать все элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Нет**.

   Откроется стандартное окно Microsoft Windows **Сохранить как**.
8. Выберите файл, в который вы хотите экспортировать список адресов веб-ресурсов, и нажмите на кнопку **Сохранить**.

► *Чтобы импортировать в правило список адресов веб-ресурсов из файла, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выполните одно из следующих действий:

   - Если вы хотите создать новое правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
4. Выполните одно из следующих действий:

   - Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке **Применять к адресам** выберите элемент **К отдельным адресам**.
   - Если вы изменяете правило доступа к веб-ресурсам, перейдите к пункту 5 этой инструкции.
5. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Если вы создаете новое правило, откроется стандартное окно Microsoft Windows **Открыть файл**.

   Если вы изменяете правило, откроется окно подтверждения действия.
6. Выполните одно из следующих действий:

   - Если вы создаете новое правило доступа к веб-ресурсам, перейдите к пункту 7 этой инструкции.
   - Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:

- Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку **Да**.
- Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку **Нет**.

Откроется стандартное окно Microsoft Windows **Открыть файл**.

7. В окне Microsoft Windows **Открыть файл** выберите файл со списком адресов веб-ресурсов для импорта.
8. Нажмите на кнопку **Открыть**.
9. Нажмите на кнопку **OK** в окне **Правило доступа к веб-ресурсам**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Вы можете проверить работу правил доступа к веб-ресурсам. Для этого в компоненте Веб-Контроль предусмотрена «Диагностика правил». В результате проверки работы правил выводится сообщение о действии Kaspersky Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу(ам) (разрешение, запрет, предупреждение). Далее проверяются все сработавшие правила.

► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна нажмите на кнопку **Диагностика**.

   Откроется окно **Диагностика правил**.
4. Заполните поля в блоке **Условия**:

a. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Security контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.

b. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Security контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей. Для этого выполните следующие действия:

   1. Установите флажок **Укажите пользователей и / или группы** и нажмите на кнопку **Выбрать**.

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

   2. В окне Microsoft Windows **Выбор пользователей или групп** укажите нужных пользователей и / или группы пользователей и нажмите на кнопку **OK**.

c. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Security контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных, и установите флажки напротив названий нужных категорий содержания и / или категорий типа данных.

d. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсу(ам), указанным в условиях диагностики правил. Справа укажите день недели и время.

5. Нажмите на кнопку **Проверить**.

Справа от кнопки **Проверить** выводится сообщение о действии Kaspersky Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу(ам). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. В таблице в нижней части окна **Диагностика правил** выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Security. Правила выводятся в порядке убывания приоритета.

Изменение приоритета правил доступа к веб-ресурсам

Вы можете изменить приоритет каждого правила доступа к веб-ресурсам из списка правил, расположив их в определенном порядке.

Вы не можете изменить приоритет правила «Правило по умолчанию», оно всегда имеет самый низкий приоритет и располагается в конце списка правил.

► *Чтобы изменить приоритет правил доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В списке правил выберите правило, приоритет которого вы хотите изменить.
4. С помощью кнопок **Вверх** и **Вниз** переместите правило на желаемую позицию в списке правил.
5. Повторите действие пунктов инструкции 3-4 для тех правил, приоритет которых вы хотите изменить.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение правила доступа к веб-ресурсам

► *Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

3. В списке правил выберите правило, которое вы хотите включить или выключить.
4. В графе **Статус** выполните следующие действия:
   - Если вы хотите включить использование правила, выберите значение *Вкл*.
   - Если вы хотите выключить использование правила, выберите значение *Выкл*.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О сообщениях Веб-Контроля

В зависимости от действия, заданного в свойствах правил доступа к веб-ресурсам, при вашей попытке получить доступ к веб-ресурсам Kaspersky Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- **Сообщение-предупреждение**. Такое сообщение предупреждает о возможной опасности веб-сайта и / или несоответствии корпоративной политике. Kaspersky Security выводит сообщение-предупреждение, если в свойствах правила, описывающего этот веб-сайт, в раскрывающемся списке **Действие** выбран элемент **Предупреждать**.

  Если, на ваш взгляд, предупреждение ошибочно, вы можете открыть уже сформированное письмо-жалобу администратору локальной сети организации по ссылке из сообщения-предупреждения.

- **Сообщение о блокировке веб-ресурса**. Kaspersky Security выводит сообщение о блокировке веб-ресурса, если в свойствах правила, которое описывает этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Запрещать**.

  Если, на ваш взгляд, доступ к веб-ресурсу был заблокирован ошибочно, по ссылке из сообщения о блокировке веб-ресурса вы можете открыть уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и письма-жалобы для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание (см. раздел «Изменение шаблонов сообщений Веб-Контроля» на стр. 209).

Изменение шаблонов сообщений Веб-Контроля

► *Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.
4. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения-предупреждения, предупреждающего о возможной опасности веб-сайта, выберите закладку **Предупреждение**.
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-сайту, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон письма-жалобы, выберите закладку **Жалоба**.
5. Измените шаблон сообщения. Для этого используйте кнопки **Переменные** и **По умолчанию**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка виртуальной машины

Этот раздел содержит информацию об особенностях и настройке задач проверки, уровнях безопасности, методах и технологиях проверки, а также инструкции по работе с файлами, которые программа Kaspersky Security не обработала в процессе проверки виртуальной машины на вирусы и другие программы, представляющие угрозу.

В этом разделе

О задачах проверки

Антивирусная проверка является важным фактором для обеспечения безопасности виртуальной машины. Требуется регулярно проверять виртуальную машину на вирусы и другие вредоносные программы, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например из-за установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов и других вредоносных программ, в состав Kaspersky Security включены следующие задачи проверки:

- **Полная проверка**. Тщательная проверка всей гостевой операционной системы, установленной на защищенной виртуальной машине. По умолчанию Kaspersky Security проверяет следующие объекты:
  - системная память;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище операционной системы;
  - все жесткие и съемные диски, подключенные к защищенной виртуальной машине.

- **Проверка важных областей**. По умолчанию Kaspersky Security проверяет объекты, загрузка которых осуществляется при старте операционной системы.
- **Выборочная проверка**. Программа проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:
  - системная память;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище операционной системы;
  - почтовые базы;
  - все жесткие, съемные и сетевые диски, которые подключены к защищенной виртуальной машине;
  - любой выбранный файл.

Задача полной проверки и задача проверки важных областей являются специфическими. Для этих задач не рекомендуется изменять область проверки.

После запуска задач проверки процесс выполнения проверки отображается в поле напротив названия запущенной задачи проверки в блоке **Управление задачами** на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23).

Информация о результатах проверки и обо всех событиях, произошедших во время выполнения задач проверки, записывается в отчет Kaspersky Security.

Запуск и остановка задачи проверки

Независимо от выбранного режима запуска задачи проверки (см. раздел «Выбор режима запуска задачи проверки» на стр. 227) вы можете запустить или остановить задачу проверки в любой момент.

► *Чтобы запустить или остановить задачу проверки, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. Выберите закладку **Центр управления**.

3. Раскройте блок **Управление задачами**.

4. Нажмите на клавишу мыши на строке с названием задачи проверки.

   Откроется меню действий с задачей проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что управление этими задачами проверки запрещено политикой для всех защищенных виртуальных машин группы администрирования (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Запустить проверку**, если вы хотите запустить задачу проверки.

     Статус выполнения задачи, отображающийся справа от названия задачи проверки, изменится на *Выполняется*.

   - Выберите в меню пункт **Остановить проверку**, если вы хотите остановить задачу проверки.

     Статус выполнения задачи, отображающийся справа от названия задачи проверки, изменится на *Остановлено*.

Вы также можете запустить выборочную проверку любого файла, вызвав контекстное меню Windows и выбрав элемент **Проверить на вирусы**.

Настройка параметров задач проверки

Для настройки параметров задач проверки вы можете выполнить следующие действия:

- Изменить уровень безопасности.

  Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

- Изменить действие, которое программа Kaspersky Security выполняет при обнаружении зараженного файла.

- Сформировать область проверки.

  Вы можете расширить или сузить область проверки, добавив или удалив объекты проверки или изменив тип проверяемых файлов.

- Оптимизировать проверку.

  Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Security исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

- Настроить проверку составных файлов.

- Настроить использование эвристического анализа.

  Во время своей работы Kaspersky Security использует сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов «Лаборатории Касперского» сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Security анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать новые вредоносные объекты, записей о которых еще нет в базах программы.

- Настроить использование технологии проверки iSwift.

  Вы можете включить использование технологии iSwift, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки. Включение технологии iSwift также подразумевает использование технологии SharedCache, которая позволяет оптимизировать скорость проверки файлов за счет исключения из проверки файлов, уже проверенных на другой виртуальной машине.

- Выбрать режим запуска задач проверки.

  Если по каким-либо причинам запуск задачи проверки невозможен (например, защищенная виртуальная машина выключена), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

  Вы можете отложить запуск задачи проверки после старта программы для случаев, если вы выбрали режим запуска задачи проверки **По расписанию** и время запуска Kaspersky Security совпадает с расписанием запуска задачи проверки. Задача проверки запускается только по истечении указанного времени после старта программы.

- Настроить запуск задач проверки с правами другого пользователя.

- Задать параметры проверки съемных дисков при их подключении к защищенной виртуальной машине.

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки Kaspersky Security применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности*. Предусмотрено три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня **Рекомендуемый** считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского».

► *Чтобы изменить уровень безопасности, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:
   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение действия над зараженными файлами

► *Чтобы изменить действие над зараженными файлами, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:

   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

В правой части окна отобразятся параметры выбранной задачи проверки.

> Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:

   - **Выбирать действие автоматически**.

     Этот вариант выбран по умолчанию. При обнаружении угрозы программа выполняет действие **Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить**.

     > В отношении файлов, являющихся частью приложения Windows Store, программа Kaspersky Security выполняет действие **Удалять** вне зависимости от выбранного варианта.

   - **Выполнять действие: Удалять**.

   - **Выполнять действие: Информировать**.

   > При удалении или лечении копии файлов сохраняются в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области проверки

Областью проверки называется местоположение и тип файлов (например, все жесткие диски, объекты автозапуска, почтовые базы), которые программа проверяет во время выполнения задачи проверки.

Для формирования области проверки требуется выполнить следующие действия:

- Сформировать список объектов, которые проверяет Kaspersky Security.
- Выбрать тип проверяемых файлов.

► *Чтобы сформировать область проверки, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление задачами**.
4. Нажмите на строку с названием нужной задачи проверки:
   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   Откроется меню действий с задачей проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.
5. Выберите в меню пункт **Область проверки**.

   Откроется окно **Область проверки**.

6. В окне **Область проверки** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, нажмите на кнопку **Добавить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите изменить путь к объекту, выберите объект в списке объектов и нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

   - Если вы хотите удалить объект из области проверки, выберите объект в списке объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.

     > Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

7. В окне **Выбор объекта** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект, в окне **Выбор объекта** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта**, отобразятся в списке объектов в окне **Область проверки**.

     Нажмите на кнопку **OK**.

   - Если вы хотите изменить путь к объекту из списка объектов, укажите другой путь к объекту в поле **Объект** и нажмите на кнопку **OK**.

   - Если вы хотите удалить объект, в окне подтверждения удаления нажмите на кнопку **Да**.

8. При необходимости повторите пункты 6 и 7 для добавления объектов, изменения пути к ним или удаления объектов из области проверки.

9. Если вы хотите исключить объект из области проверки, в списке объектов окна **Область проверки** снимите флажок рядом с ним. Объект остается в списке проверяемых объектов, но не проверяется во время выполнения задачи проверки.

10. Нажмите на кнопку **OK** в окне **Область проверки**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

► *Чтобы выбрать тип проверяемых файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы.

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:

   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В окне с названием выбранной задачи проверки выберите закладку **Область действия**.

5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять во время выполнения выбранной задачи проверки:

   - Выберите **Все файлы**, если вы хотите проверять все файлы.
   - Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.

- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.

- Злоумышленник может отправить вирус или другую вредоносную программу на вашу виртуальную машину в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Kaspersky Security проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие вредоносные программы.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:

   - **Полная проверка**.

   - **Проверка важных областей**.

   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку **Область действия**.

5. В блоке **Оптимизация проверки** выполните следующие действия:

   - Установите флажок **Проверять только новые и измененные файлы**.
   - Установите флажок **Пропускать файлы, если их проверка длится более** и задайте длительность проверки одного файла (в секундах).

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других вредоносных программ является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие вредоносные программы составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить круг проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:
   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, вложенные OLE-объекты, файлы почтовых форматов или защищенные паролем архивы, установив соответствующие флажки.
5. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение при нажатии на нее левой клавишей мыши.

   Если флажок **Проверять только новые и измененные файлы** установлен, то проверяются только новые файлы.

6. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.

7. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Если вы не хотите, чтобы программа распаковывала составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.
   - Если вы хотите, чтобы программа распаковывала составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**. Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

   Kaspersky Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

8. Нажмите на кнопку **OK** в окне **Составные файлы**.
9. Нажмите на кнопку **OK** в окне с названием задачи проверки.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования эвристического анализа

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:

   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку **Дополнительно**.

5. В блоке **Методы проверки** выполните следующие действия:

   - Если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   - Если вы хотите, чтобы программа не использовала эвристический анализ во время выполнения задачи проверки, снимите флажок **Эвристический анализ**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка использования технологии iSwift

► *Чтобы настроить использование технологии iSwift, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:

   - **Полная проверка**.

- **Проверка важных областей**.
- **Выборочная проверка**.

В правой части окна отобразятся параметры выбранной задачи проверки.

> Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

4. В открывшемся окне выберите закладку **Дополнительно**.
5. В блоке **Технология проверки** выполните одно из следующих действий:
   - Установите флажок **Технология iSwift**, если вы хотите использовать эту технологию во время проверки.
   - Снимите флажок **Технология iSwift**, если вы не хотите использовать эту технологию во время проверки.

   > Включение технологии iSwift включает использование технологии SharedCache.

6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор режима запуска задачи проверки

► *Чтобы выбрать режим запуска задачи проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки:
   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна с названием выбранной задачи.
4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи проверки:
   - Выберите вариант **Вручную**, если вы хотите запускать задачу проверки вручную.
   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи проверки.
5. Выполните одно из следующих действий:
   - Если вы выбрали вариант **Вручную**, перейдите к пункту 6 инструкции.

- Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи проверки. Для этого выполните следующие действия:

  a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу проверки. Выберите один из следующих вариантов: **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**, **После каждого обновления**.

  b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи проверки.

  c. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы программа Kaspersky Security запускала не запущенные вовремя задачи проверки при первой возможности.

  > Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы** или **После каждого обновления**, то флажок **Запускать пропущенные задачи** недоступен.

  d. Установите флажок **Приостанавливать проверку по расписанию, если экранная заставка не включена и защищенная виртуальная машина разблокирована**, если вы хотите, чтобы программа Kaspersky Security приостанавливала задачу проверки, когда ресурсы виртуальной машины заняты. Этот вариант расписания запуска задачи проверки позволяет экономить вычислительную мощность виртуальной машины во время работы.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается от имени учетной записи, с правами которой вы зарегистрированы в гостевой операционной системе на защищенной виртуальной машине. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

► *Чтобы настроить запуск задачи проверки с правами другого пользователя, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи:
   - **Полная проверка**.
   - **Проверка важных областей**.
   - **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

   > Если в блоке отсутствуют какие-то задачи проверки, это означает, что настройка параметров этих задач проверки запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна с названием выбранной задачи проверки.
4. В блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя учетной записи пользователя, права которого требуется использовать для запуска задачи проверки.

6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для запуска задачи проверки.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка съемных дисков при подключении к виртуальной машине

В последнее время широкое распространение получили вредоносные программы, которые используют уязвимости операционной системы для распространения через локальные сети и съемные диски. Kaspersky Security позволяет проверять съемные диски на вирусы и другие вредоносные программы при подключении съемных дисков к виртуальной машине.

► *Чтобы настроить проверку съемных дисков при их подключении к виртуальной машине, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна выберите блок **Задачи по расписанию**.

   В правой части окна отобразятся общие параметры задач по расписанию.

3. В блоке **Проверка съемных дисков при подключении** в раскрывающемся списке **Действие при подключении съемного диска** выберите нужное действие:

   - **Не проверять**.
   - **Полная проверка**.
   - **Быстрая проверка**.

   Если блок недоступен, это означает, что настройка параметров проверки съемных дисков запрещена политикой для всех защищенных виртуальных машин группы администрирования (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

4. Установите флажок **Максимальный размер съемного диска** и в поле рядом укажите значение в мегабайтах, если вы хотите, чтобы программа Kaspersky Security проверяла съемные диски, размер которых меньше или равен указанному значению.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с необработанными файлами

Этот раздел содержит инструкции по работе с зараженными файлами, которые программа Kaspersky Security не обработала в процессе проверки виртуальной машины на вирусы и другие программы, представляющие угрозу.

В этом разделе

О необработанных файлах

Программа Kaspersky Security фиксирует информацию о файлах, в которых обнаружила угрозу в процессе своей работы, но не обработала. Эта информация записывается в виде событий в список необработанных файлов.

Зараженный файл считается *обработанным*, если программа Kaspersky Security в процессе проверки виртуальной машины на вирусы и другие вредоносные программы совершила одно из следующих действий с зараженным файлом согласно заданным параметрам:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Зараженный файл считается *необработанным*, если программа в процессе проверки виртуальной машины на вирусы и другие вредоносные программы по каким-либо причинам не совершила действие с зараженным файлом согласно заданным параметрам.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем устройстве без прав на запись данных).
- В параметрах программы для задач проверки в блоке **Действие при обнаружении угрозы** выбрано действие **Информировать**, а когда на экране отобразилось уведомление о зараженном файле, вы выбрали вариант **Пропустить**.

Вы можете вручную запустить задачу выборочной проверки файлов из списка необработанных файлов после обновления баз программы. После проверки статус файлов может измениться. Согласно статусу вы можете самостоятельно выполнить необходимые действия с файлами.

Например, вы можете выполнить следующие действия:

- удалить файлы со статусом *Зараженный* (см. раздел «*Удаление файлов из списка необработанных файлов*» на стр. 235);
- восстановить те зараженные файлы, в которых содержится важная информация, а также восстановить файлы со статусом *Вылечен* и *Не заражен* (см. раздел «*Восстановление файлов из списка необработанных файлов*» на стр. 234).

Работа со списком необработанных файлов

Список необработанных файлов представлен в виде таблицы.

Работая со списком необработанных файлов, вы можете выполнять следующие действия с необработанными файлами:

- просматривать список необработанных файлов;
- проверять необработанные файлы, используя текущую версию баз программы;
- восстанавливать файлы из списка необработанных файлов в исходные папки или в другую выбранную вами папку (в случае, если исходная папка размещения файла недоступна для записи);
- удалять файлы из списка необработанных файлов;
- открыть папку исходного размещения необработанного файла.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать список необработанных файлов по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска необработанных файлов;
- сортировать необработанные файлы;
- изменять порядок и набор граф, отображаемых в списке необработанных файлов;
- группировать необработанные файлы;
- копировать выбранные записи о необработанных файлах в буфер обмена.

В этом разделе

Запуск задачи выборочной проверки для необработанных файлов

Вы можете вручную запустить задачу выборочной проверки для необработанных файлов, например, если проверка была прервана по какой-либо причине или вы хотите, чтобы программа Kaspersky Security проверила файлы после очередного обновления баз программы.

► *Чтобы запустить задачу выборочной проверки для необработанных файлов, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Необработанные файлы**.

4. В таблице на закладке **Необработанные файлы** выберите один или несколько файлов, которые вы хотите проверить. Чтобы выбрать несколько файлов, выделяйте их, удерживая клавишу **CTRL**.

5. Запустите задачу выборочной проверки файлов одним из следующих способов:

   - Нажмите на кнопку **Перепроверить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Перепроверить**.

После завершения проверки на экране отобразится уведомление о количестве проверенных файлов и количестве обнаруженных угроз.

Восстановление файлов из списка необработанных файлов

При необходимости вы можете восстановить файлы из списка необработанных файлов.

Специалисты «Лаборатории Касперского» рекомендуют восстанавливать файлы из списка необработанных файлов только в том случае, если файлам присвоен статус *Не заражен*.

► *Чтобы восстановить файлы из списка необработанных файлов, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

3. Выберите закладку **Необработанные файлы**.

4. Если вы хотите восстановить все файлы, то выполните следующие действия:

   a. Откройте контекстное меню по правой клавише мыши в любом месте таблицы на закладке **Необработанные файлы**.

b. Выберите пункт **Восстановить все**.

Kaspersky Security переместит все файлы из списка необработанных файлов в папки их исходного размещения, если эти папки доступны для записи.

c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, то откроется стандартное окно Microsoft Windows **Сохранить как**. В этом окне вы можете указать папку для сохранения файла.

5. Если вы хотите восстановить один или несколько файлов, то выполните следующие действия:

a. В таблице на закладке **Необработанные файлы** выберите один или несколько необработанных файлов, которые вы хотите восстановить. Чтобы выбрать несколько файлов, выделяйте их, удерживая клавишу **CTRL**.

b. Восстановите файлы одним из следующих способов:

- Нажмите на кнопку **Восстановить**.
- По правой клавише мыши откройте контекстное меню. Выберите пункт **Восстановить**.

Программа переместит выбранные файлы в папки их исходного размещения, если эти папки доступны для записи.

c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, то откроется стандартное окно Microsoft Windows **Сохранить как**. В этом окне вы можете указать папку для сохранения файла.

Удаление файлов из списка необработанных файлов

Вы можете удалить зараженный файл, помещенный в список необработанных файлов. Перед тем как удалить файл, Kaspersky Security создает резервную копию файла и сохраняет ее в резервном хранилище на тот случай, если впоследствии вам потребуется восстановить файл (см. раздел «Восстановление файлов из резервного хранилища» на стр. 259).

► *Чтобы удалить файлы из списка необработанных файлов, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

3. Выберите закладку **Необработанные файлы**.

4. В таблице на закладке **Необработанные файлы** выберите один или несколько файлов, которые вы хотите удалить. Чтобы выбрать несколько файлов, выделяйте их, удерживая клавишу **CTRL**.

5. Удалите файлы одним из следующих способов:

   - Нажмите на кнопку **Удалить**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Удалить**.

   Kaspersky Security создает для каждого файла резервную копию и сохраняет ее в резервном хранилище (см. раздел «О резервном хранилище» на стр. 255). После этого Kaspersky Security удаляет выбранные файлы из списка необработанных файлов.

Обновление баз и модулей программы

Этот раздел содержит информацию об обновлении баз и модулей программы (далее также «обновления») и инструкции о том, как настроить параметры обновления.

В этом разделе

Об обновлении баз и модулей программы

Обновление баз и модулей программы обеспечивает актуальность защиты вашей виртуальной машины. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Security. Базы программы регулярно пополняются записями о новых угрозах и способах борьбы с угрозами. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на защищенной виртуальной машине. Чтобы программа Kaspersky Security своевременно обнаруживала новые угрозы, нужно регулярно обновлять базы и модули программы.

Обновления баз и модулей программы могут изменить некоторые параметры программы Kaspersky Security, например, параметры эвристического анализа, повышающие эффективность защиты и проверки.

Kaspersky Security периодически проверяет наличие пакета обновлений в папке на SVM, к которой подключена защищенная виртуальная машина (подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). При наличии пакета обновлений программа устанавливает на защищенной виртуальной машине обновления баз и модулей, необходимых для работы программы.

Для обновления баз и модулей программы требуется действующая лицензия на использование программы.

Обновление баз и модулей программы выполняется с помощью задачи обновления. Запуск задачи обновления выполняется автоматически. При необходимости вы можете запустить задачу обновления вручную (см. раздел «Запуск и остановка задачи обновления» на стр. 238) или настроить расписание запуска задачи обновления.

Если базы и модули программы давно не обновлялись, сообщение об этом появляется в блоке **Управление задачами** закладки **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 23).

Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время виртуальная машина выключена), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта программы для тех случаев, когда вы настроили запуск задачи обновления по расписанию и время запуска Kaspersky Security совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Security.

Информация о результатах обновления и обо всех событиях, произошедших во время выполнения задачи обновления, записывается в отчет Kaspersky Security.

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Security в любой момент.

► *Чтобы запустить или остановить задачу обновления, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. Выберите закладку **Центр управления**.

3. Раскройте блок **Управление задачами**.

4. По правой клавише мыши откройте контекстное меню строки с названием задачи **Обновление**.

   Откроется меню действий с задачей обновления.

   > Если в блоке отсутствуют задачи обновления, это означает, что настройка параметров обновления баз и модулей программы запрещена политикой для всех защищенных виртуальных машин группы администрирования (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Запустить обновление**, если вы хотите запустить задачу обновления.

     Статус выполнения задачи обновления, отображающийся справа от названия задачи **Обновление**, изменится на *Выполняется*.

   - Выберите в меню пункт **Остановить обновление**, если вы хотите остановить задачу обновления.

     Статус выполнения задачи обновления, отображающийся справа от названия задачи **Обновление**, изменится на *Остановлено*.

После запуска задачи обновления процесс ее выполнения отображается в поле напротив названия задачи **Обновление** в блоке **Управление задачами** на закладке **Центр управления** главного окна программы.

Выбор режима запуска задачи обновления

► *Чтобы выбрать режим запуска задачи обновления, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.

   > Если в блоке отсутствует раздел **Обновление**, это означает, что настройка параметров обновления баз и модулей программы запрещена политикой для всех защищенных виртуальных машин группы администрирования (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

3. Нажмите на кнопку **Режим запуска**.

   Откроется окно **Обновление**.

4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи обновления:

   - Выберите вариант **Автоматически**, если вы хотите, чтобы программа Kaspersky Security запускала задачу обновления в зависимости от наличия пакета обновлений на SVM, к которой подключена защищенная виртуальная машина (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Частота проверки программой наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.

     > Если новых обновлений на SVM нет, то задача обновления не запустится.

- Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.
- Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи обновления.

5. Выполните одно из следующих действий:
   - Если вы выбрали вариант **Автоматически** или **Вручную**, перейдите к пункту 6 этой инструкции.
   - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи обновления. Для этого выполните следующие действия:
     a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу обновления. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **Каждый месяц**, **После запуска программы**, **В указанное время**.
     b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи обновления.

        При настройке периодичности запуска задачи обновления рекомендуется учитывать периодичность обновления баз программы на SVM, к которой подключена защищенная виртуальная машина (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

     c. В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта программы Kaspersky Security.

        Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы**, поле **Отложить запуск после старта программы на** недоступно.

     d. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы программа Kaspersky Security запускала при первой возможности не запущенные вовремя задачи обновления.

Если в раскрывающемся списке **Периодичность** выбран элемент **Часы**, **Минуты** или **После запуска программы**, то флажок **Запускать пропущенные задачи** недоступен.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Доверенная зона

Этот раздел содержит информацию о доверенной зоне и инструкции о том, как настроить исключения из проверки и сформировать список доверенных программ.

В этом разделе

О доверенной зоне

Доверенная зона – это сформированный вами список объектов и программ, которые программа Kaspersky Security не контролирует в процессе работы. Иначе говоря, это набор исключений из проверки и защиты.

Доверенную зону вы формируете в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных в гостевой операционной системе защищенной виртуальной машины. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны.

Вы можете исключать из проверки объекты следующих типов:

- файлы определенного формата;
- файлы по маске;
- папки;
- программы;
- процессы программ;
- объекты по классификации Вирусной энциклопедии «Лаборатории Касперского».

Исключения из проверки и защиты

Исключение – это совокупность условий, описывающих объект или программу. Если объект удовлетворяет этим условиям, Kaspersky Security не проверяет этот объект на вирусы и другие программы, представляющие угрозу.

Некоторые легальные программы могут быть использованы злоумышленниками для нанесения вреда вашей виртуальной машине или вашим данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы в качестве вспомогательного компонента вредоносной программы. К таким программам относятся, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, различные утилиты для остановки процессов или сокрытия их работы, клавиатурные перехватчики, программы вскрытия паролей, программы автоматического дозвона. Это программное обеспечение не классифицируется как вирусы. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии «Лаборатории Касперского» по ссылке https://securelist.ru/threats/riskware/.

В результате работы Kaspersky Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить исключения из защиты и проверки Kaspersky Security. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии «Лаборатории Касперского». Например, вы часто используете в своей работе программу Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. Чтобы исключить блокировку этой программы, нужно создать исключение, где указать название или маску названия по классификации Вирусной энциклопедии «Лаборатории Касперского».

Исключения могут использоваться в ходе работы следующих компонентов и задач программы:

- Файловый Антивирус.
- Почтовый Антивирус.
- Веб-Антивирус.
- Мониторинг системы.

- Контроль активности программ.
- Задачи проверки.

Список доверенных программ

Список доверенных программ – это список программ, для которых Kaspersky Security не контролирует файловую и сетевую активность (в том числе и подозрительную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Security исключает из проверки программу, добавленную в список доверенных программ (см. раздел «Формирование списка доверенных программ» на стр. 251).

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вы можете добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Security классифицирует как опасные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера программой Kaspersky Security и другой антивирусной программой), а также увеличить производительность виртуальной машины, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других вредоносных программ. Чтобы полностью исключить программу из проверки и защиты Kaspersky Security, требуется создать исключение для этой программы.

Если на вашей виртуальной машине установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, добавив ее в исключения.

Настройка доверенной зоны

Вы можете выполнить следующие действия для настройки доверенной зоны:

- Создать новое исключение.

  Вы можете создать новое исключение, при выполнении которого Kaspersky Security не проверяет указанные файлы или папки и / или объекты с указанным именем.

- Приостановить использование исключения.

  Вы можете временно приостановить использование исключения, не удаляя его из списка исключений.

- Изменить параметры существующего исключения.

  После того как вы создали новое исключение, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Удалить исключение.

  Вы можете удалить исключение, если вы не хотите, чтобы программа Kaspersky Security применяла исключение во время защиты и проверки виртуальной машины.

- Сформировать список доверенных программ.

  Вы можете сформировать список доверенных программ, для которых Kaspersky Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру.

- Приостановить исключение из проверки Kaspersky Security доверенной программы.

  Вы можете временно приостановить исключение доверенной программы из проверки программой Kaspersky Security, не удаляя ее из списка доверенных программ.

В этом разделе

Создание исключения

Kaspersky Security не проверяет исключенный объект, если при запуске одной из задач проверки указан жесткий диск или папка, в которой находится объект. Но если вы запустили задачу выборочной проверки для объекта, Kaspersky Security проверяет объект, даже если для этого объекта создано исключение.

► *Чтобы создать исключение, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение**.

5. Если вы хотите исключить из защиты и проверки файл или папку, выполните следующие действия:

    a. В блоке **Свойства** установите флажок **Файл или папка**.

    b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения**, откройте окно **Название файла или папки**. В этом окне вы можете ввести название файла или папки, маску названия файла или папки или выбрать файл или папку в дереве папок.

    c. После выбора объекта нажмите на кнопку **ОК** в окне **Название файла или папки**.

    Ссылка на добавленный объект появится в блоке **Описание исключения** окна **Исключения**.

6. Если вы хотите исключить из защиты и проверки объекты с определенным названием на основании классификации вредоносных и других программ, описанных в Вирусной энциклопедии «Лаборатории Касперского», выполните следующие действия:

    a. В блоке **Свойства** установите флажок **Название объекта**.

    b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения**, откройте окно **Название объекта**. В этом окне вы можете ввести название или маску названия объекта согласно классификации Вирусной энциклопедии «Лаборатории Касперского».

    c. Нажмите на кнопку **ОК** в окне **Название объекта**.

7. В поле **Комментарий** введите краткий комментарий к создаваемому исключению.

8. Определите компоненты программы Kaspersky Security, в работе которых должно быть использовано исключение:

    a. По ссылке **любые**, расположенной в блоке **Описание исключения**, откройте ссылку **выберите компоненты**.

    b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.

c. Выберите нужные компоненты.

d. Нажмите на кнопку **ОК** в окне **Компоненты защиты**.

Если компоненты указаны в параметрах исключения, то объект не проверяется только этими компонентам Kaspersky Security.

Если компоненты не указаны в параметрах исключения, то объект не проверяется всеми компонентами Kaspersky Security.

9. Нажмите на кнопку **ОК** в окне **Исключение**.

Добавленное исключение появится в списке исключений закладки **Исключения** окна **Доверенная зона**. В блоке **Описание исключения** отобразятся заданные параметры этого исключения.

10. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение исключения

► *Чтобы изменить исключение, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части выберите блок **Антивирусная защита**.

В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

Откроется окно **Доверенная зона** на закладке **Исключения**.

4. В списке исключений выберите нужное исключение.

5. Нажмите на кнопку **Изменить**.

Откроется окно **Исключение**.

6. Измените параметры исключения.

7. Нажмите на кнопку **ОК** в окне **Исключение**.

   В блоке **Описание исключения** отобразятся измененные параметры этого исключения.

8. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление исключения

► *Чтобы удалить исключение, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.

4. В списке исключений выберите нужное исключение.

5. Нажмите на кнопку **Удалить**.

   Удаленное исключение исчезнет из списка исключений закладки **Исключения** окна **Доверенная зона**.

6. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка использования исключения

► *Чтобы запустить или остановить использование исключения, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения**.
4. В списке исключений выберите нужное исключение.
5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием исключения, если вы хотите использовать это исключение.
   - Снимите флажок рядом с названием исключения, если вы хотите временно приостановить использование этого исключения.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка доверенных программ

► *Чтобы сформировать список доверенных программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

4. Выберите закладку **Доверенные программы**.

5. Если вы хотите добавить программу в список доверенных программ, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В раскрывшемся контекстном меню выполните одно из следующих действий:

      - Выберите пункт **Программы**, если хотите найти программу в списке программ, установленных на виртуальной машине. Откроется окно **Выбор программы**.
      - Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу нужной программы. Откроется стандартное окно Microsoft Windows **Открыть**.

   c. Выберите программу, которую вы хотите добавить в список доверенных программ.

      Откроется окно **Исключения для программы**.

   d. Установите флажки напротив нужных видов активности программы:

      - **Не проверять открываемые файлы**.
      - **Не контролировать активность программы**.
      - **Не наследовать ограничения родительского процесса (программы)**.
      - **Не контролировать активность дочерних программ**.
      - **Разрешать взаимодействие с интерфейсом программы**.
      - **Не проверять сетевой трафик**.

   e. Нажмите на кнопку **ОК** в окне **Исключения для программы**.

      В списке доверенных программ появится добавленная доверенная программа.

6. Если вы хотите изменить параметры доверенной программы, выполните следующие действия:

   a. Выберите доверенную программу в списке доверенных программ.

b. Нажмите на кнопку **Изменить**.

c. Откроется окно **Исключения для программы**.

d. Измените статусы флажков для требуемых видов активности программы.

> Если в окне **Исключения для программы** не выбран ни один из видов активности программы, то происходит включение доверенной программы в проверку (см. раздел «Включение и исключение доверенной программы из проверки» на стр. 253). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снят.

e. Нажмите на кнопку **ОК** в окне **Исключения для программы**.

7. Если вы хотите удалить доверенную программу из списка доверенных программ, выполните следующие действия:

   a. Выберите доверенную программу в списке доверенных программ.

   b. Нажмите на кнопку **Удалить**.

8. Нажмите кнопку **ОК** в окне **Доверенная зона**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и исключение доверенной программы из проверки

► *Чтобы включить доверенную программу в проверку или исключить доверенную программу из проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

4. Выберите закладку **Доверенные программы**.

5. В списке доверенных программ выберите нужную доверенную программу.

6. Выполните одно из следующих действий:

   - Установите флажок рядом с названием доверенной программы, если хотите исключить ее из проверки программой Kaspersky Security.

   - Снимите флажок рядом с названием доверенной программы, если хотите включить ее в проверку программой Kaspersky Security.

7. Нажмите на кнопку **ОК**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Резервное хранилище

Этот раздел содержит инструкции о том, как работать с резервным хранилищем.

В этом разделе

О резервном хранилище

Резервное хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его вылеченной резервной копии в папку исходного размещения файла.

При удалении программы файлы резервного хранилища удаляются с защищенной виртуальной машины.

Настройка параметров резервного хранилища

Вы можете выполнить следующие действия для настройки параметров резервного хранилища:

- Настроить максимальный срок хранения резервных копий файлов.

  По умолчанию максимальный срок хранения резервных копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Security удаляет наиболее старые файлы из хранилища. Вы можете отменить ограничение по времени или изменить максимальный срок хранения файлов.

- Настроить максимальный размер резервного хранилища.

  По умолчанию максимальный размер резервного хранилища составляет 100 МБ. После достижения максимального размера Kaspersky Security автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер. Вы можете отменить ограничение на максимальный размер резервного хранилища или изменить максимальный размер.

В этом разделе

Настройка максимального срока хранения файлов в резервном хранилище

► *Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры резервного хранилища** выполните одно из следующих действий:

   - Установите флажок **Хранить файлы не более**, если хотите ограничить срок хранения резервных копий файлов в резервном хранилище. В поле справа от флажка укажите максимальный срок хранения резервных копий файлов в резервном хранилище. По умолчанию максимальный срок хранения резервных копий файлов в резервном хранилище составляет 30 дней.

   - Снимите флажок **Хранить файлы не более**, если хотите отменить ограничение срока хранения резервных копий файлов в резервном хранилище.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка максимального размера резервного хранилища

► *Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.

3. Выполните одно из следующих действий:

   - В правой части окна в блоке **Параметры резервного хранилища** установите флажок **Максимальный размер хранилища**, если хотите ограничить размер резервного хранилища. В поле справа от флажка укажите максимальный размер резервного хранилища. По умолчанию максимальный размер составляет 100 МБ.

   - В правой части окна в блоке **Параметры резервного хранилища** снимите флажок **Максимальный размер хранилища**, если хотите отменить ограничение на размер резервного хранилища.

   По умолчанию ограничение размера резервного хранилища выключено.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с резервным хранилищем

Если в файле обнаружен вредоносный код, Kaspersky Security блокирует файл, удаляет его из папки исходного размещения, затем помещает его копию в резервное хранилище и пытается провести лечение файла. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. После этого вы можете восстановить файл из его вылеченной резервной копии в папку исходного размещения.

> В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Security не помещает файл в резервное хранилище, а сразу удаляет его. Восстановить целостность приложения Windows Store вы можете средствами операционной системы Microsoft Windows.

Kaspersky Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах программы (см. раздел «Настройка максимального срока хранения файлов в резервном хранилище» на стр. 256).

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла.

Список резервных копий файлов представлен в виде таблицы.

Работая с резервным хранилищем, вы можете выполнять следующие действия с резервными копиями файлов:

- просматривать список резервных копий файлов;
- восстанавливать файлы из резервных копий в папки их исходного размещения;
- удалять резервные копии файлов из резервного хранилища.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать список резервных копий файлов по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска резервных копий файлов;
- сортировать резервные копии файлов;

- группировать резервные копии файлов;
- изменять порядок и набор граф, отображаемых в списке резервных копий файлов;
- копировать выбранные резервные копии файлов в буфер обмена.

В этом разделе

Восстановление файлов из резервного хранилища

Рекомендуется восстанавливать файлы из резервных копий только в том случае, если им присвоен статус *Вылечен*.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Резервное хранилище**.
4. Если вы хотите восстановить все файлы из резервного хранилища, выполните следующие действия:
   a. Откройте контекстное меню по правой клавише мыши в любом месте таблицы на закладке **Резервное хранилище**.
   b. Выберите пункт **Восстановить все**.

   Kaspersky Security восстановит все файлы из их резервных копий в папки их исходного размещения.

5. Если вы хотите восстановить один или несколько файлов из резервного хранилища, выполните следующие действия:

   a. В таблице на закладке **Резервное хранилище** выберите одну или несколько резервных копий файлов. Чтобы выбрать несколько резервных копий, выделяйте их, удерживая клавишу **CTRL**.

   b. Восстановите файлы одним из следующих способов:

      - Нажмите на кнопку **Восстановить**.
      - Откройте контекстное меню по правой клавише мыши и выберите пункт **Восстановить**.

   Kaspersky Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

► *Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. Выберите закладку **Резервное хранилище**.
4. Если вы хотите удалить все резервные копии файлов из резервного хранилища, выполните одно из следующих действий:

   - Откройте контекстное меню по правой клавише мыши в любом месте таблицы на закладке **Резервное хранилище** и выберите пункт **Очистить хранилище**.
   - Нажмите на кнопку **Очистить хранилище**.

5. Если вы хотите удалить одну или несколько резервных копий файлов из резервного хранилища, выполните следующие действия:

   a. В таблице на закладке **Резервное хранилище** выберите одну или несколько резервных копий файлов. Чтобы выбрать несколько резервных копий, выделяйте их, удерживая клавишу **CTRL**.

   b. Удалите резервные копии файлов одним из следующих способов:

      - Нажмите на кнопку **Удалить**.
      - Откройте контекстное меню по правой клавише мыши и выберите пункт **Удалить**.

Работа с отчетами

Этот раздел содержит инструкции о том, как настроить параметры отчетов и как работать с отчетами.

В этом разделе

Принципы работы с отчетами

Информация о работе каждого компонента Kaspersky Security, выполнении каждой задачи проверки и задачи обновления, а также о работе программы в целом фиксируется в отчете.

Данные в отчете представлены в виде таблицы, которая содержит список событий. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. События, зарегистрированные в работе разных компонентов или задач, имеют разный набор атрибутов.

Вы можете сформировать отчеты следующих типов:

- Отчет «Системный аудит». Содержит информацию о событиях, возникающих в процессе вашего взаимодействия с программой, а также в ходе работы программы в целом и не относящихся к какому-либо отдельному компоненту или задаче Kaspersky Security.
- Отчет «Все компоненты защиты». Содержит информацию о событиях, возникающих в ходе работы следующих компонентов Kaspersky Security:
  - Файловый Антивирус.
  - Почтовый Антивирус.
  - Веб-Антивирус.
  - IM-Антивирус.
  - Мониторинг системы.
  - Сетевой экран.
  - Защита от сетевых атак.
- Отчет о работе компонента или задачи Kaspersky Security. Содержит информацию о событиях, возникающих в ходе работы выбранных компонента или задачи.

Выделяют следующие уровни важности событий:

- Значок  . **Информационные события**. События справочного характера, как правило, не содержащие важной информации.
- Значок  . **Важные события**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе программы.
- Значок  . **Критические события**. События критической важности и отказа функционирования программы, указывающие на проблемы в работе программы.

Вы можете выполнять следующие действия с данными отчетов:

- фильтровать список событий по значениям граф или по условиям сложного фильтра;

- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе;
- отображать и скрывать сгруппированные данные;
- изменять порядок и набор граф, отображаемых в отчете;
- сохранять сформированный отчет в текстовый файл.

Также вы можете удалять информацию из отчетов по компонентам и задачам программы, объединенным в группы. Kaspersky Security удаляет все записи выбранных отчетов от наиболее ранней записи до момента инициирования удаления.

Настройка параметров отчетов

Вы можете выполнить следующие действия для настройки параметров отчетов:

- Настроить максимальный срок хранения отчетов.

  По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых программой, составляет 30 дней. По истечении этого времени Kaspersky Security автоматически удаляет наиболее старые записи из файла отчета. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

- Настроить максимальный размер файла отчета.

  Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Security автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы не превышался максимальный размер файла отчета. Вы можете отменить ограничение на размер файла отчета или установить другое значение.

В этом разделе

Настройка максимального срока хранения отчетов

► *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры отчетов** выполните одно из следующих действий:

   - Установите флажок **Хранить отчеты не более**, если хотите ограничить срок хранения отчетов. В поле справа от флажка **Хранить отчеты не более** укажите максимальный срок хранения отчетов. По умолчанию максимальный срок хранения отчетов составляет 30 дней.

   - Снимите флажок **Хранить отчеты не более**, если хотите отменить ограничение срока хранения отчетов.

   По умолчанию ограничение срока хранения отчетов включено.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка максимального размера файла отчета

► *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры отчетов** выполните одно из следующих действий:

   - Установите флажок **Максимальный размер файла**, если хотите ограничить размер файла отчета. В поле справа от флажка **Максимальный размер файла** укажите максимальный размер файла отчета. По умолчанию ограничение размера файла отчета составляет 1024 МБ.

   - Снимите флажок **Максимальный размер файла**, если хотите отменить ограничение на размер файла отчета.

   По умолчанию ограничение размера файла отчета включено.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование отчетов

► *Чтобы сформировать отчеты, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит».

3. Если вы хотите сформировать отчет «Все компоненты защиты», выберите пункт **Все компоненты защиты** в левой части окна **Отчеты и хранилища** в списке компонентов и задач в разделе **Антивирусная защита**.

   В правой части окна отобразится отчет «Все компоненты защиты», содержащий список событий о работе всех компонентов защиты Kaspersky Security.

4. Если вы хотите сформировать отчет о работе компонента или задачи, в левой части окна **Отчеты и хранилища** в списке компонентов и задач выберите нужный компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Security.

   По умолчанию события в отчете отсортированы по возрастанию значений графы **Дата события**.

Просмотр информации о событии отчета в отдельном блоке

Вы можете посмотреть подробную информацию о событии отчета, представленную в отдельном блоке.

► *Чтобы просмотреть информацию о событии отчета в отдельном блоке, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит».

3. Выполните одно из следующих действий:

   - Если вы хотите сформировать отчет «Все компоненты защиты», в списке компонентов и задач выберите пункт **Все компоненты защиты**.

     В правой части окна отобразится отчет «Все компоненты защиты», содержащий список событий о работе всех компонентов защиты.

- Если вы хотите сформировать отчет о работе определенного компонента или задачи, выберите этот компонент или задачу в списке компонентов и задач.

  В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи.

4. Если требуется, воспользуйтесь функциями фильтрации, поиска и сортировки, чтобы найти нужное событие в отчете.

5. Выберите найденное событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события и информацию о его уровне важности.

Сохранение отчета в файл

Вы можете сохранить сформированный отчет в файл текстового формата TXT или CSV.

> Kaspersky Security сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть, с тем же составом и с той же последовательностью атрибутов события.

► *Чтобы сохранить отчет в файл, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит».

3. Выполните одно из следующих действий:

   - Если вы хотите сформировать отчет «Все компоненты защиты», в списке компонентов и задач выберите пункт **Все компоненты защиты**.

     В правой части окна отобразится отчет «Все компоненты защиты», содержащий список событий о работе всех компонентов защиты.

- Если вы хотите сформировать отчет о работе определенного компонента или задачи, выберите этот компонент или задачу в списке компонентов и задач.

  В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи.

4. Если требуется, измените представление данных в отчете, используя следующие возможности:

   - фильтрация событий;
   - поиск событий;
   - изменение расположения граф;
   - сортировка событий.

5. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.

   Откроется контекстное меню.

6. В контекстном меню выберите нужную кодировку для сохранения файла отчета: **Сохранить в ANSI** или **Сохранить в Unicode**.

   Откроется стандартное окно Microsoft Windows **Сохранить как**.

7. В открывшемся окне **Сохранить как** укажите папку, в которую вы хотите сохранить файл отчета.

8. В поле **Имя файла** введите название файла отчета.

9. В поле **Тип файла** выберите нужный формат файла отчета: TXT или CSV.

10. Нажмите на кнопку **Сохранить**.

Удаление информации из отчетов

► *Чтобы удалить информацию из отчетов, выполните следующие действия*:

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.
3. В правой части окна в блоке **Параметры отчетов** нажмите на кнопку **Удалить отчеты**.

   Откроется окно **Удаление информации из отчетов**.
4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:
   - **Все отчеты**.
   - **Общий отчет защиты**. Содержит информацию о работе следующих компонентов Kaspersky Security:
     - Файловый Антивирус.
     - Почтовый Антивирус.
     - Веб-Антивирус.
     - IM-Антивирус.
     - Сетевой экран.
     - Защита от сетевых атак.
   - **Отчет задач проверки**. Содержит информацию о выполненных задачах проверки:
     - Полная проверка.
     - Проверка важных областей.
     - Выборочная проверка.
   - **Отчет задач обновления**. Содержит информацию о выполненных задачах обновления.

- **Отчет обработки правил Сетевого экрана**. Содержит информацию о работе Сетевого экрана.
- **Отчет компонентов контроля**. Содержит информацию о работе следующих компонентов Kaspersky Security:
  - Контроль запуска программ.
  - Контроль активности программ.
  - Контроль устройств.
  - Веб-Контроль.
- **Данные Мониторинга системы**. Содержит информацию о работе компонента Мониторинг системы.

5. Нажмите на кнопку **ОК**.

Уведомления

Этот раздел содержит информацию об уведомлениях, оповещающих о событиях в работе Kaspersky Security, а также инструкции о том, как настроить уведомления о событиях.

В этом разделе

Об уведомлениях Kaspersky Security

В процессе работы Kaspersky Security возникают различного рода события. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события программа может уведомлять об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую требуется устранить.

Kaspersky Security может уведомлять о событиях одним из следующих способов:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Вы можете настроить способы уведомления о событиях. Способ уведомления настраивается для каждого типа событий.

Kaspersky Security позволяет также сохранять информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в отчеты программы (см. стр. 262).

Настройка уведомлений

Вы можете выполнить следующие действия для настройки уведомлений:

- настроить сохранение событий о работе Kaspersky Security (см. раздел «Настройка сохранения событий» на стр. 273);
- настроить отображение уведомлений на экране (см. раздел «Настройка отображения уведомлений на экране» на стр. 274);
- настроить уведомления о событиях по электронной почте (см. раздел «Настройка уведомлений о событиях по электронной почте» на стр. 275).

Работая с таблицей событий, вы можете выполнять следующие действия:

- использовать функцию поиска событий;
- сортировать события по возрастанию и убыванию;
- изменять набор граф, отображаемых в списке событий.

В этом разделе

Настройка сохранения событий

► *Чтобы настроить сохранение событий, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

4. Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Security. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.

5. В левой части окна выберите компонент или задачу, для которой вы хотите настроить сохранения событий.

6. В графах установите флажки напротив нужных типов событий:

   - **Сохранять в журнале программы**, если вы хотите сохранять события в отчетах программы (см. стр. 262).

   - **Сохранять в журнале событий Windows**, если вы хотите сохранять события в журнале событий Microsoft Windows.

7. Нажмите на кнопку **ОК** в окне **Уведомления**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка отображения уведомлений на экране

► *Чтобы настроить отображение уведомлений на экране, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.

3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

4. Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Security. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.

5. В левой части окна выберите компонент или задачу, для которой вы хотите настроить уведомления о событиях на экране.

6. В графе **Уведомлять на экране** установите флажки напротив нужных типов событий.

Информация о выбранных событиях будет отображаться на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.

Настройка уведомлений о событиях по электронной почте

► *Чтобы настроить уведомления о событиях по электронной почте, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.

3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

4. Откроется окно **Уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Security. В правой части окна отображается список событий, сформированный для выбранного компонента или задачи.

5. В левой части окна выберите компонент или задачу, для которой вы хотите настроить уведомления о событиях по электронной почте.

6. В графе **Уведомлять по почте** установите флажки напротив нужных типов событий.

7. Нажмите на кнопку **Настройка почтовых уведомлений**.

   Откроется окно **Настройка почтовых уведомлений**.

8. Установите флажок **Отправлять уведомления о событиях**, чтобы включить отправку информации о событиях в работе Kaspersky Security, отмеченных в графе **Уведомлять по почте**.

9. Укажите параметры отправки почтовых уведомлений.

10. Нажмите на кнопку **ОК** в окне **Настройка почтовых уведомлений**.

11. Нажмите на кнопку **ОК** в окне **Уведомления**.

12. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Производительность программы Kaspersky Security

Этот раздел содержит информацию о производительности программы Kaspersky Security и совместимости с другими программами, а также инструкции о том, как выбрать тип обнаруживаемых объектов и режим работы Kaspersky Security.

В этом разделе

О производительности программы Kaspersky Security

Под производительностью Kaspersky Security подразумевается количество обнаруживаемых типов объектов, а также потребление ресурсов защищенной виртуальной машины.

Выбор типов обнаруживаемых объектов

Kaspersky Security позволяет гибко настраивать защиту виртуальной машины и выбирать типы объектов (см. раздел «Выбор типов обнаруживаемых объектов» на стр. 279), которые программа обнаруживает в ходе работы. Kaspersky Security всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов. Такие программы могут нанести значительный вред защищенной виртуальной машине. Чтобы обеспечить большую безопасность виртуальной машины, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда вашей виртуальной машине или вашим данным.

Применение технологии лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Security выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения (см. раздел «Включение и выключение технологии лечения активного заражения для настольных операционных систем» на стр. 280). *Технология лечения активного заражения* направлена на лечение операционной системы от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают программе Kaspersky Security удалить их с помощью других методов. В результате применения технологии лечения активного заражения угроза нейтрализуется. В процессе лечения активного заражения не рекомендуется запускать новые процессы или изменять реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения на виртуальной машине с настольной операционной системой Windows Kaspersky Security запрашивает разрешение на перезагрузку виртуальной машины. После перезагрузки виртуальной машины Kaspersky Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку виртуальной машины.

> Если Kaspersky Security работает на временной виртуальной машине, в случае активного заражения этой временной виртуальной машины требуется убедиться в отсутствии вирусов и других вредоносных программ на шаблоне виртуальной машины и выполнить перезагрузку временной виртуальной машины.

Запрос перезагрузки на виртуальной машине с серверной операционной системой Windows невозможен из-за особенностей программы Kaspersky Security для серверных операционных систем. Незапланированная перезагрузка серверной операционной системы может повлечь за собой проблемы, связанные с временным отказом доступа к данным серверной операционной системы или потерей несохраненных данных.

Перезагрузку серверной операционной системы рекомендуется выполнять по расписанию. Поэтому по умолчанию технология лечения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows выключена.

В случае обнаружения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на защищенной виртуальной машине с серверной операционной системой Windows нужно включить технологию лечения активного заражения для серверных операционных систем и запустить групповую задачу поиска вирусов в удобное для пользователей серверной операционной системы время (см. подробнее в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

Выбор типов обнаруживаемых объектов

► *Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Объекты** нажмите на кнопку **Настройка**.

   Откроется окно **Объекты для обнаружения**.
4. Установите флажки для типов объектов, которые должна обнаруживать программа Kaspersky Security:
   - **Вредоносные утилиты**.
   - **Рекламные программы**.
   - **Программы автодозвона**.
   - **Другие**.
   - **Упакованные файлы**.
   - **Многократно упакованные файлы**.

   Обратите внимание, что обнаруженные объекты могут быть удалены программой.

5. Нажмите на кнопку **ОК** в окне **Объекты для обнаружения**.

   Окно **Объекты для обнаружения** закроется. В блоке **Объекты** под надписью **Включено обнаружение объектов следующих типов** отобразятся выбранные вами типы объектов.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение технологии лечения активного заражения для настольных операционных систем

► *Чтобы включить или выключить технологию лечения активного заражения для настольных операционных систем, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В правой части окна выполните одно из следующих действий:

   - Установите флажок **Применять технологию лечения активного заражения**, если хотите включить технологию лечения активного заражения.
   - Снимите флажок **Применять технологию лечения активного заражения**, если хотите выключить технологию лечения активного заражения.

   Если флажок недоступен, это означает, что вы не можете включить или выключить технологию лечения активного заражения для настольных операционных систем, так как это запрещено политикой для всех защищенных виртуальных машин группы администрирования (см. подробнее в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Самозащита программы Kaspersky Security

Этот раздел содержит информацию о механизмах самозащиты программы Kaspersky Security и защиты от внешнего управления программой и инструкции о том, как настроить параметры этих механизмов.

В этом разделе

О самозащите Kaspersky Security

Программа Kaspersky Security обеспечивает безопасность защищенной виртуальной машины от вредоносных программ, включая вредоносные программы, которые пытаются заблокировать работу Kaspersky Security или удалить программу с виртуальной машины.

Стабильность системы безопасности виртуальной машины обеспечивают реализованные в Kaspersky Security механизмы самозащиты и защиты от внешнего управления.

Механизм самозащиты предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Механизм защиты от внешнего управления позволяет блокировать все попытки управления службами программы с удаленного компьютера.

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Security включен. При необходимости вы можете выключить механизм самозащиты.

Выключение самозащиты снижает уровень защиты виртуальной машины от вредоносных программ.

► *Чтобы включить или выключить механизм самозащиты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите блок **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить самозащиту**, если вы хотите включить механизм самозащиты.
   - Снимите флажок **Включить самозащиту**, если вы хотите выключить механизм самозащиты.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение механизма защиты от внешнего управления

По умолчанию механизм защиты от внешнего управления включен. При необходимости вы можете выключить механизм защиты от внешнего управления.

► *Чтобы включить или выключить механизм защиты от внешнего управления, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части окна выберите блок **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. Выполните одно из следующих действий:
   - Установите флажок **Выключить внешнее управление системной службой**, если вы хотите включить механизм защиты от внешнего управления.
   - Снимите флажок **Выключить внешнее управление системной службой**, если вы хотите выключить механизм защиты от внешнего управления.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить программы удаленного администрирования.

► *Чтобы обеспечить работу программ удаленного администрирования, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.
4. Выберите закладку **Доверенные программы**.
5. Нажмите на кнопку **Добавить**.

6. В раскрывшемся контекстном меню выполните одно из следующих действий:

   - Выберите пункт **Программы**, если хотите найти программу удаленного администрирования в списке установленных на защищенной виртуальной машине программ. Откроется окно **Выбор программы**.

   - Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу программы удаленного администрирования. Откроется стандартное окно Microsoft Windows **Выбор файла или папки**.

7. Выберите программу.

   Откроется окно **Исключения для программы**.

8. Установите флажок **Не контролировать активность программы**.

9. Нажмите на кнопку **ОК** в окне **Исключения для программы**.

   В списке доверенных программ появится добавленная доверенная программа.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита паролем

Этот раздел содержит информацию об ограничении доступа к программе Kaspersky Security с помощью пароля.

В этом разделе

Об ограничении доступа к программе

Виртуальную машину могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к программе Kaspersky Security и ее параметрам может привести к снижению уровня безопасности виртуальной машины в целом.

Чтобы ограничить доступ к программе Kaspersky Security, вы можете задать пароль и указать операции, для выполнения которых программа должна запрашивать пароль:

- все операции (кроме уведомлений об опасности);
- настройка параметров программы;
- завершение работы программы;
- выключение компонентов защиты и остановка задач проверки;
- выключение компонентов контроля;
- удаление / изменение / восстановление программы.

Включение и выключение защиты паролем

► *Чтобы включить или выключить защиту паролем, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 25).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.

3. Если вы хотите ограничить доступ к программе Kaspersky Security с помощью пароля, выполните следующие действия:

   a. В блоке **Защита паролем** установите флажок **Включить защиту паролем**.

   > Если флажок недоступен, это означает, что вы не можете включить или выключить защиту паролем, так как для всех защищенных виртуальных машин группы администрирования используется значение параметра, заданное политикой (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Обратитесь к администратору системы.

   b. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

      Откроется окно **Защита паролем**.

   c. В поле **Новое имя пользователя** введите имя пользователя, от имени которого будет осуществляться доступ к программе.

   d. В поле **Новый пароль** введите пароль для доступа к программе.

   e. В поле **Подтверждение пароля** повторите пароль.

   f. В блоке **Область действия пароля** укажите операции с программой, для выполнения которых пользователь должен ввести пароль:

      - Выберите вариант **Все операции (кроме уведомлений об опасности)**, если хотите ограничить доступ для всех операций с программой.

- Выберите вариант **Отдельные операции**, если хотите указать операции.

g. Если вы выбрали вариант **Отдельные операции**, установите флажки напротив названий нужных операций:

- **Настройка параметров программы**.
- **Завершение работы программы**.
- **Выключение компонентов защиты и остановка задач проверки**.
- **Выключение компонентов контроля**.
- **Удаление / изменение / восстановление программы**.
- **Просмотр отчетов**.

h. Нажмите на кнопку **ОК**.

> Рекомендуется с осторожностью использовать пароль для ограничения доступа к программе. Если вы забыли пароль, то для получения инструкций по отмене защиты паролем вам нужно обратиться в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru).

4. Если вы хотите отменить ограничение доступа к программе Kaspersky Security с помощью пароля, выполните следующие действия:

a. Снимите флажок **Включить защиту паролем**.

b. Нажмите на кнопку **Сохранить**.

Программа проверяет, есть ли защита на операцию отмены ограничения доступа.

- Если операция отмены ограничения доступа к программе не защищена паролем, то ограничение доступа к программе отменяется.
- Если операция отмены ограничения доступа к программе защищена паролем, то откроется окно **Проверка пароля**. Это окно появляется каждый раз, когда пользователь совершает какую-либо операцию, защищенную паролем.

c. В поле **Пароль** окна **Проверка пароля** введите пароль.

d. Установите флажок **Запомнить пароль на текущую сессию работы программы**, если хотите, чтобы во время текущей сессии работы программа не требовала ввода пароля при попытке выполнения этой операции. При следующем запуске программы ограничение доступа к программе будет отменено.

   Снятый флажок **Запомнить пароль на текущую сессию работы программы** означает, что программа запрашивает пароль каждый раз при попытке выполнения этой операции.

e. Нажмите на кнопку **ОК**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление параметрами программы Kaspersky Security

Этот раздел содержит инструкции о том, как перенести настроенные параметры программы Kaspersky Security в программу Kaspersky Security, установленную на другой виртуальной машине, а также как восстановить стандартные параметры работы программы.

В этом разделе

Перенос параметров Kaspersky Security в программу, установленную на другой виртуальной машине

Настроив параметры программы Kaspersky Security, вы можете применить их к программе Kaspersky Security, установленной на другой виртуальной машине. В результате программа Kaspersky Security на обеих виртуальных машинах будет настроен одинаково.

Вы можете сохранить параметры программы в специальном конфигурационном файле в формате CFG, а затем перенести конфигурационный файл с одной виртуальной машины на другую.

Конфигурационный файл в формате CFG также используется для импорта параметров при удаленной установке программы и при создании политики для Легкого агента (см. подробнее в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Конфигурационный файл, который используется для импорта параметров при удаленной установке программы, должен иметь название install.cfg.

► *Чтобы перенести параметры Kaspersky Security в программу на другой виртуальной машине, выполните следующие действия:*

1. Сохраните текущие параметры программы Kaspersky Security в конфигурационный файл следующим образом:

   a. Откройте окно настройки параметров программы (на стр. 25).

   b. В левой части окна выберите блок **Дополнительные параметры**.

      В правой части окна отобразятся дополнительные параметры программы.

   c. В блоке **Управление параметрами** нажмите на кнопку **Сохранить**.

      Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.

   d. Введите название конфигурационного файла и укажите место его сохранения.

   e. Нажмите на кнопку **Сохранить**.

2. Перенесите сохраненный конфигурационный файл на другую виртуальную машину (например, отправьте по электронной почте или переместите на съемном диске).

3. На другой виртуальной машине загрузите параметры работы программы в программу Kaspersky Security из конфигурационного файла следующим образом:

   a. Откройте окно настройки параметров программы.

   b. В левой части окна выберите блок **Дополнительные параметры**.

      В правой части окна отобразятся дополнительные параметры программы.

   c. В блоке **Управление параметрами** нажмите на кнопку **Загрузить**.

      Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.

   d. Выберите файл, из которого вы хотите импортировать параметры программы.

   e. Нажмите на кнопку **Открыть**.

   f. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Восстановление стандартных параметров программы

На основе информации об операционной системе и установленных на защищенной виртуальной машине программах специалисты «Лаборатории Касперского» рекомендуют вам оптимальные параметры защиты виртуальной машины. В процессе работы с программой Kaspersky Security вы всегда можете восстановить стандартные параметры программы. Восстановление параметров выполняется с помощью мастера первоначальной настройки программы.

► *Чтобы восстановить стандартные параметры программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы.
2. В левой части окна выберите блок **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. В блоке **Управление параметрами** нажмите на кнопку **Восстановить**.

   Запустится мастер первоначальной настройки программы.
4. В окне **Добро пожаловать** нажмите на кнопку **Далее**, чтобы начать работу мастера первоначальной настройки программы.
5. В окне **Восстановление параметров** представлены компоненты и задачи программы, параметры которых были изменены.

   Если для какого-либо компонента в процессе работы программы были сформированы уникальные параметры, они также отображаются в этом окне. В число уникальных параметров входят, например, списки доверенных веб-адресов, созданные исключения, сетевые правила Сетевого экрана, правила контроля программ и другие.

   Эти уникальные параметры формируются в процессе работы с программой с учетом индивидуальных задач и требований безопасности. Формирование уникальных параметров зачастую занимает много времени, поэтому специалисты «Лаборатории Касперского» рекомендуют сохранять их, иначе все сформированные в процессе работы программы параметры будут утеряны.

Установите флажки для тех компонентов и задач, для которых вы хотите восстановить стандартные параметры.

6. Нажмите на кнопку **Далее**.

7. На следующем этапе мастер первоначальной настройки программ анализирует информацию о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ (см. раздел «Формирование списка доверенных программ» на стр. 251), которые не имеют ограничений на действия, совершаемые в операционной системе. Выполнение анализа информации отображается в окне **Анализ системы**.

   Завершив анализ операционной системы, мастер первоначальной настройки программы автоматически переходит к следующему шагу.

8. Нажмите на кнопку **Завершить** в окне **Завершение первоначальной настройки программы**.

   Мастер первоначальной настройки программы закроется, стандартные параметры программы восстановятся.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как проверить подключение к Kaspersky Security Network.

В этом разделе

Об участии в Kaspersky Security Network

Чтобы повысить эффективность защиты виртуальной машины, Kaspersky Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных базы Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security на неизвестные угрозы и повышает эффективность работы некоторых компонентов защиты.

Участие пользователей в Kaspersky Security Network позволяет «Лаборатории Касперского» оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний.

В зависимости от расположения инфраструктуры различают:

- Глобальный KSN (Global Kaspersky Security Network) – инфраструктура расположена на серверах «Лаборатории Касперского».
- Локальный KSN (Kaspersky Private Security Network) – инфраструктура расположена на сторонних серверах поставщика услуг, например, внутри сети интернет-провайдера.

Настройка использования Локального KSN выполняется в свойствах Сервера администрирования Kaspersky Security Center в разделе **Прокси-сервер KSN**. См. подробнее в документации Kaspersky Security Center.

Чтобы продолжить использовать Локальный KSN после изменения ключа, требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с KSN невозможен.

Во время использования KSN программа Kaspersky Security автоматически отправляет в Kaspersky Security Network статистическую информацию, полученную в результате своей работы (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*). Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями и действующими правилами «Лаборатории Касперского».

«Лаборатория Касперского» использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно. Более подробную информацию об отправке в «Лабораторию Касперского», хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о KSN и на веб-сайте «Лаборатории Касперского» http://www.kaspersky.ru/privacy.

Участие в Kaspersky Security Network является добровольным. Включение и выключение использования KSN настраивается администратором программы в параметрах политики (см. *Руководство администратора Kaspersky Security для виртуальных сред 4.0 Легкий агент*).

Проверка подключения к Kaspersky Security Network

► *Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 23).

2. В верхней части окна нажмите на кнопку **Kaspersky Security Network**.

   Откроется окно **Kaspersky Security Network**.

   Круглая кнопка **KSN** в левой части окна обозначает режим подключения программы к Kaspersky Security Network:

   - Если программа Kaspersky Security подключена к базе Kaspersky Security Network, кнопка **KSN** имеет зеленый цвет. Под кнопкой **KSN** отображается статус *Включено*, тип используемого KSN: Локальный KSN (KPSN) или Глобальный KSN и дата последней синхронизации с серверами KSN. В правой части окна отображается статистика о репутации файлов и веб-ресурсов.

     > Получение статистических данных по использованию программой Kaspersky Security служб Kaspersky Security Network происходит при открытии окна **Kaspersky Security Network**. Обновление статистики в реальном времени не производится.

   - Если программа Kaspersky Security не подключена к Kaspersky Security Network, то кнопка **KSN** имеет серый цвет. Под кнопкой **KSN** отображается статус *Выключено*.

     Подключение с серверам Kaspersky Security Network может отсутствовать по следующим причинам:

     - программа не активирована или срок действия лицензии истек;
     - служба KSN Proxy выключена в Kaspersky Security Center (см. в документации Kaspersky Security Center).

Глоссарий

K

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ «Лаборатории Касперского» получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network «Лаборатории Касперского» со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

Объект, который присоединен к другому файлу или встроен в другой файл с использованием технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft® Office Excel®, встроенная в документ Microsoft Office Word.

S

SVM

Secure virtual machine, виртуальная машина защиты. Виртуальная машина на гипервизоре, на которой установлен компонент Сервер защиты Kaspersky Security.

А

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

Б

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами «Лаборатории Касперского», регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами «Лаборатории Касперского» как фишинговые. База регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

Базы программы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Базы программы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

З

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами.

Защищенная виртуальная машина

Виртуальная машина, на которой установлен компонент Легкий агент.

К

Клавиатурный перехватчик

Программа, предназначенная для скрытой записи информации о клавишах, нажимаемых пользователем во время работы на компьютере. Клавиатурные перехватчики также называют кейлоггерами.

Л

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный из-за того, что его код напоминает код вируса.

О

Объекты автозапуска

Набор программ, необходимых для запуска и работы установленных на вашей виртуальной машине операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать такие объекты, что может привести, например, к блокированию запуска операционной системы.

Р

Резервная копия файла

Копия файла с виртуальной машины, которая создается при лечении или удалении этого файла. Резервные копии файлов хранятся в резервном хранилище в специальном формате и не представляют опасности.

Резервное хранилище

Специализированное хранилище для резервных копий тех файлов, которые были удалены или изменены в процессе лечения.

С

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы программы «Лаборатории Касперского», содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов «Лаборатории Касперского» этот метод анализа всегда включен.

Составной файл

Составной файл представляет собой несколько отдельных файлов, которые хранятся в одном физическом файле, к каждому из этих файлов можно получить доступ. Примерами составных файлов являются архивы, инсталляционные пакеты, вложенные OLE-объекты, файлы почтовых форматов. Распространенная практика сокрытия вирусов – внедрение их в составные файлы. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать.

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Э

Эвристический анализ

Технология обнаружения угроз, информация о которых еще не занесена в базы программы «Лаборатории Касперского». Позволяет находить файлы, которые могут содержать вредоносную программу, не указанную в базах, или новую модификацию известного вируса.

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 34 офисами в 31 стране 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:	http://newvirus.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

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe и Acrobat – товарные знаки или зарегистрированные в Соединенных Штатах Америки и / или в других странах товарные знаки Adobe Systems Incorporated.

Citrix и XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

FireWire – товарный знак Apple Inc., зарегистрированный в США и других странах.

ICQ – товарный знак и/или знак обслуживания ICQ LLC.

Microsoft, Excel, Hyper-V, Outlook, Windows, Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Thunderbird – товарные знаки Mozilla Foundation.

VMware ESXi – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Предметный указатель

I

K

Б

В

Г

Д

З

И

К

М

О

П

P

C

У

Ф

Э