Kaspersky Internet Security 2012

Руководство пользователя

ВЕРСИЯ ПРОГРАММЫ: 12.0

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 19.04.2011

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Вас приветствуют специалисты «Лаборатории Касперского».

Это руководство содержит сведения по установке, настройке и использованию программы Kaspersky Internet Security. Мы надеемся, что информация, представленная в этом руководстве, поможет вам в работе с программой.

Это руководство предназначено для следующих целей:

- помочь установить Kaspersky Internet Security, активировать и использовать программу;
- обеспечить быстрый поиск информации для решения вопросов, связанных с работой программы;
- рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

Для успешного использования программы вам требуется обладать начальными навыками работы с компьютером: быть знакомыми с интерфейсом используемой операционной системы, владеть основными приемами работы в ней, уметь работать с электронной почтой и интернетом.

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ РУКОВОДСТВЕ

В это руководство включены следующие разделы.

Источники информации о программе

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Kaspersky Internet Security

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

Установка и удаление программы

Этот раздел содержит информацию о том, как установить программу на компьютер, и о том, как удалить программу с компьютера.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

Интерфейс программы

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы и контекстном меню значка программы, главном окне, окне настройки, окнах уведомлений.

Запуск и остановка программы

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

Управление защитой компьютера

Этот раздел содержит информацию о том, как определить наличие угроз безопасности компьютера и настроить уровень его защиты. Из этого раздела вы также узнаете о включении, отключении и временной приостановке защиты во время работы программы.

Решение типовых задач

Этот раздел содержит информацию о том, как решать основные задачи по защите компьютера с помощью программы.

Расширенная настройка программы

Этот раздел содержит подробную информацию о том, как настроить параметры каждого компонента программы.

Проверка работы программы

Этот раздел содержит сведения о том, как проверить работу программы – убедиться в том, что программа обнаруживает вирусы и их модификации и выполняет над ними действия.

Обращение в Службу технической поддержки

Этот раздел содержит сведения о способах обращения в Службу технической поддержки «Лаборатории Касперского».

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Глоссарий

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

ЗАО «Лаборатория Касперского»

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде

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

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

Текст документа сопровождается смысловыми элементами, на которые мы рекомендуем вам обращать особое внимание, – предупреждениями, советами, примерами.

Для выделения смысловых элементов используются условные обозначения. Условные обозначения и примеры их использования приведены в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации или нарушению работы компьютера.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения или важные частные случаи в работе программы.
Пример: ...	Примеры приведены в блоках на желтом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие смысловые 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 нужно 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 пользователю.
`<IP-адрес вашего компьютера>`	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

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

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

- страница на веб-сайте «Лаборатории Касперского»;
- страница на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. 196).

Для использования источников информации на веб-сайте «Лаборатории Касперского» необходимо подключение к интернету.

Страница на веб-сайте «Лаборатории Касперского»

Веб-сайт «Лаборатории Касперского» содержит отдельную страницу для каждой программы.

На странице (http://www.kaspersky.ru/kaspersky_internet_security) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница http://www.kaspersky.ru содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница на веб-сайте Службы технической поддержки (База знаний)

База знаний – раздел веб-сайта Службы технической поддержки, содержащий рекомендации по работе с программами «Лаборатории Касперского». База знаний состоит из справочных статей, сгруппированных по темам.

На странице программы в Базе знаний (http://support.kaspersky.ru/kis2012) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи могут отвечать на вопросы, которые относятся не только к Kaspersky Internet Security, но и к другим программам «Лаборатории Касперского», а также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят файлы справки.

Контекстная справка содержит сведения о каждом окне программы: перечень и описание параметров и список решаемых задач.

Полная справка содержит подробную информацию о том, как управлять защитой компьютера с помощью программы.

Документация

Руководство пользователя программы содержит информацию об установке, активации, настройке параметров программы, а также сведения о работе с программой. В документе приведено описание интерфейса программы, предложены способы решения типовых задач пользователя при работе с программой.

Обсуждение программ «Лаборатории Касперского» на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (http://forum.kaspersky.com).

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

Обращение в Департамент продаж

Если у вас возникли вопросы по выбору, приобретению или продлению срока использования программы, вы можете связаться с нашими специалистами из Департамента продаж одним из следующих способов:

- Позвонив по телефонам нашего центрального офиса в Москве (http://www.kaspersky.ru/contacts).
- Отправив письмо с вопросом по электронной почте sales@kaspersky.com.

Обслуживание осуществляется на русском и английском языках.

Обращение в Группу разработки документации по электронной почте

Для обращения в Группу разработки документации требуется отправить письмо по электронному адресу docfeedback@kaspersky.com. В качестве темы письма нужно указать «Kaspersky Help Feedback: Kaspersky Internet Security».

KASPERSKY INTERNET SECURITY

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

В ЭТОМ РАЗДЕЛЕ

Что нового

В Kaspersky Internet Security появились следующие новые возможности:

- Улучшенный интерфейс главного окна Kaspersky Internet Security обеспечивает быстрый доступ к функциям программы.
- Доработана логика работы с карантином и резервным хранилищем (см. стр. 172): теперь они представлены на двух закладках и выполняют разные функции.
- Для удобного управления задачами Kaspersky Internet Security добавлен Менеджер задач (см. раздел «Управление задачами проверки. Менеджер задач» на стр. 78).
- Участие в Kaspersky Security Network (см. стр. 187) позволяет определять репутацию программ и веб-сайтов на основе данных, полученных от пользователей во всем мире.
- При работе Веб-Антивируса можно отдельно включить эвристический анализ для проверки веб-страниц на наличие фишинга (см. раздел «Использование эвристического анализа при работе Веб-Антивируса» на стр. 100). При этом, при проверке на наличие фишинга эвристический анализ будет использоваться независимо от того, включен ли эвристический анализ для Веб-Антивируса.
- Изменен внешний вид Kaspersky Gadget (см. стр. 41).

Комплект поставки

Вы можете приобрести программу одним из следующих способов:

- **В коробке**. Распространяется через магазины наших партнеров.
- **Через интернет-магазин**. Распространяется через интернет-магазины «Лаборатории Касперского» (например, http://www.kaspersky.ru, раздел **Интернет-магазин**) или компаний-партнеров.

Если вы приобретаете программу в коробке, в комплект поставки входят следующие компоненты:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программы и файлы документации к программе;

- краткое руководство пользователя, содержащее код активации программы;
- лицензионное соглашение, в котором указано, на каких условиях вы можете пользоваться программой.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

Если вы приобретаете Kaspersky Internet Security через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

За подробной информацией о способах приобретения и комплекте поставки вы можете обратиться в Департамент продаж.

Сервис для зарегистрированных пользователей

Приобретая лицензию на использование программы, вы становитесь зарегистрированным пользователем программ «Лаборатории Касперского» и в течение срока действия лицензии можете получать следующие услуги:

- обновление баз и предоставление новых версий программы;
- консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы;
- оповещение о выходе новых программ «Лаборатории Касперского» и о новых вирусах. Для использования этой услуги требуется подписаться на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки.

Консультации по работе операционных систем, стороннего программного обеспечения и технологиям не проводятся.

Аппаратные и программные требования

Для нормального функционирования Kaspersky Internet Security компьютер должен удовлетворять следующим требованиям:

Общие требования:

- 480 МБ свободного места на жестком диске (в том числе 380 МБ на системном диске).
- CD- / DVD-ROM (для установки Kaspersky Internet Security с дистрибутивного CD-диска).
- Подключение к интернету (для активации программы, а также обновления баз и программных модулей).
- Microsoft Internet Explorer 6.0 или выше.
- Microsoft Windows Installer 2.0.

Требования для операционных систем Microsoft Windows XP Home Edition (Service Pack 2 или выше), Microsoft Windows XP Professional (Service Pack 2 или выше), Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше):

- процессор Intel Pentium 800 МГц 32-разрядный (x86) / 64-разрядный (x64) или выше (или совместимый аналог);
- 512 МБ свободной оперативной памяти.

Требования для операционных систем Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- процессор Intel Pentium 1 ГГц 32-разрядный (x86) / 64-разрядный (x64) или выше (или совместимый аналог).
- 1 ГБ свободной оперативной памяти (для 32-разрядной операционной системы); 2 ГБ свободной оперативной памяти (для 64-разрядной операционной системы).

При работе в операционной системе Microsoft Windows XP (64-разрядной) использование безопасной среды невозможно. При работе в операционных системах Microsoft Windows Vista (64-разрядной) и Microsoft Windows 7 (64-разрядной) использование безопасной среды ограничено.

Требования для нетбуков:

- Процессор Intel Atom 1,6 ГГц или совместимый аналог.
- Видеокарта Intel GMA950 с видеопамятью объемом не менее 64 МБ (или совместимый аналог).
- Диагональ экрана не менее 10,1 дюйма.

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит информацию о том, как установить программу на компьютер, и о том, как удалить программу с компьютера.

В ЭТОМ РАЗДЕЛЕ

СТАНДАРТНАЯ ПРОЦЕДУРА УСТАНОВКИ

Kaspersky Internet Security устанавливается на компьютер в интерактивном режиме с помощью Мастера установки.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров зависит от вашей лицензии), то на все компьютеры она устанавливается одинаково. Следует помнить, что в этом случае в соответствии с лицензионным соглашением срок действия лицензии начинается с даты первой активации программы. При активации программы на втором и последующих компьютерах срок действия лицензии будет уменьшаться на тот период времени, который прошел с момента первой активации. Таким образом, срок действия лицензии истечет одновременно для всех установленных копий программы.

- *Чтобы установить Kaspersky Internet Security на ваш компьютер,*

  на CD-диске с продуктом запустите файл дистрибутива (файл с расширением exe).

Процесс установки Kaspersky Internet Security с дистрибутива, полученного через интернет, полностью совпадает с процессом установки программы с дистрибутивного CD-диска.

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Поиск более новой версии программы

Перед установкой проверяется наличие более актуальной версии Kaspersky Internet Security на серверах обновлений «Лаборатории Касперского».

Если более новой версии программы на серверах обновлений «Лаборатории Касперского» не обнаружено, будет запущен мастер установки текущей версии.

Если на серверах обновлений выложена более новая версия Kaspersky Internet Security, вам будет предложено загрузить и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. В случае отказа от более новой версии будет запущен мастер установки текущей версии. Если же вы примете решение установить более новую версию, файлы дистрибутива будут скопированы на ваш компьютер и мастер установки новой версии будет запущен автоматически. Дальнейшее описание установки более новой версии читайте в документации к соответствующей версии программы.

Шаг 2. Проверка соответствия системы необходимым условиям установки

Перед установкой Kaspersky Internet Security на вашем компьютере проверяется соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки (см. раздел «Аппаратные и программные требования» на стр. 18). Помимо этого, проверяется наличие требуемого программного обеспечения, а также прав на установку программного обеспечения. Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

Если компьютер соответствует предъявляемым требованиям, мастер выполняет поиск программ «Лаборатории Касперского», совместное использование с которыми программы Kaspersky Internet Security может привести к возникновению конфликтов. Если такие программы будут найдены, вам будет предложено удалить их вручную.

Если в числе обнаруженных программ есть Антивирус Касперского или Kaspersky Internet Security одной из предыдущих версий, все данные, которые могут быть использованы Kaspersky Internet Security 2012 (например, информация об активации или параметры программы), будут сохранены и использованы при установке, а ранее установленная программа будет автоматически удалена.

Шаг 3. Выбор типа установки

На этом этапе установки вы можете выбрать наиболее подходящий тип установки Kaspersky Internet Security:

- *Стандартная установка*. При выборе этого варианта (флажок **Изменить параметры установки** снят) программа будет полностью установлена на ваш компьютер с параметрами защиты, рекомендуемыми специалистами «Лаборатории Касперского».

- *Установка с возможностью изменения параметров*. В данном случае (флажок **Изменить параметры установки** установлен) вам будет предложено указать папку, в которую будет установлена программа (см. раздел «Шаг 7. Выбор папки назначения» на стр. 22), и при необходимости выключить защиту процесса установки (см. раздел «Шаг 8. Подготовка к установке» на стр. 23).

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 4. Просмотр лицензионного соглашения

На этом этапе следует ознакомиться с лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочтите соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Я согласен**. Установка программы на ваш компьютер будет продолжена.

Если вы не согласны с лицензионным соглашением, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 5. Положение об использовании Kaspersky Security Network

На этом этапе вам предлагается принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации о системе. При этом гарантируется, что персональные данные отправляться не будут.

Ознакомьтесь с положением об использовании Kaspersky Security Network. Чтобы ознакомиться с полным текстом положения, нажмите на кнопку **ПОЛОЖЕНИЕ О KSN**. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я принимаю условия участия в Kaspersky Security Network**.

Нажмите на кнопку **Далее**, если вы выполняете установку с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке нажмите на кнопку **Установить**. Установка будет продолжена.

Шаг 6. Поиск несовместимых программ

На этом этапе осуществляется поиск установленных на вашем компьютере программ, несовместимых с Kaspersky Internet Security.

Если таких программ не найдено, мастер автоматически перейдет к следующему шагу.

При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Kaspersky Internet Security не может удалить автоматически, необходимо удалить вручную. В процессе удаления несовместимых программ потребуется перезагрузка системы, после чего установка Kaspersky Internet Security продолжится автоматически.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 7. Выбор папки назначения

Этот шаг мастера установки доступен только в том случае, если выполняется установка программы с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке шаг пропускается и программа устанавливается в папку, предусмотренную по умолчанию.

На этом этапе установки вам предлагается определить папку, в которую будет установлен Kaspersky Internet Security. По умолчанию задан следующий путь:

- **<диск>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2012** – для 32-разрядных систем;
- **<диск>\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 2012** – для 64-разрядных систем.

Чтобы установить Kaspersky Internet Security в другую папку, укажите путь к ней в поле ввода или нажмите на кнопку **Обзор** и выберите папку в открывшемся окне.

Обратите внимание на следующие ограничения:

- Нельзя устанавливать программу на сетевые и съемные диски, а также на виртуальные диски (диски, созданные с помощью команды `SUBST`).
- Не рекомендуется устанавливать программу в папку, содержащую файлы или другие папки, так как впоследствии к ней будет запрещен доступ на редактирование.
- Путь к папке установки должен быть не длиннее 160 символов и не должен содержать спецсимволы **/**, **?**, **:**, *****, **"**, **>**, **<** и **|**.

Чтобы узнать, достаточно ли дискового пространства на вашем компьютере для установки программы, нажмите на кнопку **Диск**. В открывшемся окне вы сможете просмотреть информацию о дисковом пространстве. Чтобы закрыть окно, нажмите на кнопку **ОК**.

Для продолжения установки нажмите в окне мастера на кнопку **Далее**.

Шаг 8. Подготовка к установке

Этот шаг мастера установки доступен только в том случае, если выполняется установка программы с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке этот шаг пропускается.

Поскольку на вашем компьютере могут присутствовать вредоносные программы, способные помешать установке Kaspersky Internet Security, процесс установки необходимо защищать.

По умолчанию защита процесса установки включена – в окне мастера установлен флажок **Защитить процесс установки**.

Снимать этот флажок рекомендуется в том случае, когда невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). Причиной этому может быть включенная защита.

В этом случае прервите установку и запустите процесс установки с начала, установите флажок **Изменить параметры установки** на шаге Выбор типа установки (см. раздел «Шаг 3. Выбор типа установки» на стр. 21) и, дойдя до шага Подготовка к установке, снимите флажок **Защитить процесс установки**.

Для продолжения установки нажмите на кнопку **Установить**.

При установке программы на компьютер под управлением операционной системы Microsoft Windows XP текущие сетевые соединения разрываются. Большинство разорванных соединений восстанавливается через некоторое время.

Шаг 9. Установка

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

В случае возникновения ошибки установки, которая может быть вызвана наличием на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит скачать специальное средство для устранения заражения – *утилиту Kaspersky Virus Removal Tool*.

Если вы согласитесь установить утилиту, мастер установки загрузит ее с серверов «Лаборатории Касперского», после чего автоматически запустится установка утилиты. Если мастер не сможет загрузить утилиту, вам будет предложено скачать ее самостоятельно, перейдя по предлагаемой ссылке.

После завершения работы с утилитой ее необходимо удалить и запустить установку Kaspersky Internet Security с начала.

Шаг 10. Завершение установки

Это окно мастера информирует вас о завершении установки программы. Чтобы начать работу Kaspersky Internet Security, убедитесь, что флажок **Запустить Kaspersky Internet Security 2012** установлен, и нажмите на кнопку **Завершить**.

В некоторых случаях может потребоваться перезагрузка операционной системы. Если флажок **Запустить Kaspersky Internet Security 2012** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок, программу нужно запустить вручную (см. раздел «Запуск и завершение работы программы вручную» на стр. 43).

Шаг 11. Активация программы

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Для активации программы необходимо подключение к интернету.

Вам предлагаются следующие варианты активации Kaspersky Internet Security:

- **Активировать коммерческую версию**. Выберите этот вариант и введите код активации, если вы приобрели коммерческую версию программы.

  Если в поле ввода вы укажете код активации Антивируса Касперского, по завершении активации запустится процедура переключения на Антивирус Касперского.

- **Активировать пробную версию**. Выберите этот вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вы сможете использовать полнофункциональную версию программы в течение срока действия, ограниченного лицензией для пробной версии программы. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

Шаг 12. Регистрация пользователя

Этот шаг доступен только при активации коммерческой версии программы. При активации пробной версии шаг пропускается.

Чтобы в дальнейшем иметь возможность обращаться за помощью в Службу технической поддержки «Лаборатории Касперского», вам нужно зарегистрироваться.

Если вы согласны зарегистрироваться, для отправки своих регистрационных данных укажите их в соответствующих полях и затем нажмите на кнопку **Далее**.

Шаг 13. Завершение активации

Мастер информирует вас об успешном завершении активации Kaspersky Internet Security. Кроме того, приводится информация о лицензии: тип (коммерческая или пробная), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

В случае активации подписки вместо даты окончания срока действия лицензии приводится информация о статусе подписки.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Обновление предыдущей версии Kaspersky Internet Security

Если на вашем компьютере уже установлен Kaspersky Internet Security 2010 или 2011, вам нужно обновить программу до версии Kaspersky Internet Security 2012. При наличии действующей лицензии Kaspersky Internet Security 2010 или 2011 вам не понадобится активировать программу: мастер установки автоматически получит информацию о лицензии на Kaspersky Internet Security 2010 или 2011 и использует ее в процессе установки.

Kaspersky Internet Security устанавливается на компьютер в интерактивном режиме с помощью Мастера установки.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров зависит от вашей лицензии), то на все компьютеры она устанавливается одинаково. Следует помнить, что в этом случае в соответствии с лицензионным соглашением срок действия лицензии начинается с даты первой активации программы. При активации программы на втором и последующих компьютерах срок действия лицензии будет уменьшаться на тот период времени, который прошел с момента первой активации. Таким образом, срок действия лицензии истечет одновременно для всех установленных копий программы.

- *Чтобы установить Kaspersky Internet Security на ваш компьютер,*

  на CD-диске с продуктом запустите файл дистрибутива (файл с расширением exe).

  Процесс установки Kaspersky Internet Security с дистрибутива, полученного через интернет, полностью совпадает с процессом установки программы с дистрибутивного CD-диска.

В этом разделе

Шаг 1. Поиск более новой версии программы

Перед установкой проверяется наличие более актуальной версии Kaspersky Internet Security на серверах обновлений «Лаборатории Касперского».

Если более новой версии программы на серверах обновлений «Лаборатории Касперского» не обнаружено, будет запущен мастер установки текущей версии.

Если на серверах обновлений выложена более новая версия Kaspersky Internet Security, вам будет предложено загрузить и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. В случае отказа от более новой версии будет запущен мастер установки текущей версии. Если же вы примете решение установить более новую версию, файлы дистрибутива будут скопированы на ваш компьютер и мастер установки новой версии будет запущен автоматически. Дальнейшее описание установки более новой версии читайте в документации к соответствующей версии программы.

Шаг 2. Проверка соответствия системы необходимым условиям установки

Перед установкой Kaspersky Internet Security на вашем компьютере проверяется соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки (см. раздел «Аппаратные и программные требования» на стр. 18). Помимо этого, проверяется наличие требуемого программного обеспечения, а также прав на установку программного обеспечения. Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

Если компьютер соответствует предъявляемым требованиям, мастер выполняет поиск программ «Лаборатории Касперского», совместное использование с которыми программы Kaspersky Internet Security может привести к возникновению конфликтов. Если такие программы будут найдены, вам будет предложено удалить их вручную.

Если в числе обнаруженных программ есть Антивирус Касперского или Kaspersky Internet Security одной из предыдущих версий, все данные, которые могут быть использованы Kaspersky Internet Security 2012 (например, информация об активации или параметры программы), будут сохранены и использованы при установке, а ранее установленная программа будет автоматически удалена.

Шаг 3. Выбор типа установки

На этом этапе установки вы можете выбрать наиболее подходящий тип установки Kaspersky Internet Security:

- *Стандартная установка*. При выборе этого варианта (флажок **Изменить параметры установки** снят) программа будет полностью установлена на ваш компьютер с параметрами защиты, рекомендуемыми специалистами «Лаборатории Касперского».

- *Установка с возможностью изменения параметров*. В данном случае (флажок **Изменить параметры установки** установлен) вам будет предложено указать папку, в которую будет установлена программа (см. раздел «Шаг 7. Выбор папки назначения» на стр. 22), и при необходимости выключить защиту процесса установки (см. раздел «Шаг 8. Подготовка к установке» на стр. 23).

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 4. Просмотр лицензионного соглашения

На этом этапе следует ознакомиться с лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочтите соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Я согласен**. Установка программы на ваш компьютер будет продолжена.

Если вы не согласны с лицензионным соглашением, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 5. Положение об использовании Kaspersky Security Network

На этом этапе вам предлагается принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации о системе. При этом гарантируется, что персональные данные отправляться не будут.

Ознакомьтесь с положением об использовании Kaspersky Security Network. Чтобы ознакомиться с полным текстом положения, нажмите на кнопку **ПОЛОЖЕНИЕ О KSN**. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я принимаю условия участия в Kaspersky Security Network**.

Нажмите на кнопку **Далее**, если вы выполняете установку с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке нажмите на кнопку **Установить**. Установка будет продолжена.

Шаг 6. Поиск несовместимых программ

На этом этапе осуществляется поиск установленных на вашем компьютере программ, несовместимых с Kaspersky Internet Security.

Если таких программ не найдено, мастер автоматически перейдет к следующему шагу.

При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Kaspersky Internet Security не может удалить автоматически, необходимо удалить вручную. В процессе удаления несовместимых программ потребуется перезагрузка системы, после чего установка Kaspersky Internet Security продолжится автоматически.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 7. Выбор папки назначения

Этот шаг мастера установки доступен только в том случае, если выполняется установка программы с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке шаг пропускается и программа устанавливается в папку, предусмотренную по умолчанию.

На этом этапе установки вам предлагается определить папку, в которую будет установлен Kaspersky Internet Security. По умолчанию задан следующий путь:

- **<диск>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2012** – для 32-разрядных систем;
- **<диск>\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 2012** – для 64-разрядных систем.

Чтобы установить Kaspersky Internet Security в другую папку, укажите путь к ней в поле ввода или нажмите на кнопку **Обзор** и выберите папку в открывшемся окне.

Обратите внимание на следующие ограничения:

- Нельзя устанавливать программу на сетевые и съемные диски, а также на виртуальные диски (диски, созданные с помощью команды `SUBST`).
- Не рекомендуется устанавливать программу в папку, содержащую файлы или другие папки, так как впоследствии к ней будет запрещен доступ на редактирование.
- Путь к папке установки должен быть не длиннее 160 символов и не должен содержать спецсимволы **/**, **?**, **:**, *****, **"**, **>**, **<** и **|**.

Чтобы узнать, достаточно ли дискового пространства на вашем компьютере для установки программы, нажмите на кнопку **Диск**. В открывшемся окне вы сможете просмотреть информацию о дисковом пространстве. Чтобы закрыть окно, нажмите на кнопку **ОК**.

Для продолжения установки нажмите в окне мастера на кнопку **Далее**.

Шаг 8. Подготовка к установке

Этот шаг мастера установки доступен только в том случае, если выполняется установка программы с возможностью изменения параметров (см. раздел «Шаг 3. Выбор типа установки» на стр. 21). При стандартной установке этот шаг пропускается.

Поскольку на вашем компьютере могут присутствовать вредоносные программы, способные помешать установке Kaspersky Internet Security, процесс установки необходимо защищать.

По умолчанию защита процесса установки включена – в окне мастера установлен флажок **Защитить процесс установки**.

Снимать этот флажок рекомендуется в том случае, когда невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). Причиной этому может быть включенная защита.

В этом случае прервите установку и запустите процесс установки с начала, установите флажок **Изменить параметры установки** на шаге Выбор типа установки (см. раздел «Шаг 3. Выбор типа установки» на стр. 21) и, дойдя до шага Подготовка к установке, снимите флажок **Защитить процесс установки**.

Для продолжения установки нажмите на кнопку **Установить**.

При установке программы на компьютер под управлением операционной системы Microsoft Windows XP текущие сетевые соединения разрываются. Большинство разорванных соединений восстанавливается через некоторое время.

Шаг 9. Установка

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

В случае возникновения ошибки установки, которая может быть вызвана наличием на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит скачать специальное средство для устранения заражения – *утилиту Kaspersky Virus Removal Tool*.

Если вы согласитесь установить утилиту, мастер установки загрузит ее с серверов «Лаборатории Касперского», после чего автоматически запустится установка утилиты. Если мастер не сможет загрузить утилиту, вам будет предложено скачать ее самостоятельно, перейдя по предлагаемой ссылке.

После завершения работы с утилитой ее необходимо удалить и запустить установку Kaspersky Internet Security с начала.

Шаг 10. Завершение работы мастера

Это окно мастера информирует вас о завершении установки программы. Чтобы начать работу Kaspersky Internet Security, убедитесь, что флажок **Запустить Kaspersky Internet Security 2012** установлен, и нажмите на кнопку **Завершить**.

В некоторых случаях может потребоваться перезагрузка операционной системы. Если флажок **Запустить Kaspersky Internet Security 2012** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок, программу нужно запустить вручную (см. раздел «Запуск и завершение работы программы вручную» на стр. 43).

Нетиповые сценарии установки

В этом разделе описаны сценарии установки программы, которые отличаются от стандартной установки или обновления с предыдущей версии.

Установка Kaspersky Internet Security с последующей активацией кодом активации Антивируса Касперского

Если в процессе установки Kaspersky Internet Security на шаге Активация программы вы введете код активации Антивируса Касперского, то будет запущена процедура переключения, в результате которой на ваш компьютер будет установлен Антивирус Касперского.

Если в процессе установки Kaspersky Internet Security на шаге Активация программы вы выберете вариант **Активировать позже**, а затем активируете установленную программу кодом активации Антивируса Касперского, то также будет запущена процедура переключения, в результате которой на ваш компьютер будет установлен Антивирус Касперского.

Установка Kaspersky Internet Security 2012 поверх Антивируса Касперского 2010 или 2011

Если вы запустите установку Kaspersky Internet Security 2012 на компьютере, на котором уже установлен Антивирус Касперского 2010 или 2011 с действующей лицензией, то мастер установки, обнаружив информацию о лицензии, предложит вам выбрать вариант дальнейших действий:

- Использовать действующую лицензию от Антивируса Касперского 2010 или 2011. В этом случае будет запущена процедура переключения, в результате которой на ваш компьютер будет установлен Антивирус Касперского 2012. Вы сможете пользоваться Антивирусом Касперского 2012 в течение срока действия лицензии от Антивируса Касперского 2010 или 2011.

- Продолжить установку Kaspersky Internet Security 2012. В этом случае процедура установки будет продолжена согласно стандартному сценарию, начиная с шага Активация программы.

Начало работы

После установки и настройки программа готова к работе. Чтобы обеспечить должную защиту вашего компьютера, рекомендуем сразу после установки и настройки выполнить следующие действия:

- Обновить базы программы (см. раздел «Как обновить базы и модули программы» на стр. 50).

- Проверить компьютер на вирусы (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 53), а также на уязвимости (см. раздел «Как проверить компьютер на уязвимости» на стр. 53).

- Проверить состояние защиты компьютера и при необходимости устранить проблемы в защите.

Удаление программы

В результате удаления Kaspersky Internet Security компьютер и ваши личные данные окажутся незащищенными!

Удаление Kaspersky Internet Security выполняется с помощью мастера установки.

Чтобы запустить мастер,

в меню **Пуск** выберите пункт **Программы → Kaspersky Internet Security 2012 → Удалить Kaspersky Internet Security 2012**.

В этом разделе

Шаг 1. Сохранение данных для повторного использования

На этом шаге вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии).

По умолчанию программа удаляется с компьютера полностью.

Чтобы сохранить данные для повторного использования, выполните следующие действия:

1. Выберите вариант **Сохранить объекты программы**.

2. Установите флажки напротив тех данных, которые нужно сохранить:

   - **Информация об активации** – данные, позволяющие в дальнейшем не активировать устанавливаемую программу, а автоматически использовать текущую лицензию, если срок ее действия не истечет к моменту установки.

   - **Объекты резервного хранилища и карантина** – файлы, проверенные программой и помещенные в резервное хранилище и карантин.

   - **Параметры работы программы** – значения параметров работы программы, установленные в процессе ее настройки.

   - **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных на вирусы.

   - **Данные общей папки безопасной среды** – файлы, сохраненные при работе в безопасной среде в специальной папке, которая доступна и в обычной среде.

   - **Базы Анти-Спама** – базы, содержащие образцы спам-сообщений, полученные и сохраненные программой в процессе работы.

Шаг 2. Подтверждение удаления программы

Поскольку удаление программы ставит под угрозу защиту компьютера и ваших личных данных, требуется подтвердить свое намерение удалить программу. Для этого нажмите на кнопку **Удалить**.

До завершения удаления вы в любой момент можете отменить это действие, нажав на кнопку **Отмена**.

Шаг 3. Удаление программы. Завершение удаления

На этом шаге мастер удаляет программу с вашего компьютера. Дождитесь завершения процесса удаления.

В процессе удаления может понадобиться перезагрузка операционной системы. Если вы откажетесь от немедленной перезагрузки, завершение процедуры удаления будет отложено до того момента, когда операционная система будет перезагружена или компьютер будет выключен и включен.

ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения при установке программы «Лаборатории Касперского».

Считается, что вы принимаете условия Лицензионного соглашения в следующих ситуациях:

- Открывая коробку с установочным компакт-диском (только если вы приобрели программу в коробке в розничных магазинах или в магазинах наших партнеров).
- Подтверждая свое согласие с текстом Лицензионного соглашения при установке программы.

Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы.

О предоставлении данных

Для повышения уровня оперативной защиты, принимая условия лицензионного соглашения, вы соглашаетесь в автоматическом режиме передавать информацию о контрольных суммах обрабатываемых файлов (MD5), информацию для определения репутации URL, а также статистические данные для защиты от спама. Полученная информация не содержит персональных данных и иной конфиденциальной информации. Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. Вы можете получить более подробную информацию на веб-сайте http://support.kaspersky.com.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. Лицензия содержит уникальный код активации вашего экземпляра Kaspersky Internet Security.

Лицензия предоставляет вам право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

  Количество устройств, на которых вы можете использовать программу, указано в Лицензионном соглашении.

- Обращение в Службу технической поддержки «Лаборатории Касперского».

- Получение полного набора услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии (см. раздел «Сервис для зарегистрированных пользователей» на стр. 18).

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

Предусмотрены следующие типы лицензий:

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

  Если вы копируете программу с сайта http://www.kaspersky.ru, вы автоматически становитесь обладателем пробной лицензии. По завершении срока действия лицензии Kaspersky Internet Security прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести коммерческую лицензию.

- *Коммерческая* – платная лицензия с ограниченным сроком действия, предоставляемая при приобретении программы.

  По окончании срока действия коммерческой лицензии программа продолжает работать в режиме ограниченной функциональности. Вы по-прежнему можете проверять компьютер на наличие вирусов и использовать другие компоненты программы, но только на основе баз, установленных до даты окончания срока действия лицензии. Для продолжения использования Kaspersky Internet Security требуется продлить коммерческую лицензию.

  Рекомендуется продлевать срок действия лицензии не позднее даты окончания срока действия текущей лицензии, чтобы обеспечить максимальную антивирусную защиту вашего компьютера.

О коде активации

Код активации – это код, который вы получаете, приобретая коммерческую лицензию Kaspersky Internet Security. Этот код необходим для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр, в формате xxxxx-xxxxx-xxxxx-xxxxx.

Код активации поставляется в одной из следующих форм, зависящих от способа приобретения программы:

- Если вы приобрели коробочную версию Kaspersky Internet Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.

- Если вы приобрели Kaspersky Internet Security в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с момента активации программы. Если вы приобрели лицензию, предназначенную для использования Kaspersky Internet Security на нескольких устройствах, то отсчет срока действия лицензии начинается с момента активации кода на первом компьютере.

Если код активации был потерян или случайно удален после активации, то для его восстановления требуется отправить запрос в Службу технической поддержки «Лаборатории Касперского» из Личного кабинета (см. раздел «Получение технической поддержки через Личный кабинет» на стр. 196).

По окончании активации программы с помощью кода активации вам присваивается *номер клиента*. Номер клиента – это персональный идентификационный номер пользователя, который является обязательным условием для получения технической поддержки по телефону или в Личном кабинете (см. раздел «Получение технической поддержки через Личный кабинет» на стр. 196).

ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы и контекстном меню значка программы, главном окне, окне настройки, окнах уведомлений.

В ЭТОМ РАЗДЕЛЕ

Значок в области уведомлений

Сразу после установки Kaspersky Internet Security его значок появляется в области уведомлений панели задач Microsoft Windows.

В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить (см. документацию на операционную систему).

Значок выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню, главному окну программы и окну просмотра новостей.

Индикация работы программы

Значок служит индикатором работы программы. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых программой на текущий момент:

 – проверяется почтовое сообщение;

 – проверяется веб-трафик;

 – обновляются базы и модули программы;

 – требуется перезагрузка компьютера для применения обновлений;

 – произошел сбой в работе какого-либо компонента программы.

По умолчанию включена анимация значка: например, при проверке почтового сообщения на фоне значка программы пульсирует миниатюрный значок письма, а при обновлении баз программы – вращается значок глобуса. Вы можете выключить анимацию (см. раздел «Полупрозрачность окон уведомлений» на стр. 184).

При выключенной анимации значок может принимать следующий вид:

(цветной значок) – все или некоторые компоненты защиты работают;

(черно-белый значок) – все компоненты защиты выключены.

Доступ к контекстному меню и окнам программы

С помощью значка вы можете открыть контекстное меню (на стр. 36) (по правой клавише мыши) и главное окно программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37) (по левой клавише мыши).

При появлении новостей от «Лаборатории Касперского» в области уведомлений панели задач Microsoft Windows появляется значок . Двойным щелчком мыши на этом значке можно открыть окно Новостного агента (см. раздел «Новостной агент» на стр. 41).

Контекстное меню

С помощью контекстного меню вы можете быстро выполнить ряд действий с программой.

Меню Kaspersky Internet Security содержит следующие пункты:

- **Менеджер задач** – открывает окно **Менеджер задач**.
- **Обновление** – запускает процесс обновления баз и модулей программы.
- **Инструменты** – открывает вложенное меню, содержащее следующие пункты:
  - **Активность программ** – открывает окно **Активность программ**;
  - **Мониторинг сети** – открывает окно **Мониторинг сети**;
  - **Виртуальная клавиатура** – выводит на экран виртуальную клавиатуру.
- **Безопасная среда** – запускает безопасный рабочий стол для работы с программами, которые, по вашему мнению, могут быть небезопасны. Если безопасный рабочий стол уже запущен, то выполняется переключение на него.

  При работе на безопасном рабочем столе этот пункт меню называется **Вернуться на основной рабочий стол** и служит для переключения на основной рабочий стол.
- **Kaspersky Internet Security** – открывает главное окно программы.
- **Приостановить защиту** / **Возобновить защиту** – временно выключает / включает работу компонентов постоянной защиты. Этот пункт меню не влияет на обновление программы и на выполнение задач поиска вирусов.
- **Включить Родительский контроль** / **Выключить Родительский контроль** – включает / выключает Родительский контроль для текущей учетной записи.
- **Настройка** – открывает окно настройки параметров работы программы.
- **О программе** – открывает информационное окно со сведениями о программе.
- **Новости** – открывает окно новостного агента (см. раздел «Новостной агент» на стр. 41). Этот пункт меню отображается при наличии непрочитанных новостей.

- **Выход** – завершает работу Kaspersky Internet Security (при выборе данного пункта меню программа будет выгружена из оперативной памяти компьютера).

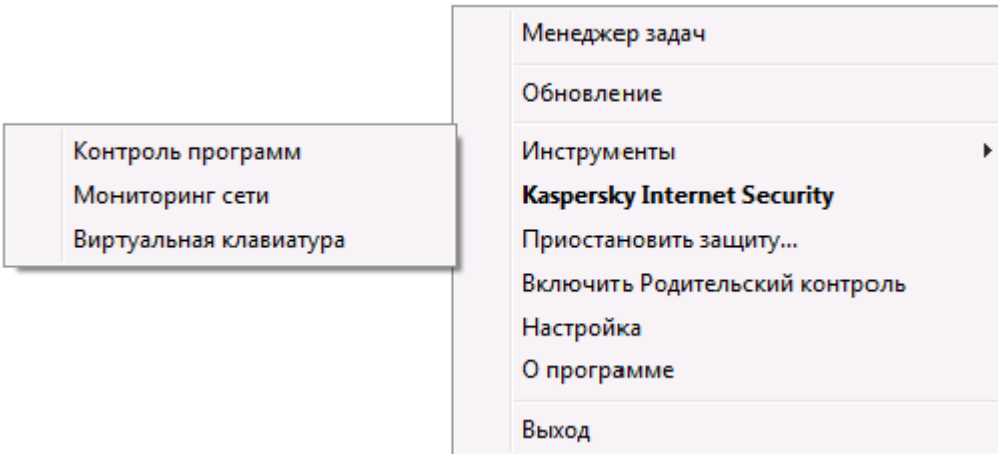

Рисунок 1. Контекстное меню

Если в момент открытия контекстного меню запущена какая-либо задача проверки на вирусы или задача обновления программы, ее название будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав пункт меню с названием задачи, вы можете перейти к главному окну с отчетом о текущих результатах ее выполнения.

Чтобы открыть контекстное меню,

наведите курсор мыши на значок программы в области уведомлений панели задач и нажмите на правую клавишу мыши.

В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить (см. документацию на операционную систему).

Главное окно Kaspersky Internet Security

В главном окне программы сосредоточены элементы интерфейса, предоставляющие доступ ко всем основным функциям программы.

Главное окно можно условно разделить на две части:

- Верхняя часть окна содержит информацию о состоянии защиты вашего компьютера.

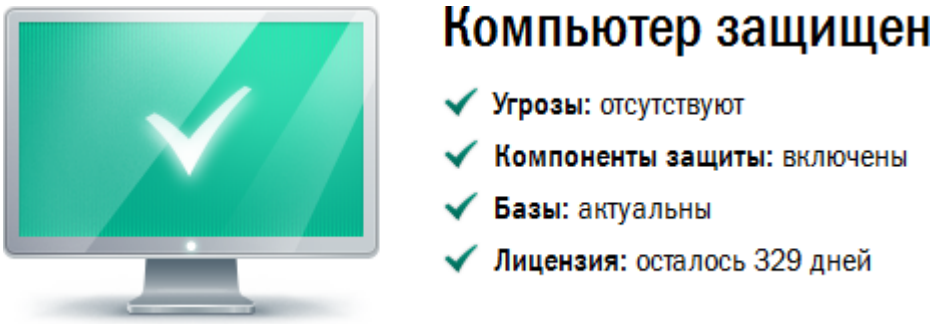

Рисунок 2. Верхняя часть главного окна

- В нижней части окна вы можете быстро перейти к работе с основными функциями программы (например, к выполнению задач проверки на вирусы, обновлению баз и модулей программы).

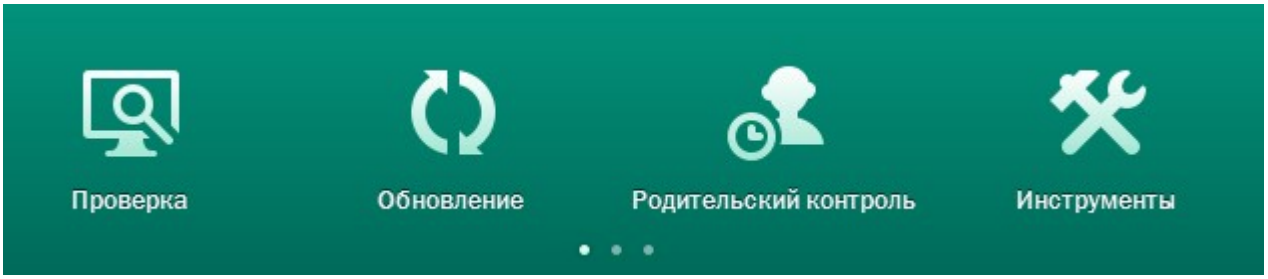

Рисунок 3. Нижняя часть главного окна

При выборе одного из разделов в нижней части окна открывается окно соответствующей функции программы. Вы можете вернуться к выбору функций, нажав на кнопку **Назад** в верхнем левом углу окна.

Вы можете воспользоваться также следующими кнопками и ссылками:

- **Защита из облака** – переход к информации о Kaspersky Security Network (на стр. 187).
- **Настройка** – переход к окну настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 40).
- **Отчеты** – переход к отчетам о работе программы.
- **Новости** – переход к просмотру новостей в окне новостного агента (см. раздел «Новостной агент» на стр. 41). Ссылка отображается после получения программой новости.
- **Справка** – переход к справочной системе Kaspersky Internet Security.
- **Личный кабинет** – переход в Личный кабинет пользователя на веб-сайте Службы технической поддержки.
- **Поддержка** – открытие окна с информацией о системе и ссылками на информационные ресурсы «Лаборатории Касперского» (сайт Службы технической поддержки, форум).
- **Управление лицензиями** – переход к активации Kaspersky Internet Security, продлению срока действия лицензии.

Вы можете открыть главное окно программы одним из следующих способов:

- Нажав на левую клавишу мыши на значке программы в области уведомлений панели задач.

  В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить (см. документацию на операционную систему).

- Выбрав пункт **Kaspersky Internet Security** в контекстном меню (см. раздел «Контекстное меню» на стр. 36).
- Нажав на значок Kaspersky Internet Security, расположенный в центральной части Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

Окна уведомлений и всплывающие сообщения

Kaspersky Internet Security уведомляет вас о значимых событиях, происходящих в процессе его работы, с помощью *окон уведомлений* и *всплывающих сообщений*, которые появляются над значком программы в области уведомлений панели задач.

Окна уведомлений Kaspersky Internet Security выводит на экран в тех случаях, когда возможны различные варианты действий в связи с событием: например, при обнаружении вредоносного объекта вы можете заблокировать доступ к нему, удалить его или попытаться вылечить. Программа предложит вам выбрать действие из числа возможных. Окно уведомления исчезнет с экрана только после того, как вы выберете одно из предложенных действий.

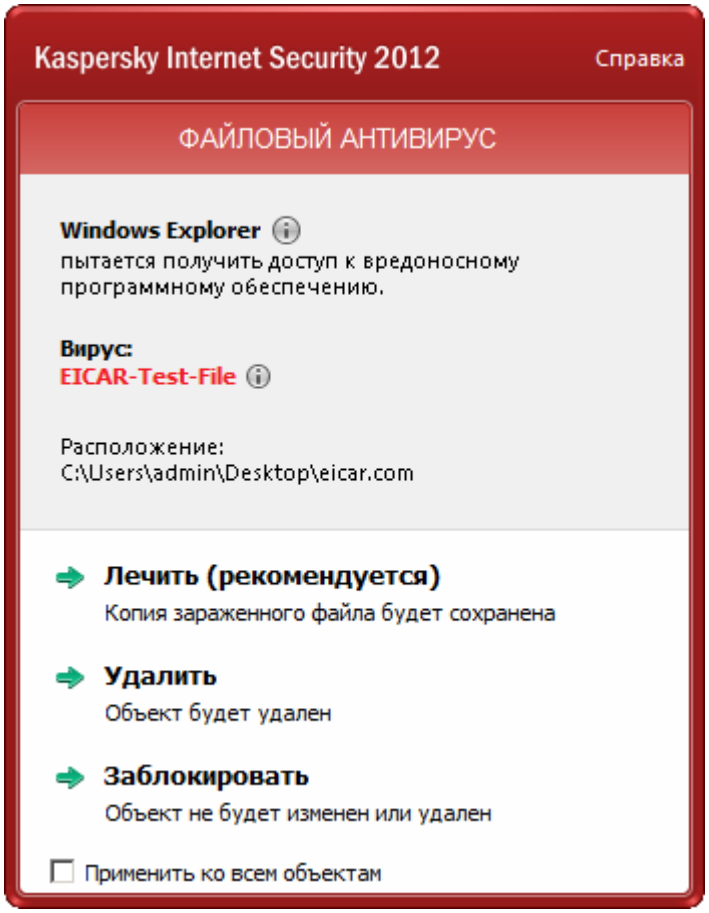

Рисунок 4. Окно уведомления

Всплывающие сообщения Kaspersky Internet Security выводит на экран, чтобы проинформировать о событиях, не требующих от вас обязательного выбора действия. В некоторых всплывающих сообщениях доступны ссылки, по которым вы можете выполнить предлагаемое действие (например, запустить обновление баз или перейти к активации программы). Всплывающие сообщения автоматически исчезают с экрана вскоре после появления.

Рисунок 5. Всплывающее сообщение

В зависимости от степени важности события с точки зрения безопасности компьютера, уведомления и всплывающие сообщения делятся на три типа:

- Критические – информируют о событиях, имеющих первостепенную важность для обеспечения безопасности компьютера (например, об обнаружении вредоносного объекта или опасной активности в системе). Окна критических уведомлений и всплывающих сообщений – красные.

- Важные – информируют о событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в системе). Окна важных уведомлений и всплывающих сообщений – желтые.

- Информационные – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые.

Окно настройки параметров программы

Окно настройки параметров Kaspersky Internet Security (далее также «окно настройки») предназначено для настройки параметров работы программы в целом, отдельных компонентов защиты, задач проверки и обновления, а также для выполнения других задач расширенной настройки (см. раздел «Расширенная настройка программы» на стр. 68).

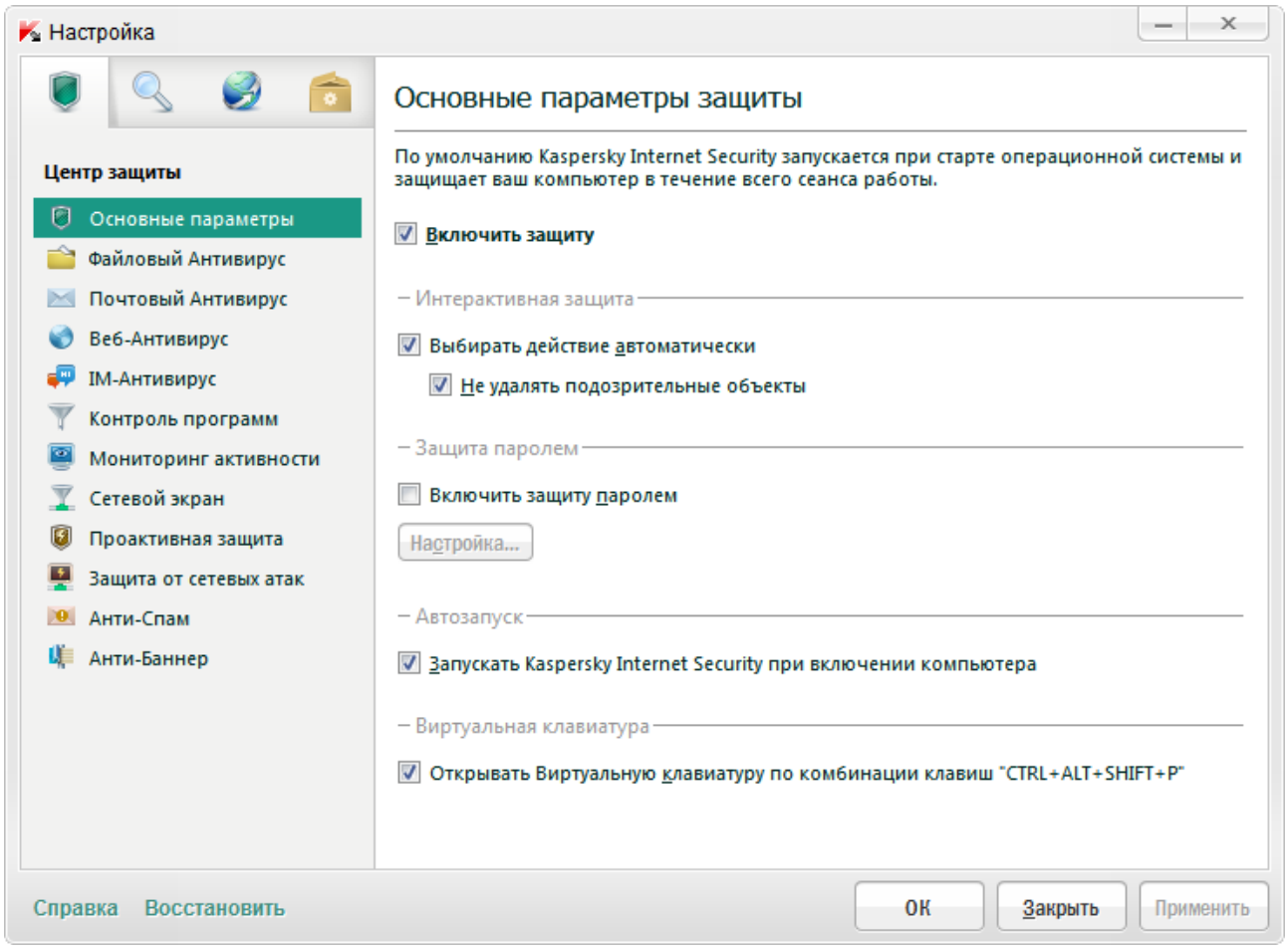

Рисунок 6. Окно настройки параметров программы

Окно настройки состоит из двух частей:

- в левой части окна можно выбрать компонент программы, задачу или другую составляющую, которую нужно настроить;

- в правой части окна содержатся элементы управления, с помощью которых можно настроить работу составляющей, выбранной в левой части окна.

Компоненты, задачи и другие составляющие в левой части окна объединены в следующие разделы:

– **Центр защиты**;

– **Проверка компьютера**;

– **Обновление**;

– **Дополнительные параметры**.

Вы можете открыть окно настройки одним из следующих способов:

- перейдя по ссылке **Настройка** в верхней части главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- выбрав пункт **Настройка** в контекстном меню программы (см. раздел «Контекстное меню» на стр. 36);
- нажав на кнопку со значком **Настройка** в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7). Для кнопки должна быть назначена функция открывания окна настройки (см. раздел «Как использовать Kaspersky Gadget» на стр. 65).

Kaspersky Gadget

При использовании Kaspersky Internet Security на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вам доступен Kaspersky Gadget (далее также *гаджет*). Kaspersky Gadget предназначен для быстрого доступа к основным функциям программы (например, индикации состояния защиты компьютера, проверке объектов на вирусы, просмотру отчетов о работе программы.

После установки Kaspersky Internet Security на компьютер под управлением операционной системы Microsoft Windows 7 гаджет появляется на рабочем столе автоматически. После установки программы на компьютер под управлением операционной системы Microsoft Windows Vista гаджет нужно добавить на боковую панель Microsoft Windows вручную (см. документацию на операционную систему).

Рисунок 7. Kaspersky Gadget

Новостной агент

С помощью *новостного агента* «Лаборатория Касперского» информирует вас обо всех важных событиях, касающихся Kaspersky Internet Security и защиты от компьютерных угроз в целом.

Программа будет уведомлять вас о появлении новостей с помощью значка в области уведомлений панели задач (см. ниже) и всплывающего сообщения. Информация о количестве непрочитанных новостей также отображается в главном окне программы. В интерфейсе гаджета Kaspersky Internet Security появляется значок новости.

Прочитать новости вы можете одним из следующих способов:

- нажав на значок в области уведомлений панели задач;

- перейдя по ссылке **Читать новости** во всплывающем сообщении о новостях;
- перейдя по ссылке **Новости** в главном окне программы;
- нажав на значок  , который отображается в центре гаджета при появлении новости (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

Перечисленные способы открывания окна новостного агента доступны только при наличии непрочитанных новостей.

Если вы не хотите получать новости, вы можете выключить доставку новостей.

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

Под автоматическим запуском программы подразумевается запуск Kaspersky Internet Security, который выполняется без вашего участия сразу после старта операционной системы. Такой вариант запуска предусмотрен по умолчанию.

- *Чтобы отключить или включить автоматический запуск программы, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** подраздел **Основные параметры**.
  3. Чтобы отключить автоматический запуск программы, в правой части окна в блоке **Автозапуск** снимите флажок **Запускать Kaspersky Internet Security при включении компьютера**. Чтобы включить автоматический запуск программы, установите этот флажок.

Запуск и завершение работы программы вручную

«Лаборатория Касперского» не рекомендует завершать работу Kaspersky Internet Security, поскольку в этом случае защита компьютера и ваших личных данных окажется под угрозой. Рекомендуется временно приостанавливать защиту компьютера, не завершая работу программы.

Запускать Kaspersky Internet Security вручную нужно в случае, если вы отключили автоматический запуск программы (см. раздел «Включение и выключение автоматического запуска» на стр. 43).

- *Чтобы запустить программу вручную,*

  в меню **Пуск** выберите пункт **Программы → Kaspersky Internet Security 2012 → Kaspersky Internet Security 2012**.

- *Чтобы завершить работу программы,*

  по правой клавише мыши вызовите контекстное меню значка программы, расположенного в области уведомлений панели задач, и выберите в меню пункт **Выход**.

В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить (см. документацию на операционную систему).

УПРАВЛЕНИЕ ЗАЩИТОЙ КОМПЬЮТЕРА

Этот раздел содержит информацию о том, как определить наличие угроз безопасности компьютера и настроить уровень его защиты. Из этого раздела вы также узнаете о включении, отключении и временной приостановке защиты во время работы программы.

В ЭТОМ РАЗДЕЛЕ

Диагностика и устранение проблем в защите компьютера

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в левой части главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37). Индикатор представляет собой изображение монитора, которое меняет цвет в зависимости от состояния защиты компьютера: зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера.

Рисунок 8. Индикатор состояния защиты

Проблемы и угрозы безопасности рекомендуется немедленно устранять.

Нажав на индикатор в главном окне программы, можно открыть окно **Проблемы безопасности** (см. рис. ниже), в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

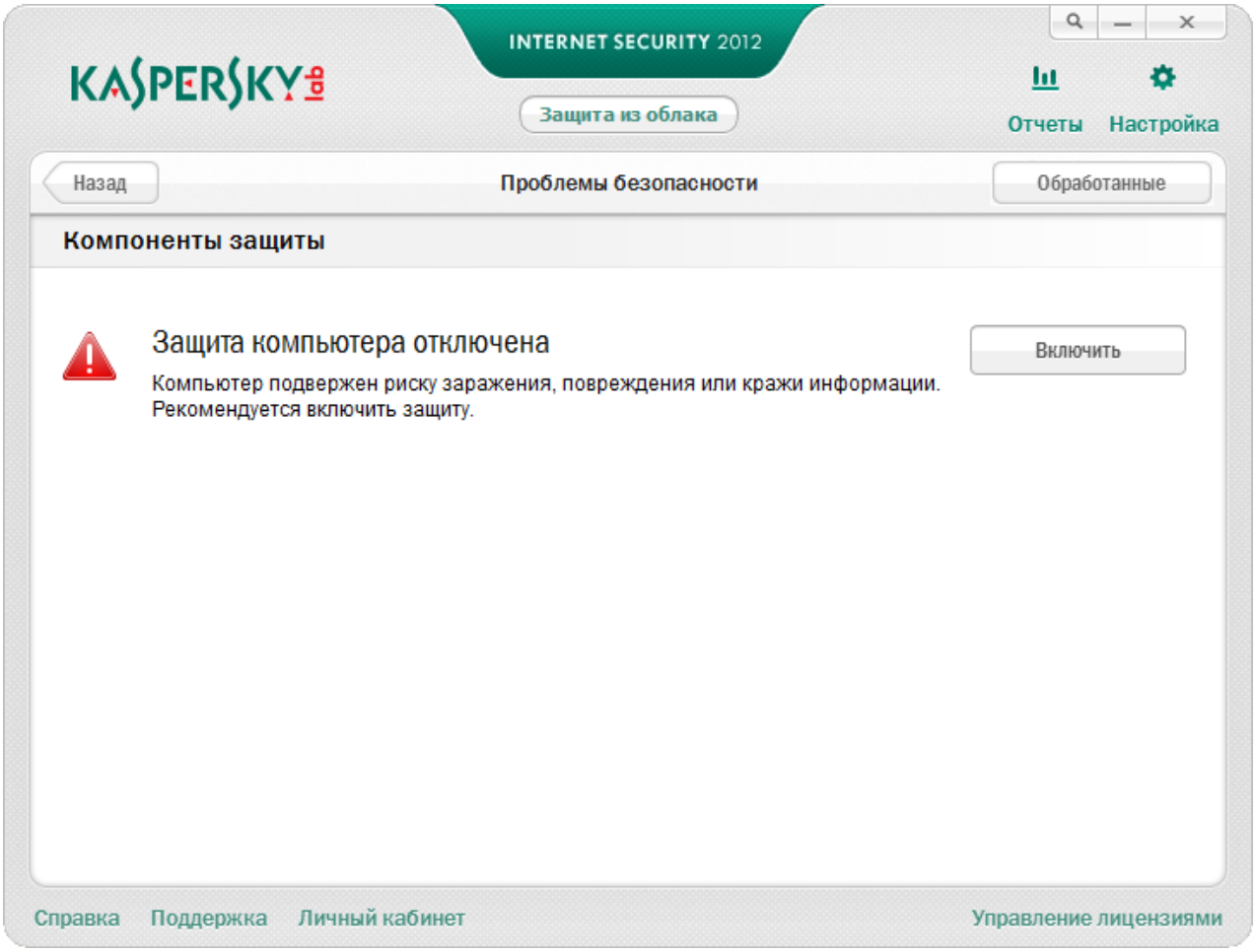

Рисунок 9. Окно Проблемы безопасности

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете предпринять, чтобы решить проблему.

Включение и выключение защиты

По умолчанию Kaspersky Internet Security запускается при старте операционной системы и защищает ваш компьютер в течение всего сеанса работы. Все компоненты защиты работают.

Вы можете полностью или частично выключить защиту, обеспечиваемую Kaspersky Internet Security.

«Лаборатория Касперского» рекомендует не отключать защиту, поскольку это может привести к заражению вашего компьютера и потере данных. Рекомендуется приостанавливать защиту на необходимый срок (см. раздел «Приостановка и возобновление защиты» на стр. 46).

О приостановке или отключении защиты свидетельствуют следующие признаки:

- неактивный (серый) значок программы в области уведомлений панели задач (см. раздел «Значок в области уведомлений» на стр. 35);
- красный цвет индикатора безопасности в верхней части главного окна программы.

В этом случае защита рассматривается в контексте компонентов защиты. Отключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки на вирусы и обновления Kaspersky Internet Security.

Включить или отключить как защиту, так и отдельные компоненты программы, можно из окна настройки программы (см. раздел «Окно настройки параметров программы» на стр. 40).

Чтобы полностью отключить или включить защиту, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Центр защиты**, подраздел **Основные параметры**.
3. Снимите флажок **Включить защиту**, если нужно отключить защиту. Установите этот флажок, если защиту нужно включить.

Чтобы отключить или включить компонент защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент, который нужно включить или отключить.
3. В правой части окна снимите флажок **Включить <наименование компонента>**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Приостановка и возобновление защиты

Приостановка защиты означает отключение на некоторое время всех ее компонентов.

О приостановке или отключении защиты свидетельствуют следующие признаки:

- неактивный (серый) значок программы в области уведомлений панели задач (см. раздел «Значок в области уведомлений» на стр. 35);
- красный цвет индикатора безопасности в верхней части главного окна программы.

В этом случае защита рассматривается в контексте компонентов защиты. Отключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки на вирусы и обновления Kaspersky Internet Security.

Если в момент приостановки защиты были установлены сетевые соединения, на экран будет выведено уведомление о разрыве этих соединений.

На компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вы можете приостановить защиту с помощью Kaspersky Gadget. Для этого нужно назначить функцию приостановки защиты для одной из его кнопок (см. раздел «Как использовать Kaspersky Gadget» на стр. 65).

Чтобы приостановить защиту компьютера, выполните следующие действия:

1. Откройте окно **Приостановка защиты** одним из следующих способов:
   - выберите пункт **Приостановить защиту** в контекстном меню значка программы (см. раздел «Контекстное меню» на стр. 36);
   - нажмите на кнопку со значком **Приостановить защиту** в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

2. В окне **Приостановка защиты** выберите период, по истечении которого защита будет включена:

   - **Приостановить на указанное время** – защита будет включена через интервал, выбранный в раскрывающемся списке ниже.

   - **Приостановить до перезагрузки** – защита будет включена после перезапуска программы или перезагрузки системы (при условии, что включен автоматический запуск программы (см. раздел «Включение и выключение автоматического запуска» на стр. 43)).

   - **Приостановить** – защита будет включена тогда, когда вы решите возобновить ее (см. ниже).

Чтобы возобновить защиту компьютера,

выберите пункт **Возобновить защиту** в контекстном меню значка программы (см. раздел «Контекстное меню» на стр. 36).

Возобновить защиту компьютера таким способом вы можете не только тогда, когда в процессе приостановки был выбран вариант **Приостановить**, но и в случае, если был выбран вариант **Приостановить на указанное время** или **Приостановить до перезагрузки**.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит информацию о том, как решать основные задачи по защите компьютера с помощью программы.

В ЭТОМ РАЗДЕЛЕ

Как активировать программу

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Если вы не активировали программу во время установки, вы можете сделать это позже. О необходимости активировать программу вам будут напоминать уведомления Kaspersky Internet Security, появляющиеся в области уведомлений панели задач.

Чтобы запустить мастер активации Kaspersky Internet Security, выполните одно из следующих действий:

- Перейдите по ссылке **Пожалуйста, активируйте программу** в окне уведомления Kaspersky Internet Security, появляющегося в области уведомлений панели задач.

- Перейдите по ссылке **Введите код активации**, расположенной в нижней части главного окна программы. В открывшемся окне **Управление лицензиями** нажмите на кнопку **Активировать программу**.

В процессе работы Мастера активации программы требуется указать ряд параметров.

Шаг 1. Ввод кода активации

Введите код активации в соответствующее поле и нажмите на кнопку **Далее**.

Шаг 2. Запрос на активацию

При успешном выполнении запроса на активацию мастер автоматически переходит к следующему шагу.

Шаг 3. Ввод регистрационных данных

Регистрация пользователя необходима для того, чтобы в дальнейшем он мог обращаться в Службу технической поддержки. Незарегистрированным пользователям оказывается минимальная поддержка.

Укажите ваши данные для регистрации, затем нажмите на кнопку **Далее**.

Шаг 4. Активация

Если активация программы прошла успешно, мастер автоматически переходит к следующему окну.

Шаг 5. Завершение работы мастера

В этом окне мастера отображается информация о результатах активации: тип используемой лицензии и дата окончания срока ее действия.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

КАК ПРИОБРЕСТИ ЛИЦЕНЗИЮ ИЛИ ПРОДЛИТЬ СРОК ЕЕ ДЕЙСТВИЯ

Если вы установили Kaspersky Internet Security, не имея лицензии, вы можете приобрести лицензию уже после установки программы. При покупке лицензии вы получите код активации, с помощью которого нужно активировать программу (см. раздел «Как активировать программу» на стр. 48).

Когда срок действия лицензии подходит к концу, вы можете его продлить. Вы можете приобрести новую лизенцию, не дожидаясь окончания срока действия используемого кода активации. Для этого требуется добавить резервный код активации. По истечении срока действия используемой лицензии Kaspersky Internet Security будет автоматически активирован с резервным кодом активации.

Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Управление лицензиями**, расположенной в нижней части главного окна, откройте окно **Управление лицензиями**.

3. В открывшемся окне нажмите на кнопку **Купить код активации**.

   Откроется веб-страница интернет-магазина, где вы можете приобрести лицензию.

Чтобы добавить резервный код активации, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Управление лицензиями**, расположенной в нижней части главного окна, откройте окно **Управление лицензиями**.

   Откроется окно **Управление лицензиями**.

3. В открывшемся окне в блоке **Резервный код активации** нажмите на кнопку **Ввести код активации**.

   Откроется мастер активации программы.

4. Введите код активации в соответствующие поля и нажмите на кнопку **Далее**.

   Kaspersky Internet Security отправит данные на сервер активации для проверки. Если проверка завершена успешно, мастер автоматически переходит на следующий шаг.

5. Выберите вариант **Сделать резервным** и нажмите на кнопку **Далее**.
6. По завершении работы мастера нажмите на кнопку **Завершить**.

Что делать при появлении уведомлений программы

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания. В зависимости от степени важности события уведомления могут быть следующих типов:

- Критические – информируют о событиях, имеющих первостепенную важность для обеспечения безопасности компьютера (например, об обнаружении вредоносного объекта или опасной активности в системе). Окна критических уведомлений и всплывающих сообщений – красные.
- Важные – информируют о событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в системе). Окна важных уведомлений и всплывающих сообщений – желтые.
- Информационные – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован экспертами «Лаборатории Касперского» по умолчанию.

Как обновить базы и модули программы

По умолчанию Kaspersky Internet Security автоматически проверяет наличие обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Kaspersky Internet Security загружает и устанавливает их в фоновом режиме. Вы можете в любой момент запустить обновление Kaspersky Internet Security вручную.

Для загрузки обновлений с серверов «Лаборатории Касперского» требуется соединение с интернетом.

- *Чтобы запустить обновление из контекстного меню,*

  выберите пункт **Обновление** в контекстном меню значка программы.

- *Чтобы запустить обновление из главного окна, выполните следующие действия:*

  1. Откройте главное окно программы и в нижней части окна выберите раздел **Обновление**.
  2. В открывшемся окне **Обновление** нажмите на кнопку **Обновить**.

Как проверить важные области компьютера на вирусы

Под проверкой важных областей подразумевается проверка следующих объектов:

- объектов, которые загружаются при запуске операционной системы;
- системной памяти;
- загрузочных секторов диска;
- объектов, добавленных пользователем (см. раздел «Формирование списка объектов для проверки» на стр. 74).

Вы можете запустить проверку важных областей следующими способами:

- с помощью ранее созданного ярлыка (см. стр. 78);
- из главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37).

- *Чтобы запустить проверку с помощью ярлыка, выполните следующие действия:*

  1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
  2. Двойным щелчком мыши на ярлыке запустите проверку.

- *Чтобы запустить проверку из главного окна программы, выполните следующие действия:*

  1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.
  2. В открывшемся окне **Проверка** в блоке **Проверка важных областей** нажмите на кнопку  .

Как проверить на вирусы файл, папку, диск или другой объект

Проверить на вирусы отдельный объект вы можете следующими способами:

- с помощью контекстного меню объекта;
- из главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- с помощью гаджета Kaspersky Internet Security (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

Чтобы запустить задачу проверки на вирусы из контекстного меню объекта, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с объектом, который нужно проверить.

2. По правой клавише мыши откройте контекстное меню объекта (см. рисунок ниже) и выберите пункт **Проверить на вирусы**.

   Процесс и результат выполнения задачи будут отображаться в окне **Менеджер задач**.

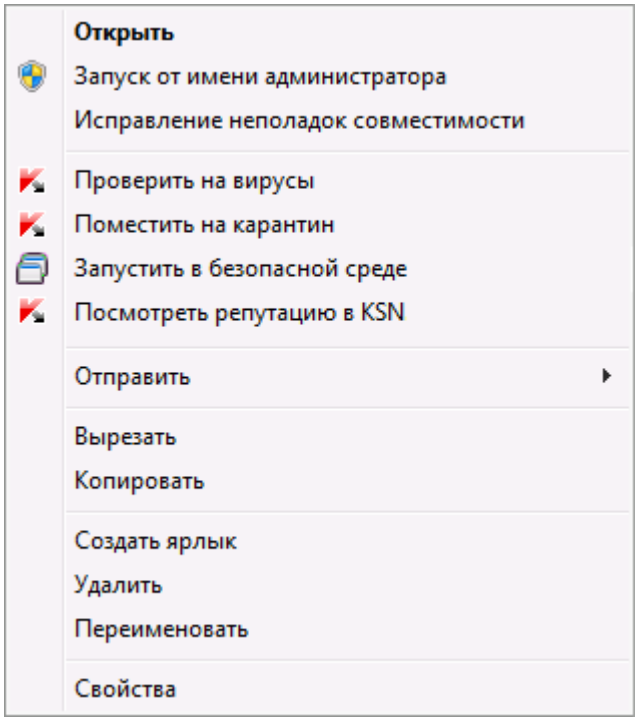

Рисунок 10. Контекстное меню объекта в Microsoft Windows

Чтобы запустить проверку объекта на вирусы из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.

2. Укажите объект, который нужно проверить, одним из следующих способов:

   - По ссылке **укажите**, расположенной в нижней правой части окна, откройте окно **Выборочная проверка** и установите флажки напротив папок и дисков, которые нужно проверить.

     Если в окне отсутствует объект, который требуется проверить, выполните следующие действия:

     a. Нажмите на кнопку **Добавить**.

     b. В открывшемся окне **Выбор объекта для проверки** выберите объект для проверки.

   - Перетащите объект для проверки в предназначенную для этого область главного окна (см. рисунок ниже).

Процесс выполнения задачи будет отображаться в открывшемся окне **Менеджер задач**.

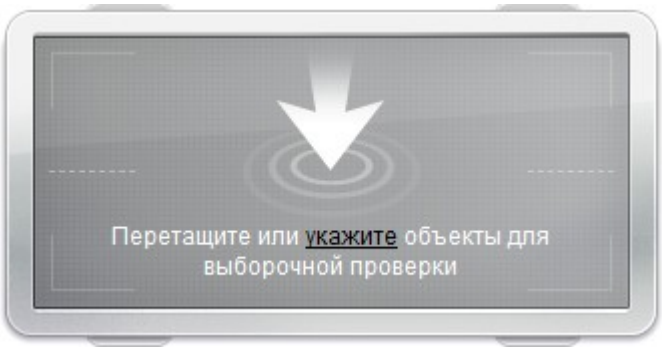

Рисунок 11. Область окна Проверка, в которую нужно перетащить объект для проверки

- *Чтобы проверить объект на вирусы с помощью гаджета,*

  перетащите объект проверки на гаджет.

  Процесс выполнения задачи будет отображаться в окне **Менеджер задач**.

КАК ВЫПОЛНИТЬ ПОЛНУЮ ПРОВЕРКУ КОМПЬЮТЕРА НА ВИРУСЫ

Вы можете запустить полную проверку на вирусы следующими способами:

- с помощью ранее созданного ярлыка (см. стр. 78);
- из главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37).

- *Чтобы запустить полную проверку с помощью ярлыка, выполните следующие действия:*

  1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
  2. Двойным щелчком мыши на ярлыке запустите проверку.

- *Чтобы запустить полную проверку из главного окна программы, выполните следующие действия:*

  1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.
  2. В открывшемся окне **Проверка** в блоке **Полная проверка** нажмите на кнопку .

КАК ПРОВЕРИТЬ КОМПЬЮТЕР НА УЯЗВИМОСТИ

Уязвимости – это незащищенные места программного кода, которые злоумышленники могут использовать в своих целях: например, копировать данные, используемые программами с незащищенным кодом. Проверка вашего компьютера на наличие потенциальных уязвимостей позволяет найти такие «слабые места» в защите компьютера. Найденные уязвимости рекомендуется устранить.

Запустить поиск уязвимостей вы можете следующими способами:

- из главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- с помощью ранее созданного ярлыка (см. стр. 78).

Чтобы запустить задачу с помощью ярлыка, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
2. Двойным щелчком мыши на ярлыке запустите задачу поиска уязвимостей.

Чтобы запустить задачу из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.
2. В открывшемся окне **Проверка** в блоке **Поиск уязвимостей** нажмите на кнопку  .

Как защитить ваши личные данные от кражи

С помощью Kaspersky Internet Security вы можете защитить от кражи злоумышленниками свои личные данные, например следующие:

- пароли, имена пользователя и другие регистрационные данные;
- номера счетов и кредитных карт.

В состав Kaspersky Internet Security входят следующие компоненты и инструменты, позволяющие защитить ваши личные данные:

- Анти-Фишинг. Защищает от кражи данных с использованием фишинга.
- Виртуальная клавиатура. Предотвращает перехват данных, вводимых с клавиатуры.
- Родительский контроль (см. стр. 155). Ограничивает пересылку личных данных через интернет.

В этом разделе

Защита от фишинга

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Веб-Антивирус, Анти-Спам и IM-Антивирус. «Лаборатория Касперского» рекомендует включить проверку на фишинг при работе всех компонентов защиты.

Чтобы включить защиту от фишинга при работе Веб-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. Откроется окно **Веб-Антивирус**.
5. В открывшемся окне на закладке **Общие** в блоке **Проверка ссылок** установите флажок **Проверять веб-страницы на наличие фишинга**.

Чтобы включить защиту от фишинга при работе IM-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
3. В правой части окна в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

Чтобы включить защиту от фишинга при работе Анти-Спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. В открывшемся окне на закладке **Точные методы** в блоке **Считать спамом следующие сообщения** установите флажок **С элементами фишинга**.

ЗАЩИТА ОТ ПЕРЕХВАТА ДАННЫХ С КЛАВИАТУРЫ

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, при совершении покупок в интернет-магазинах, при использовании интернет-банкинга.

В таких случаях существует опасность перехвата персональной информации с помощью аппаратных перехватчиков либо клавиатурных шпионов – программ, регистрирующих нажатие клавиш.

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.

Многие программы-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Виртуальная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана.

Виртуальная клавиатура защищает от перехвата персональной информации только при работе с интернет-браузерами Microsoft Internet Explorer, Mozilla Firefox и Google Chrome.

Виртуальная клавиатура имеет следующие особенности:

- На клавиши виртуальной клавиатуры нужно нажимать с помощью мыши.
- В отличие от настоящей клавиатуры, на виртуальной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы использовать комбинации клавиш (например, **ALT+F4**), нужно сначала нажать первую клавишу (например, **ALT**), затем следующую (например, **F4**), а затем повторно нажать первую клавишу. Повторное нажатие заменяет отпускание клавиши на настоящей клавиатуре.
- На виртуальной клавиатуре язык ввода переключается с помощью сочетания клавиш **CTRL+SHIFT** (при этом на клавишу **SHIFT** надо нажимать правой клавишей мыши) или **CTRL+LEFT ALT** (на клавишу **LEFT ALT** надо нажимать правой клавишей мыши), в зависимости от установленных параметров.

Открыть виртуальную клавиатуру можно следующими способами:

- из контекстного меню значка программы;

- из главного окна программы;
- из окна браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome;
- с помощью комбинации клавиш.

Чтобы открыть виртуальную клавиатуру из контекстного меню значка программы,

выберите пункт **Инструменты** →**Виртуальная клавиатура** в контекстном меню значка программы.

Чтобы открыть виртуальную клавиатуру из главного окна программы,

в нижней части главного окна программы выберите раздел **Виртуальная клавиатура**.

Чтобы открыть виртуальную клавиатуру из окна браузера,

нажмите на кнопку  **Виртуальная клавиатура** в панели инструментов браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome.

Чтобы открыть виртуальную клавиатуру с помощью компьютерной клавиатуры,

нажмите комбинацию клавиш **CTRL+ALT+SHIFT+P**.

Защита конфиденциальных данных, вводимых на веб-сайтах

Для защиты конфиденциальных данных, которые вы вводите на веб-сайтах (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), Kaspersky Internet Security предлагает открывать такие веб-сайты в безопасном браузере.

Вы можете включить контроль доступа к сервисам интернет-банкинга (см. раздел «Контроль обращения к сервисам интернет-банкинга» на стр. 102) для автоматического определения банковских веб-сайтов, а также запускать безопасный браузер вручную.

Запустить безопасный браузер можно следующими способами:

- из главного окна Kaspersky Internet Security (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- с помощью ярлыка на рабочем столе (см. раздел «Создание ярлыка безопасной среды на рабочем столе» на стр. 152).

Чтобы запустить безопасный браузер из главного окна Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасная среда**.
3. В открывшемся окне нажмите на кнопку **Запустить безопасный браузер**.

Что делать, если вы подозреваете, что объект заражен вирусом

Если вы подозреваете, что объект может быть заражен, проверьте его с помощью Kaspersky Internet Security (см. раздел «Как проверить на вирусы файл, папку, диск или другой объект» на стр. 51).

Если в результате проверки программа сообщит, что объект не заражен, но вы подозреваете обратное, вы можете выполнить одно из следующих действий:

- Поместить объект на *карантин*. Объекты, помещенные на карантин, не представляют угрозу для вашего компьютера. Возможно, после обновления баз Kaspersky Internet Security сможет однозначно определить угрозу и обезвредить ее.

- Отправить объект в *Вирусную лабораторию*. Специалисты Вирусной лаборатории проверят объект и, если он действительно заражен вирусом, внесут описание нового вируса в базы, которые будут загружены программой в процессе обновления (см. раздел «Как обновить базы и модули программы» на стр. 50).

Поместить файл на карантин можно двумя способами:

- по кнопке **Поместить на карантин** в окне **Карантин**;

- с помощью контекстного меню файла.

Чтобы поместить файл на карантин из окна Карантин, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Карантин**.

3. На закладке **Карантин** нажмите на кнопку **Поместить на карантин**.

4. В открывшемся окне выберите файл, который нужно поместить на карантин.

Чтобы поместить файл на карантин с помощью контекстного меню, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с файлом, который нужно поместить на карантин.

2. По правой клавише мыши откройте контекстное меню файла и выберите пункт **Поместить на карантин**.

Чтобы отправить файл в Вирусную лабораторию, выполните следующие действия:

1. Перейдите на страницу отправки запроса в Вирусную лабораторию (http://support.kaspersky.ru/virlab/helpdesk.html).

2. Следуйте инструкциям, приведенным на странице, чтобы отправить запрос.

Как запустить неизвестную программу без вреда для системы

Программы, в безопасности которых вы не уверены, рекомендуется запускать в безопасной среде.

Безопасная среда изолирована от основной операционной системы компьютера. При работе в безопасной среде реальные объекты операционной системы не подвергаются изменениям. Поэтому, если вы запустите в безопасной среде зараженную программу, ее действия не повлияют на операционную систему компьютера.

Вы можете запустить безопасную среду в виде отдельного рабочего стола (см. стр. 149) или запустить отдельную программу в безопасном режиме на основном рабочем столе.

Программы, запущенные в безопасном режиме на основном рабочем столе, обозначены зеленой рамкой вокруг окна программы, а также имеют признак безопасного запуска в списке программ, контролируемых Контролем программ (см. раздел «Контроль программ» на стр. 109).

После завершения работы программы будет произведена автоматический откат всех изменений, сделанных в ходе работы этой программы.

- *Чтобы запустить программу в безопасном режиме из контекстного меню Microsoft Windows,*

  по правой клавише мыши откройте контекстное меню для выбранного объекта: ярлыка или исполняемого файла программы и выберите пункт **Запустить в безопасной среде**.

Что делать с большим количеством спам-сообщений

Если вы получаете большое количество нежелательной почты (спама), включите компонент Анти-Спам и установите для него рекомендуемый уровень безопасности.

- *Чтобы включить Анти-Спам и установить рекомендуемый уровень безопасности, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
  3. В правой части окна установите флажок **Включить Анти-Спам**.
  4. Убедитесь, что в блоке **Уровень безопасности** установлен уровень безопасности **Рекомендуемый**.

     Если установлен уровень безопасности **Низкий** или **Другой**, нажмите на кнопку **По умолчанию**. Уровень безопасности будет автоматически установлен в значение **Рекомендуемый**.

Что делать, если вы подозреваете, что ваш компьютер заражен

Если вы подозреваете, что в результате активности вредоносных программ или системных сбоев операционная система вашего компьютера была повреждена, используйте *Мастер восстановления системы*, устраняющий следы пребывания в системе вредоносных объектов. Специалисты «Лаборатории Касперского» рекомендуют также запускать мастер после лечения компьютера, чтобы убедиться, что все возникшие угрозы и повреждения устранены.

Мастер восстановления проверяет наличие в системе изменений и повреждений (например, изменения расширений файлов, блокировка сетевого окружения и панели управления). Причинами изменений и повреждений могут быть быть активность вредоносных программ, некорректная настройка системы, системные сбои или применение некорректно работающих программ-оптимизаторов системы.

После исследования мастер анализирует собранную информацию с целью выявления в системе повреждений, которые требуют немедленного вмешательства. По результатам исследования составляется список действий, которые следует выполнить, чтобы устранить повреждения. Мастер группирует действия по категориям с учетом серьезности обнаруженных проблем.

- *Чтобы запустить Мастер восстановления системы, выполните следующие действия:*

  1. Откройте главное окно программы (см. стр. 37).
  2. В нижней части окна выберите раздел **Инструменты**.
  3. В открывшемся окне в блоке **Восстановление после заражения** нажмите на кнопку **Выполнить**.

     Откроется окно Мастера восстановления системы.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Шаг 1. Запуск восстановления системы

Убедитесь, что в окне мастера выбран вариант **Провести поиск проблем, связанных с активностью вредоносного ПО**, и нажмите на кнопку **Далее**.

Шаг 2. Поиск проблем

Мастер выполняет поиск проблем и возможных повреждений, которые следует исправить. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для устранения проблем

Все найденные на предыдущем шаге повреждения группируются с точки зрения опасности, которую они представляют. Для каждой группы повреждений специалисты «Лаборатории Касперского» предлагают набор действий, выполнение которых поможет устранить повреждения. Всего выделено три группы действий:

- *Настоятельно рекомендуемые действия* помогут избавиться от повреждений, представляющих серьезную проблему. Рекомендуем вам выполнить все действия данной группы.
- *Рекомендуемые действия* направлены на устранение повреждений, которые могут представлять потенциальную опасность. Действия данной группы также рекомендуется выполнять.
- *Дополнительные действия* предназначены для устранения неопасных в данный момент повреждений системы, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение проблем

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение проблем может занять некоторое время. По завершении устранения проблем мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Как восстановить удаленный или вылеченный программой файл

«Лаборатория Касперского» не рекомендует восстанавливать удаленные и вылеченные файлы, поскольку они могут представлять угрозу для вашего компьютера.

Если необходимо восстановить удаленный или вылеченный файл, используется его резервная копия, созданная программой в ходе проверки.

Чтобы восстановить удаленный или вылеченный программой файл, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.
3. На закладке **Хранилище** выберите нужный файл в списке и нажмите на кнопку **Восстановить**.

Как создать и использовать диск аварийного восстановления

После установки Kaspersky Internet Security и первой проверки компьютера рекомендуется создать диск аварийного восстановления.

Диск аварийного восстановления представляет собой программу Kaspersky Rescue Disk, записанную на съемный носитель (компакт-диск или USB-устройство).

В дальнейшем вы сможете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

В этом разделе

Создание диска аварийного восстановления

Создание диска аварийного восстановления заключается в формировании образа диска (файла формата ISO) с актуальной версией программы Kaspersky Rescue Disk и его записи на съемный носитель.

Исходный образ диска можно загрузить с сервера «Лаборатории Касперского» или скопировать с локального источника.

Диск аварийного восстановления создается с помощью *Мастера создания и записи Kaspersky Rescue Disk*. Сформированный мастером файл образа rescuecd.iso сохраняется на жестком диске вашего компьютера:

- в операционной системе Microsoft Windows XP – в папке Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\;
- в операционных системах Microsoft Windows Vista и Microsoft Windows 7 – в папке ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

Чтобы создать диск аварийного восстановления, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Инструменты**.
3. В открывшемся окне в блоке **Kaspersky Rescue Disk** нажмите на кнопку **Создать**.

   Откроется окно **Мастер создания диска аварийного восстановления**.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера. Поиск существующего образа диска

В первом окне мастера представлена информация о программе Kaspersky Rescue Disk.

Если мастер обнаружит ранее созданный файл образа диска в предназначенной для этого папке (см. выше), то в первом окне мастера отобразится флажок **Использовать существующий образ**. Чтобы использовать найденный файл в качестве исходного образа диска и сразу перейти к шагу **Обновление файла образа** (см. ниже), установите этот флажок. Если вы не хотите использовать найденный образ диска, снимите этот флажок. Мастер перейдет к окну **Выбор источника образа диска**.

Шаг 2. Выбор источника образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

На этом шаге вам следует выбрать источник образа диска из предложенных вариантов:

- Если у вас уже есть записанный диск аварийного восстановления или его образ (файл формата ISO), сохраненный на вашем компьютере или на ресурсе локальной сети, выберите вариант **Копировать образ с локального или сетевого диска**.
- Если у вас нет файла образа диска аварийного восстановления, и вы хотите загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 175 МБ), выберите вариант **Загрузить образ с сервера «Лаборатории Касперского»**.

Шаг 3. Копирование (загрузка) образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

Если на предыдущем шаге вы выбрали вариант **Копировать образ с локального или сетевого диска**, нажмите на кнопку **Обзор**. Указав путь к файлу, нажмите на кнопку **Далее**. В окне мастера будет отображен процесс копирования образа диска.

Если на предыдущем шаге вы выбрали вариант **Загрузить образ с сервера «Лаборатории Касперского»**, то процесс загрузки образа диска отображается сразу.

По завершении копирования или загрузки образа диска мастер автоматически переходит к следующему шагу.

Шаг 4. Обновление файла образа диска

Процедура обновления файла образа диска включает в себя следующие действия:

- обновление антивирусных баз;
- обновление конфигурационных файлов.

Конфигурационные файлы определяют возможность загрузки компьютера со съемного носителя (например, CD / DVD-диска или USB-устройства с Kaspersky Rescue Disk), полученного в результате работы мастера.

При обновлении антивирусных баз используются базы, полученные при последнем обновлении Kaspersky Internet Security. Если базы устарели, рекомендуется выполнить задачу обновления и запустить Мастер создания и записи Kaspersky Rescue Disk заново.

Для начала обновления файла образа нажмите на кнопку **Далее**. В окне мастера будет отображен ход выполнения обновления.

Шаг 5. Запись образа диска на носитель

На этом шаге мастер проинформирует вас об успешном создании образа диска и предложит записать образ диска на носитель.

Укажите носитель для записи Kaspersky Rescue Disk:

- Для записи на CD / DVD-диск выберите вариант **Записать на CD/DVD диск** и укажите диск, на который вы хотите записать образ диска.
- Для записи на USB-устройство выберите вариант **Записать на USB-устройство** и укажите устройство, на которое вы хотите записать образ диска.

> «Лаборатория Касперского» не рекомендует записывать образ диска на устройства, не предназначенные исключительно для хранения данных, например, смартфоны, мобильные телефоны, КПК, MP3-плееры. В дальнейшем такие устройства, использованные для записи образа диска, могут работать некорректно.

- Для записи на жесткий диск на вашем компьютере или на другом компьютере, к которому вы имеете доступ по сети, выберите вариант **Сохранить образ в файл на локальном или сетевом диске** и укажите папку, в которую вы хотите записать образ диска, и имя файла формата ISO.

Шаг 6. Завершение работы мастера

Для завершения работы мастера нажмите на кнопку **Завершить**. Созданный диск аварийного восстановления вы можете использовать для загрузки компьютера (см. стр. 62), если в результате действий вирусов или вредоносных программ невозможно выполнить загрузку компьютера и запуск Kaspersky Internet Security в обычном режиме.

Загрузка компьютера с помощью диска аварийного восстановления

Если в результате вирусной атаки невозможно загрузить операционную систему, воспользуйтесь диском аварийного восстановления.

Для загрузки операционной системы необходим CD / DVD-диск или USB-устройство с записанной на него программой Kaspersky Rescue Disk (см. раздел «Создание диска аварийного восстановления» на стр. 60).

Загрузка компьютера со съемного носителя не всегда возможна. В частности, она не поддерживается некоторыми устаревшими моделями компьютеров. Прежде чем выключить компьютер для последующей загрузки со съемного носителя, уточните возможность такой загрузки.

- *Чтобы загрузить компьютер с помощью диска аварийного восстановления, выполните следующие действия:*

1. В параметрах BIOS включите загрузку с CD / DVD-диска или USB-устройства (подробную информацию можно получить из документации к материнской плате вашего компьютера).

2. Поместите в дисковод зараженного компьютера CD / DVD-диск или подключите USB-устройство с предварительно записанной программой Kaspersky Rescue Disk.

3. Перезагрузите компьютер.

Более подробную информацию об использовании диска аварийного восстановления можно найти в руководстве пользователя Kaspersky Rescue Disk.

КАК ПРОСМОТРЕТЬ ОТЧЕТ О РАБОТЕ ПРОГРАММЫ

Kaspersky Internet Security ведет отчеты о работе каждого своего компонента. С помощью отчета вы можете получить статистическую информацию о работе программы (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время программа обновлялась, сколько обнаружено спам-сообщений и многое другое).

При работе на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вы можете открыть отчеты с помощью Kaspersky Gadget. Для этого Kaspersky Gadget должен быть настроен таким образом, чтобы одной из его кнопок была назначена функция открывания окна отчетов (см. раздел «Как использовать Kaspersky Gadget» на стр. 65).

- *Чтобы просмотреть отчет о работе программы, выполните следующие действия:*

1. Откройте окно **Отчеты** одним из следующих способов:

   - перейдите по ссылке **Отчеты** в верхней части главного окна программы;

   - нажмите на кнопку со значком **Отчеты** в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

   В окне **Отчеты** отображаются отчеты о работе программы в виде диаграмм.

2. Если нужно просмотреть подробный отчет о работе программы (например, о работе каждого из ее компонентов), нажмите на кнопку **Подробный отчет**, расположенную в нижней части окна **Отчет**.

   Откроется окно **Подробный отчет**, в котором данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты группировки записей.

КАК ВОССТАНОВИТЬ СТАНДАРТНЫЕ ПАРАМЕТРЫ РАБОТЫ ПРОГРАММЫ

Вы в любое время можете восстановить параметры работы Kaspersky Internet Security, рекомендуемые «Лабораторией Касперского». Восстановление параметров осуществляется с помощью *Мастера настройки программы*.

В результате работы мастера для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**. При восстановлении рекомендуемого уровня безопасности вы можете выборочно сохранять ранее сделанные настройки параметров для компонетов программы.

Чтобы восстановить стандартные параметры работы программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. Запустите Мастер настройки программы одним из следующих способов:
   - перейдите по ссылке **Восстановить** в нижней части окна;
   - в левой части окна выберите раздел **Дополнительные параметры**, подраздел **Управление параметрами** и нажмите на кнопку **Восстановить** в блоке **Восстановление стандартных параметров**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Нажмите на кнопку **Далее**, чтобы продолжить работу мастера.

Шаг 2. Восстановление параметров

В этом окне мастера представлены компоненты защиты Kaspersky Internet Security, параметры которых были изменены пользователем или накоплены Kaspersky Internet Security в результате обучения компонентов защиты Сетевой экран и Анти-Спам. Если для какого-либо компонента были сформированы уникальные параметры, они также будут представлены в окне.

В число уникальных параметров входят списки разрешенных и запрещенных фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, правила исключений защиты для компонентов программы, правила фильтрации пакетов и программ Сетевого экрана.

Уникальные параметры формируются в процессе работы с Kaspersky Internet Security с учетом индивидуальных задач и требований безопасности. «Лаборатория Касперского» рекомендует сохранять уникальные параметры при восстановлении первоначальных параметров программы.

Установите флажки для тех параметров, которые нужно сохранить и нажмите на кнопку **Далее**.

Шаг 3. Анализ системы

На данном этапе производится сбор информации о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в системе.

По завершении анализа мастер автоматически переходит к следующему шагу.

Шаг 4. Завершение восстановления

Для завершения работы мастера нажмите на кнопку **Завершить**.

Как перенести параметры программы в Kaspersky Internet Security, установленный на другом компьютере

Настроив программу, вы можете применить параметры ее работы к Kaspersky Internet Security, установленному на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково. Это полезно, например, в случае, когда Kaspersky Internet Security установлен и на домашнем, и на офисном компьютере.

Параметры работы программы сохраняются в конфигурационном файле, который вы можете перенести с одного компьютера на другой.

Перенос параметров Kaspersky Internet Security с одного компьютера на другой производится в три этапа:

1. Сохранение параметров программы в конфигурационном файле.
2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на съемном носителе).
3. Применение параметров из конфигурационного файла к программе, установленной на другом компьютере.

Чтобы экспортировать текущие параметры работы Kaspersky Internet Security, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Управление параметрами**.
3. В правой части окна нажмите на кнопку **Сохранить**.
4. В открывшемся окне введите название конфигурационного файла и укажите место его сохранения.
5. Нажмите на кнопку **ОК**.

Чтобы импортировать параметры работы из конфигурационного файла, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Управление параметрами**.
3. В правой части окна нажмите на кнопку **Загрузить**.
4. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Kaspersky Internet Security.
5. Нажмите на кнопку **ОК**.

КАК ИСПОЛЬЗОВАТЬ KASPERSKY GADGET

При использовании Kaspersky Internet Security на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вам доступен Kaspersky Gadget (далее также *гаджет*).После установки Kaspersky Internet Security на компьютер под управлением операционной системы Microsoft Windows 7 гаджет появляется на рабочем столе автоматически. После установки программы на компьютер под управлением операционной системы Microsoft Windows Vista гаджет нужно добавить на боковую панель Microsoft Windows вручную (см. документацию на операционную систему).

Цветовой индикатор гаджета сигнализирует о состоянии защиты вашего компьютера, так же, как индикатор, расположенный в главном окне программы (см. раздел «Диагностика и устранение проблем в защите компьютера» на стр. 44). Зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Серый цвет индикатора означает, что работа программы остановлена.

Во время обновления баз и модулей программы в центре гаджета отображается значок вращающегося глобуса.

С помощью гаджета вы можете выполнять следующие действия:

- возобновить работу программы, если она была приостановлена;
- открывать главное окно программы;
- проверять отдельные объекты на вирусы;
- открывать окно просмотра новостей.

Также вы можете настроить кнопки гаджета, чтобы выполнять дополнительные действия:

- запускать обновление;
- изменять параметры работы программы;
- просматривать отчеты программы;
- переключаться в безопасную среду (только для 32-битных операционных систем);
- просматривать отчеты Родительского контроля;
- просматривать информацию о сетевой активности (мониторинг сети) и об активности программ;
- приостанавливать защиту;
- открывать виртуальную клавиатуру;
- открывать окно Менеджера задач.

Чтобы запустить программу с помощью гаджета,

нажмите на значок **Включить**, расположенный в центре гаджета.

Чтобы открыть главное окно программы с помощью гаджета,

нажмите на изображение монитора в центре гаджета.

Чтобы проверить объект на вирусы с помощью гаджета,

перетащите объект проверки на гаджет.

Процесс выполнения задачи будет отображаться в окне **Менеджер задач**.

Чтобы открыть окно просмотра новостей с помощью гаджета,

нажмите на значок , который отображается в центре гаджета при появлении новости.

Чтобы настроить гаджет, выполните следующие действия:

1. Откройте окно настройки гаджета, нажав на значок , появляющийся в правом верхнем углу блока с гаджетом при наведении курсора мыши.
2. В раскрывающихся списках, соответствующих кнопкам гаджета, выберите действия, которые должны выполняться при нажатии на кнопки гаджета.
3. Нажмите на кнопку **ОК**.

Как проверить репутацию программы

Kaspersky Internet Security позволяет проверить репутацию программ у пользователей во всем мире. В состав репутации программы входят следующие показатели:

- название производителя;
- информация о цифровой подписи (доступно при наличии цифровой подписи);
- информация о группе, в которую программа помещена Контролем программ или большинством пользователей Kaspersky Security Network;
- количество пользователей Kaspersky Security Network, использующих программу (доступно, если программа отнесена к группе Доверенные в базе Kaspersky Security Network);
- время, когда программа стала известна в Kaspersky Security Network;
- страны, в которых программа наиболее всего распространена.

Для проверки репутации программы требуется, чтобы при установке Kaspersky Internet Security вы согласились участвовать в Kaspersky Security Network (см. стр. 188).

Чтобы узнать репутацию программы,

откройте контекстное меню исполняемого файла программы и выберите пункт **Посмотреть репутацию в KSN**.

См. также

Kaspersky Security Network 187

РАСШИРЕННАЯ НАСТРОЙКА ПРОГРАММЫ

Этот раздел содержит подробную информацию о том, как настроить параметры каждого компонента программы.

В ЭТОМ РАЗДЕЛЕ

ОСНОВНЫЕ ПАРАМЕТРЫ ЗАЩИТЫ

В окне настройки программы, в подразделе **Основные параметры** раздела **Центр защиты** вы можете выполнить следующие операции:

- отключить все компоненты защиты (см. раздел «Включение и выключение защиты» на стр. 45);
- выбрать интерактивный или автоматический режим защиты (см. раздел «Выбор режима защиты» на стр. 70);
- ограничить доступ пользователей к программе с помощью пароля (см. раздел «Ограничение доступа к Kaspersky Internet Security» на стр. 69);
- отключить или включить автоматический запуск программы при старте операционной системы (см. раздел «Включение и выключение автоматического запуска» на стр. 43);
- включить назначенную комбинацию клавиш для вывода на экран виртуальной клавиатуры (см. раздел «Защита от перехвата данных с клавиатуры» на стр. 55).

В ЭТОМ РАЗДЕЛЕ

ОГРАНИЧЕНИЕ ДОСТУПА К KASPERSKY INTERNET SECURITY

Персональный компьютер могут использовать несколько пользователей, имеющих разные уровни компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Internet Security и его параметрам может привести к снижению уровня защищенности компьютера в целом.

Чтобы ограничить доступ к программе, вы можете задать пароль и указать, при выполнении каких действий он должен запрашиваться:

- изменение параметров работы программы;
- включение и настройка Родительского контроля;
- завершение работы программы;
- удаление программы.

С осторожностью используйте пароль для ограничения доступа к удалению программы. Если вы забудете пароль, то удалить программу с компьютера будет сложно.

Чтобы ограничить доступ к Kaspersky Internet Security с помощью пароля, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Центр защиты**, подраздел **Основные параметры**.
3. В правой части окна в блоке **Защита паролем** установите флажок **Включить защиту паролем** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Защита паролем** введите пароль и укажите область, на которую будет распространяться ограничение доступа.

Выбор режима защиты

Kaspersky Internet Security по умолчанию работает в *автоматическом режиме защиты*. В этом режиме при возникновении опасных событий программа автоматически применяет действие, рекомендуемое экспертами «Лаборатории Касперского». Вы можете установить *интерактивный режим защиты*, чтобы Kaspersky Internet Security уведомлял вас обо всех опасных и подозрительных событиях в системе и предоставлял возможность самостоятельно принимать решение о том, какое из предлагаемых программой действий нужно применять.

Чтобы выбрать режим защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** подраздел **Основные параметры**.
3. В блоке **Интерактивная защита** снимите или установите флажки в зависимости от выбранного вами режима защиты:
   - чтобы установить интерактивный режим защиты, снимите флажок **Выбирать действие автоматически**;
   - чтобы установить автоматический режим защиты, установите флажок **Выбирать действие автоматически**.

     Чтобы Kaspersky Internet Security не удалял подозрительные объекты при работе в автоматическом режиме, установите флажок **Не удалять подозрительные объекты**.

Проверка компьютера

Проверка компьютера на уязвимости, вирусы и другие программы, представляющие угрозу, является одной из важнейших задач для обеспечения безопасности компьютера.

Необходимо регулярно проверять ваш компьютер на присутствие вирусов, и других программ, представляющих угрозу, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например из-за установленного низкого уровня защиты или по другим причинам.

Задача поиска уязвимостей заключается в диагностике безопасности операционной системы и обнаружении в программном обеспечении особенностей, которые могут быть использованы злоумышленниками для распространения вредоносных объектов и для доступа к персональным данным.

Этот раздел содержит информацию об особенностях и настройке задач проверки, а также об уровнях безопасности, методах и технологиях проверки.

В этом разделе

Проверка на вирусы

Для поиска вирусов и других программ, представляющих угрозу, в состав Kaspersky Internet Security включены следующие задачи:

- **Полная проверка**. Проверка всей системы. По умолчанию Kaspersky Internet Security проверяет следующие объекты:

- системную память;
- объекты, которые загружаются при старте операционной системы;
- резервное хранилище системы;
- почтовые базы;
- жесткие, съемные и сетевые диски.

- **Проверка важных областей**. По умолчанию Kaspersky Internet Security проверяет объекты, загрузка которых осуществляется при старте операционной системы.
- **Выборочная проверка**. Kaspersky Internet Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:
  - системную память;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище системы;
  - почтовые базы;
  - жесткие, съемные и сетевые диски;
  - любой выбранный файл или папку.

Задачи полной проверки и проверки важных областей являются специфическими. Для этих задач не рекомендуется изменять списки объектов для проверки.

Каждая задача проверки выполняется в заданной области и может запускаться по заранее сформированному расписанию. Кроме того, каждая задача проверки характеризуется уровнем безопасности (набором параметров, влияющих на тщательность проверки). По умолчанию всегда включен *сигнатурный режим* – режим поиска угроз с помощью записей в базах программы. В дополнение можно задействовать различные методы и технологии проверки.

После запуска задачи полной проверки или проверки важных областей процесс выполнения проверки отображается в окне **Проверка** в блоке под названием запущенной задачи, а также в Менеджере задач (см. раздел «Управление задачами проверки. Менеджер задач» на стр. 78).

При обнаружении угрозы Kaspersky Internet Security присваивает найденному объекту один из следующих статусов:

- Статус одной из вредоносных программ (например, *вирус*, *троянская программа*).
- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен объект или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам, или модифицированный код известного вируса.

После этого программа отображает уведомление (см. стр. 185) об обнаруженной угрозе и выполняет заданное действие. Вы можете изменить действие при обнаружении угрозы.

Если вы работаете в автоматическом режиме (см. раздел «Выбор режима защиты» на стр. 70), Kaspersky Internet Security при обнаружении опасных объектов будет автоматически применять действия, рекомендуемые специалистами «Лаборатории Касперского». Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Выбор режима защиты» на стр. 70), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky Internet Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

Информация о результатах проверки и обо всех событиях, произошедших при выполнении задач, записывается в отчет Kaspersky Internet Security (см. стр. 180).

В этом разделе

Изменение и восстановление уровня безопасности

В зависимости от ваших текущих потребностей вы можете выбрать один из предустановленных уровней безопасности или настроить параметры проверки на вирусы самостоятельно.

Настраивая параметры выполнения задачи проверки, вы всегда можете вернуться к рекомендуемым. Эти параметры считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень безопасности, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры проверки вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить рекомендуемые параметры проверки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

ФОРМИРОВАНИЕ РАСПИСАНИЯ ЗАПУСКА ПРОВЕРКИ

Для автоматического запуска задач проверки можно сформировать расписание: задать периодичность запуска задачи, время запуска (если это необходимо), а также дополнительные параметры.

Если по каким-либо причинам запуск невозможен (например, в это время компьютер был выключен), вы можете настроить автоматический запуск пропущенной задачи, как только это станет возможным. Кроме того, можно включить автоматическую приостановку проверки в том случае, если выключена экранная заставка или компьютер разблокирован. Данная возможность позволяет отложить запуск задачи до того момента, пока пользователь не закончит свою работу на компьютере. Таким образом, задача проверки не будет занимать ресурсы компьютера во время его работы.

Специальный режим Проверки во время простоя компьютера (см. раздел «Запуск задач в фоновом режиме» на стр. 169) позволяет запускать проверку системной памяти, системного раздела и объектов автозапуска в то время, когда компьютер не используется.

Чтобы настроить расписание запуска задачи проверки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Поиск уязвимостей**).
3. В правой части окна нажмите на кнопку **Режим запуска**.
4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и настройте режим запуска проверки, указав нужные значения параметра **Периодичность**.

Чтобы включить автоматический запуск пропущенной задачи, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Поиск уязвимостей**).
3. В правой части окна нажмите на кнопку **Режим запуска**.
4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Запускать пропущенные задачи**.

Чтобы запускать проверку только после того, как пользователь закончит свою работу, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Поиск уязвимостей**).

3. В правой части окна нажмите на кнопку **Режим запуска**.

4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Выполнять проверку по расписанию, когда компьютер заблокирован или включена экранная заставка**.

Формирование списка объектов для проверки

По умолчанию каждой задаче проверки на вирусы соответствует свой список объектов. К таким объектам могут относиться как объекты файловой системы компьютера (например, логические диски, почтовые базы), так и объекты других типов (например, сетевые диски). Вы можете внести в этот список изменения.

Если область проверки пуста или ни один из объектов, входящих в нее, не отмечен, то запустить задачу проверки невозможно.

- *Чтобы сформировать список объектов для задачи выборочной проверки, выполните следующие действия:*

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Проверка**.

3. В нижней части открывшегося окна по ссылке **укажите** откройте список объектов для проверки.

4. В открывшемся окне **Выборочная проверка** нажмите на кнопку **Добавить**.

5. В открывшемся окне **Выбор объекта для проверки** выберите нужный объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**. Чтобы исключить какие-либо объекты из списка проверки, снимите флажки рядом с ними.

   Вы можете также напрямую перетащить файлы для проверки в специально отмеченную область в разделе **Проверка**.

- *Чтобы сформировать список объектов для задач полной проверки, проверки важных областей или поиска уязвимостей, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу проверки (**Полная проверка**, **Проверка важных областей** или **Поиск уязвимостей**).

3. В правой части окна нажмите на кнопку **Объекты для проверки**.

4. В открывшемся окне **Объекты для проверки** с помощью кнопок **Добавить**, **Изменить**, **Удалить** сформируйте список. Чтобы исключить какие-либо объекты из списка проверки, снимите флажки рядом с ними.

   Объекты, добавленные в список по умолчанию, невозможно отредактировать или удалить.

Выбор методов проверки

При проверке компьютера на вирусы всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky Internet Security сравнивает найденный объект с записями в базах.

Для повышения эффективности поиска предназначены дополнительные методы проверки: *эвристический анализ* (анализ активности, которую объект производит в системе) и *поиск руткитов* (утилит, обеспечивающих сокрытие вредоносных программ в операционной системе).

Чтобы выбрать нужные методы проверки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выберите нужные методы проверки.

Выбор технологии проверки

В дополнение к методам проверки вы можете задействовать специальные технологии проверки объектов, которые позволяют оптимизировать скорость проверки на вирусы за счет исключения файлов, не измененных с момента последней проверки.

Чтобы выбрать технологии проверки объектов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужные значения.

Изменение действия при обнаружении угрозы

При обнаружении зараженных объектов программа выполняет заданное действие.

Чтобы изменить действие при обнаружении угрозы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. В правой части окна в блоке **Действие при обнаружении угрозы** выберите нужный вариант.

Запуск проверки с правами другого пользователя

По умолчанию задачи проверки запускаются от имени учетной записи, с правами которой вы зарегистрировались в системе. Однако может возникнуть необходимость запустить задачу с правами другого пользователя. Вы можете указать учетную запись, с правами которой будет запускаться каждая задача проверки.

Чтобы запускать проверку с правами другого пользователя, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Поиск уязвимостей**).
3. В правой части окна нажмите на кнопку **Режим запуска**.

4. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**. В полях ниже задайте имя пользователя и пароль.

Изменение типа проверяемых объектов

Указывая тип проверяемых объектов, вы определяете, файлы какого формата будут проверяться при выполнении выбранной задачи проверки.

При выборе типа файлов помните 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, EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.

- Злоумышленник может отправить вирус на ваш компьютер в исполняемом файле, переименованном в txt-файл. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл будет пропущен. 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 EXE-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).

3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Область действия** в блоке **Типы файлов** выберите нужный вариант.

Проверка составных файлов

Распространенная практика сокрытия вирусов – внедрение их в составные файлы, например архивы, инсталляционные пакеты, вложенные OLE-объекты, файлы почтовых форматов. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы или только новые. Для выбора перейдите по ссылке, расположенной рядом с названием объекта. Она меняет свое значение при нажатии на нее левой клавишей мыши. Если установлен режим проверки только новых и измененных файлов (см. стр. 77), ссылки для выбора проверки всех или только новых файлов будут недоступны.

Вы можете ограничить максимальный размер проверяемого составного файла. Составные файлы, размер которых превышает заданное значение, проверяться не будут.

При извлечении из архивов файлы больших размеров будут проверяться на вирусы даже в том случае, если установлен флажок **Не распаковывать составные файлы большого размера**.

Чтобы изменить список проверяемых составных файлов, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).

3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** выберите нужные типы проверяемых составных файлов.

Чтобы задать максимальный размер составных файлов, которые будут проверяться, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
5. В открывшемся окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и укажите максимальный размер проверяемых файлов.

Оптимизация проверки

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

Кроме того, можно задать ограничение длительности проверки одного объекта. По истечении заданного времени объект будет исключен из текущей проверки (кроме архивов и файлов, в состав которых входит несколько объектов).

Чтобы проверять только новые и измененные файлы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

Чтобы задать ограничение длительности проверки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Проверка важных областей** или **Выборочная проверка**).
3. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Пропускать объекты, если их проверка длится более** и задайте длительность проверки одного файла.

Проверка съемных дисков при подключении

В последнее время широкое распространение получили вредоносные объекты, которые используют уязвимости операционной системы для распространения через локальные сети и съемные носители информации. Kaspersky Internet Security позволяет проверять на вирусы съемные диски при их подключении к компьютеру.

Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** раздел **Основные параметры**.
3. В блоке **Проверка съемных дисков при подключении** выберите действие и, если необходимо, укажите максимальный размер проверяемого диска в поле ниже.

Создание ярлыка для запуска задачи

Для быстрого запуска задач полной и быстрой проверок на вирусы, а также поиска уязвимостей в программе предусмотрена возможность создания ярлыков. Это позволяет запускать нужную задачу проверки, не открывая главного окна программы или контекстного меню.

Чтобы создать ярлык для запуска задачи проверки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** раздел **Основные параметры**.
3. В правой части окна в блоке **Быстрый запуск задач** нажмите на кнопку **Создать ярлык** рядом с названием нужной задачи (**Проверка важных областей**, **Полная проверка** или **Поиск уязвимостей**).
4. В открывшемся окне укажите путь для сохранения ярлыка и его имя. По умолчанию ярлык создается с именем задачи в папке Мой компьютер текущего пользователя компьютера.

Поиск уязвимостей

Уязвимости в операционной системе могут появляться, например, из-за ошибок программирования, ненадежных паролей, действий вредоносных программ. В рамках поиска уязвимостей программа производит различные меры безопасности, например, изучение системы, анализ параметров операционной системы и браузера, поиск уязвимых служб.

Диагностика может занять некоторое время. После ее проведения обнаруженные проблемы анализируются с точки зрения их опасности для системы.

После запуска задачи поиска уязвимостей (см. стр. 53) процесс ее выполнения отображается в окне **Проверка** в блоке **Поиск уязвимостей**, а также в Менеджере задач (см. раздел «Управление задачами проверки. Менеджер задач» на стр. 78).

Информация о результатах выполнения задачи поиска уязвимостей записывается в отчет Kaspersky Internet Security (см. стр. 180).

Как и для задач проверки на вирусы, для задачи поиска уязвимостей можно задать расписание запуска, сформировать список объектов для проверки (см. стр. 74), выбрать учетную запись (см. раздел «Запуск проверки с правами другого пользователя» на стр. 75) и создать ярлык для быстрого запуска задачи. По умолчанию в качестве объекта проверки выбраны установленные на компьютере программы.

Управление задачами проверки. Менеджер задач

В Менеджере задач отображается информация о последних выполненных или выполняемых задачах проверки компьютера (например, проверка на вирусы, поиск уязвимостей, поиск руткитов, лечение активного заражения).

С помощью Менеджера задач вы можете посмотреть процесс и результат выполнения задачи или остановить задачу. Для некоторых задач также доступны дополнительные действия (например, по окончании поиска уязвимостей вы можете открыть список обнаруженных уязвимостей и исправить их).

Чтобы открыть Менеджер задач, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Проверка**.
3. В открывшемся окне **Проверка** нажмите на кнопку **Менеджер задач** в верхнем правом углу окна.

Обновление

Обновление баз и программных модулей Kaspersky Internet Security обеспечивает актуальность защиты вашего компьютера. Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Internet Security. Чтобы своевременно обнаруживать новые угрозы, вам нужно регулярно обновлять базы и программные модули.

Для регулярного обновления требуется действительная лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

В процессе обновления программа загружает и устанавливает на ваш компьютер следующие объекты:

- Базы Kaspersky Internet Security.

  Защита информации обеспечивается на основании баз данных, содержащих сигнатуры угроз, описания сетевых атак, а также информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании опасных объектов на вашем компьютере. Базы регулярно пополняются записями о новых угрозах и способах борьбы с ними. Поэтому настоятельно рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Internet Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Программные модули.

  Помимо баз Kaspersky Internet Security, можно обновлять и программные модули. Обновления программных модулей устраняют уязвимости Kaspersky Internet Security, добавляют новые функции или улучшают существующие.

В процессе обновления программные модули и базы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и программные модули отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Перед обновлением баз Kaspersky Internet Security создает их резервную копию на тот случай, если вы захотите вернуться к использованию баз предыдущей версии (см. раздел «Откат последнего обновления» на стр. 82).

Информация о текущем состоянии баз Kaspersky Internet Security отображается в разделе **Обновление** главного окна программы.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Internet Security (см. стр. 180).

Вы можете выбрать источник обновлений (см. раздел «Выбор источника обновлений» на стр. 80), а также настроить параметры автоматического запуска обновления.

В этом разделе

Выбор источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и программных модулей Kaspersky Internet Security.

Основным источником обновлений служат серверы обновлений «Лаборатории Касперского», на которые выкладываются обновления баз и программных модулей для всех продуктов «Лаборатории Касперского».

Для успешной загрузки обновлений с серверов ваш компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, может потребоваться настройка параметров подключения к нему (см. раздел «Настройка параметров прокси-сервера» на стр. 127).

Одновременно с обновлением Kaspersky Internet Security вы можете копировать обновления баз и программных модулей, полученные с серверов «Лаборатории Касперского», в локальную папку (см. раздел «Обновление из папки общего доступа» на стр. 81), а затем предоставлять доступ к ним другим компьютерам сети. Это позволит экономить интернет-трафик.

Если серверы обновлений «Лаборатории Касперского» вам недоступны (например, ограничен доступ к интернету), вы можете обратиться в наш центральный офис (http://www.kaspersky.ru/contacts) и узнать адреса партнеров «Лаборатории Касперского», которые смогут предоставить вам обновления на съемном диске.

При заказе обновлений на съемных дисках обязательно уточняйте, хотите ли вы получить обновления программных модулей.

Добавление источника обновлений

По умолчанию список источников обновлений содержит только серверы обновлений «Лаборатории Касперского». Вы можете добавить в качестве источника обновлений локальную папку или другой сервер. Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Internet Security обращается к ним последовательно по списку и загружает обновления с первого доступного источника.

Чтобы добавить источник обновлений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В правой части окна нажмите на кнопку **Источник обновлений**.
4. В открывшемся окне на закладке **Источник** откройте окно выбора, нажав на кнопку **Добавить**.
5. В открывшемся окне **Выбор источника обновлений** выберите папку, которая содержит обновления, или введите адрес сервера, с которого требуется загружать обновления, в поле **Источник**.

ВЫБОР РЕГИОНА СЕРВЕРА ОБНОВЛЕНИЙ

Если в качестве источника обновлений вы используете серверы «Лаборатории Касперского», можно выбрать предпочтительное для вас местоположение сервера для загрузки обновлений. Серверы «Лаборатории Касперского» расположены в нескольких странах мира.

Использование географически ближайшего к вам сервера обновления «Лаборатории Касперского» поможет сократить время получения обновлений и увеличить его скорость. По умолчанию используется информация о текущем регионе из реестра операционной системы. Вы можете выбрать регион вручную.

Чтобы выбрать регион сервера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В правой части окна нажмите на кнопку **Источник обновлений**.
4. В открывшемся окне на закладке **Источник** в блоке **Региональные параметры** выберите вариант **Выбрать из списка** и в раскрывающемся списке выберите ближайшую к вашему текущему местонахождению страну.

ОБНОВЛЕНИЕ ИЗ ПАПКИ ОБЩЕГО ДОСТУПА

Для экономии интернет-трафика можно настроить обновление Kaspersky Internet Security на компьютерах сети из папки общего доступа. При этом один из компьютеров сети получает пакет обновлений с серверов «Лаборатории Касперского» в интернете или с другого веб-ресурса, содержащего актуальный набор обновлений. Полученные обновления копируются в папку общего доступа, после чего другие компьютеры сети обращаются к этой папке для получения обновлений Kaspersky Internet Security.

При работе под гостевой учетной записью в операционной системе Microsoft Windows 7 обновления в папку общего доступа не копируются. Рекомендуется зайти под другой учетной записью, чтобы копирование обновлений было возможно.

Чтобы включить режим копирования обновлений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В блоке **Дополнительно** установите флажок **Копировать обновления в папку** и в поле ниже укажите путь к папке общего доступа, в которую будут помещаться полученные обновления. Вы также можете выбрать папку, нажав на кнопку **Обзор**.

Чтобы загружать обновления для компьютера из указанной папки общего доступа, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В правой части окна нажмите на кнопку **Источник обновлений**.
4. В открывшемся окне на закладке **Источник** откройте окно выбора, нажав на кнопку **Добавить**.
5. В открывшемся окне **Выбор источника обновлений** выберите папку или введите полный путь к ней в поле **Источник**.
6. На закладке **Источник** снимите флажок **Серверы обновлений «Лаборатории Касперского»**.

Формирование расписания запуска обновления

Для автоматического запуска задачи обновления можно сформировать расписание: задать периодичность запуска задачи, время запуска (если это необходимо), а также дополнительные параметры.

Если по каким-либо причинам запуск невозможен (например, в это время компьютер был выключен), вы можете настроить автоматический запуск пропущенной задачи, как только это станет возможным.

Вы также можете отложить автоматический запуск задачи после старта программы. При этом все задачи по расписанию будут запускаться только по истечении указанного времени после старта Kaspersky Internet Security.

Специальный режим Проверки во время простоя компьютера (см. раздел «Запуск задач в фоновом режиме» на стр. 169) позволяет запускать автоматическое обновление в то время, когда компьютер не используется.

- *Чтобы настроить расписание запуска задачи обновления, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
  3. В правой части окна нажмите на кнопку **Режим запуска**.
  4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и настройте режим запуска обновления.

- *Чтобы включить автоматический запуск пропущенной задачи, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
  3. В правой части окна нажмите на кнопку **Режим запуска**.
  4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Запускать пропущенные задачи**.

- *Чтобы отложить запуск задач после старта программы, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
  3. В правой части окна нажмите на кнопку **Режим запуска**.
  4. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию**, затем в поле **Отложить запуск после старта программы на** укажите время, на которое нужно откладывать запуск задач.

Откат последнего обновления

После первого обновления Kaspersky Internet Security становится доступной функция отката к предыдущим базам.

Возможность отката обновления полезна, например, в случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Internet Security блокирует безопасную программу.

При повреждении баз Kaspersky Internet Security рекомендуется запустить задачу обновления, чтобы загрузить актуальный набор баз.

Чтобы вернуться к использованию предыдущей версии баз, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Обновление**.
3. В открывшемся окне **Обновление** нажмите на кнопку и в открывшемся меню выберите пункт **Откат к предыдущим базам**.

ЗАПУСК ОБНОВЛЕНИЯ С ПРАВАМИ ДРУГОГО ПОЛЬЗОВАТЕЛЯ

По умолчанию обновление запускается от имени учетной записи, с правами которой вы зарегистрировались в системе. Однако обновление Kaspersky Internet Security может производиться из источника, к которому у вас нет доступа (например, из сетевой папки, содержащей обновления) или нет прав авторизованного пользователя прокси-сервера. Вы можете запускать обновление Kaspersky Internet Security от имени пользователя, обладающего такими привилегиями.

Чтобы запускать обновление с правами другого пользователя, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В правой части окна нажмите на кнопку **Режим запуска**.
4. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**. В полях ниже задайте имя пользователя и пароль.

ИСПОЛЬЗОВАНИЕ ПРОКСИ-СЕРВЕРА

Если для выхода в интернет используется прокси-сервер, необходимо настроить его параметры для корректного обновления Kaspersky Internet Security.

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В правой части окна нажмите на кнопку **Источник обновлений**.
4. В открывшемся окне на закладке **Источник** нажмите на кнопку **Прокси-сервер**.
5. В открывшемся окне **Параметры прокси-сервера** настройте параметры прокси-сервера.

ФАЙЛОВЫЙ АНТИВИРУС

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках на наличие в них вирусов и других программ, представляющих угрозу.

Вы можете сформировать область защиты и выбрать уровень безопасности (набор параметров, влияющих на тщательность проверки).

При обращении пользователя или программы к файлу, который находится в области защиты, Файловый Антивирус проверяет наличие информации об этом файле в базах iChecker и iSwift и на основании полученных сведений принимает решение о необходимости проверки файла.

По умолчанию всегда включен *сигнатурный анализ* – режим поиска угроз с помощью записей в базах программы. В дополнение можно задействовать эвристический анализ и различные технологии проверки.

При обнаружении угрозы в файле Kaspersky Internet Security присваивает файлу один из следующих статусов:

- Статус, обозначающий тип обнаруженной вредоносной программы (например, *вирус*, *троянская программа*).

- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен файл или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.

После этого программа выводит на экран уведомление (см. стр. 185) об обнаруженной угрозе и выполняет над файлом действие, заданное в параметрах Файлового Антивируса. Вы можете изменить действие (см. стр. 88), которое должна выполнять программа при обнаружении угрозы.

Если вы работаете в автоматическом режиме (см. раздел «Выбор режима защиты» на стр. 70), Kaspersky Internet Security при обнаружении опасных объектов будет автоматически применять действия, рекомендуемые специалистами «Лаборатории Касперского». Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Выбор режима защиты» на стр. 70), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky Internet Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

В этом разделе

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.

Чтобы выключить использование Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна снимите флажок **Включить Файловый Антивирус**.

АВТОМАТИЧЕСКАЯ ПРИОСТАНОВКА РАБОТЫ ФАЙЛОВОГО АНТИВИРУСА

При выполнении работ, требующих значительных ресурсов операционной системы, работу Файлового Антивируса можно приостанавливать. Чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить автоматическую приостановку работы компонента в указанное время или при работе с определенными программами.

Приостановка работы Файлового Антивируса при конфликте с определенными программами является экстренной мерой. Если при работе компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru). Специалисты помогут вам наладить совместную работу Kaspersky Internet Security с другими программами на вашем компьютере.

Чтобы приостанавливать работу компонента в указанное время, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **По расписанию** и нажмите на кнопку **Расписание**.
5. В окне **Приостановка задачи** укажите время (в формате чч:мм), в течение которого защита будет приостановлена (поля **Приостановить в** и **Возобновить в**).

Чтобы приостанавливать работу компонента при запуске указанных программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**.
5. В окне **Программы** сформируйте список программ, при работе которых работа компонента будет приостановлена.

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ ФАЙЛОВОГО АНТИВИРУСА

Под областью защиты подразумеваются расположение и тип проверяемых файлов. По умолчанию Kaspersky Internet Security проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков.

Чтобы сформировать область защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Общие** в блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять Файловым Антивирусом:

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

   При выборе типа 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, EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
   - Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер 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 программы, представляющие угрозу.

5. В списке **Область защиты** выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, перейдите по ссылке **Добавить**.
   - Если вы хотите изменить расположение объекта, выберите объект в списке и перейдите по ссылке **Изменить**.

   Откроется окно **Выбор объекта для проверки**.

   - Если вы хотите удалить объект из списка проверяемых объектов, выберите объект в списке и перейдите по ссылке **Удалить**.

     Откроется окно подтверждения удаления.

6. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект в список проверяемых объектов, в окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **ОК**.
   - Если вы хотите изменить расположение объекта, в окне **Выбор объекта для проверки** измените путь к объекту в поле **Объект** и нажмите на кнопку **ОК**.
   - Если вы хотите удалить объект из списка проверяемых объектов, в окне подтверждения удаления нажмите на кнопку **Да**.

7. При необходимости повторите пункты 6 – 7 для добавления, изменения расположения или удаления объектов из списка проверяемых объектов.

8. Чтобы исключить объект из списка проверяемых объектов, в списке **Область защиты** снимите флажок рядом с ним. Объект при этом остается в списке проверяемых объектов, но исключается из проверки Файловым Антивирусом.

ИЗМЕНЕНИЕ И ВОССТАНОВЛЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ФАЙЛОВ

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности файлов и памяти или настроить параметры работы Файлового Антивируса самостоятельно.

Настраивая параметры работы Файлового Антивируса, всегда можно вернуться к рекомендуемым значениям. Эти параметры считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

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

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

- *Чтобы восстановить уровень безопасности файлов по умолчанию, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

ВЫБОР РЕЖИМА ПРОВЕРКИ ФАЙЛОВ

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять файлы. По умолчанию Kaspersky Internet Security использует интеллектуальный режим. Работая в этом режиме проверки файлов, Файловый Антивирус принимает решение о проверке файлов на основании анализа операций, которые пользователь выполняет над файлами, и типа файлов. Например, при работе с документом Microsoft Office Kaspersky Internet 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 программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим.

При выборе режима проверки нужно учитывать, с какими файлами вы работаете большую часть времени.

Использование эвристического анализа при работе Файлового Антивируса

При работе Файлового Антивируса всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky Internet Security сравнивает найденный объект с записями в базах.

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

- *Чтобы включить использование эвристического анализа, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки.

Выбор технологии проверки файлов

В дополнение к эвристическому анализу вы можете задействовать специальные технологии, которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

- *Чтобы выбрать технологии проверки объектов, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужные значения.

Изменение действия над зараженными файлами

При обнаружении зараженных объектов программа выполняет заданное действие.

- *Чтобы изменить действие над зараженными файлами, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна в блоке **Действие при обнаружении угрозы** выберите нужный вариант.

Проверка составных файлов Файловым Антивирусом

Распространенная практика сокрытия вирусов – внедрение их в составные файлы, например архивы, инсталляционные пакеты, вложенные OLE-объекты, файлы почтовых форматов. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы или только новые. Для выбора перейдите по ссылке, расположенной рядом с названием объекта. Она меняет свое значение при нажатии на нее левой клавишей мыши. Если установлен режим проверки только новых и измененных файлов, ссылки для выбора проверки всех или только новых файлов будут недоступны.

По умолчанию Kaspersky Internet Security проверяет только вложенные OLE-объекты.

При проверке составных файлов большого размера их предварительная распаковка может занять много времени. Это время можно сократить, включив распаковку составных файлов, превышающих заданный размер, в фоновом режиме. Если в ходе работы с таким файлом будет обнаружен вредоносный объект, Kaspersky Internet Security уведомит вас об этом.

Вы можете ограничить максимальный размер проверяемого составного файла. Составные файлы, размер которых превышает заданное значение, проверяться не будут.

При извлечении из архивов файлы больших размеров будут проверяться на вирусы даже в том случае, если установлен флажок **Не распаковывать составные файлы большого размера**.

- *Чтобы изменить список проверяемых составных файлов, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
  3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  4. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** выберите нужные типы проверяемых составных файлов.

- *Чтобы задать максимальный размер составных файлов, которые будут проверяться, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
  3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  4. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
  5. В окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и укажите максимальный размер проверяемых файлов.

- *Чтобы распаковывать составные файлы большого размера в фоновом режиме, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
  3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  4. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
  5. В окне **Составные файлы** установите флажок **Распаковывать составные файлы в фоновом режиме** и укажите минимальный размер файла.

Оптимизация проверки файлов

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

Чтобы проверять только новые и измененные файлы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Производительность** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие сообщения на наличие в них опасных объектов. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP, а также через защищенные соединения (SSL) по протоколам POP3 и IMAP (см. раздел «Проверка защищенных соединений» на стр. 125).

Индикатором работы компонента служит значок в области уведомлений панели задач, который принимает вид  каждый раз при проверке письма.

Почтовый Антивирус перехватывает и проверяет каждое почтовое сообщение, принимаемое или отправляемое пользователем. Если угрозы в почтовом сообщении не обнаружены, оно становится доступным для пользователя.

Вы можете указать типы сообщений, которые нужно проверять, и выбрать уровень безопасности (см. стр. 92) (набор параметров, влияющих на тщательность проверки).

По умолчанию всегда включен *сигнатурный анализ* – режим поиска угроз с помощью записей в базах программы. В дополнение к нему можно задействовать эвристический анализ. Кроме того, вы можете включить фильтрацию вложений (см. стр. 94), которая позволяет автоматически переименовывать или удалять файлы указанных типов.

При обнаружении угрозы в файле Kaspersky Internet Security присваивает файлу один из следующих статусов:

- Статус, обозначающий тип обнаруженной вредоносной программы (например, *вирус*, *троянская программа*).
- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен файл или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.

После этого программа блокирует почтовое сообщение, выводит на экран уведомление (см. стр. 185) об обнаруженной угрозе и выполняет действие, заданное в параметрах Почтового Антивируса. Вы можете изменить действие при обнаружении угрозы (см. раздел «Изменение действия над зараженными почтовыми сообщениями» на стр. 93).

Если вы работаете в автоматическом режиме (см. раздел «Выбор режима защиты» на стр. 70), Kaspersky Internet Security при обнаружении опасных объектов будет автоматически применять действия, рекомендуемые специалистами «Лаборатории Касперского». Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Выбор режима защиты» на стр. 70), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky Internet Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

Если лечение проходит успешно, почтовое сообщение становится доступным для работы. Если же лечение произвести не удалось, зараженный объект удаляется из почтового сообщения. Почтовый Антивирус помещает в тему почтового сообщения текст, уведомляющий о том, что почтовое сообщение обработано Kaspersky Internet Security.

Для почтовой программы Microsoft Office Outlook предусмотрен встраиваемый модуль расширения, позволяющий производить более тонкую настройку проверки почты.

Если вы используете почтовую программу The Bat!, Kaspersky Internet Security может использоваться наряду с другими антивирусными программами. При этом правила обработки почтового трафика настраиваются непосредственно в программе The Bat! и имеют преимущество перед параметрами защиты почты Kaspersky Internet Security.

При работе с остальными популярными почтовыми программами (в том числе с Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) Почтовый Антивирус проверяет почту на трафике по протоколам SMTP, POP3, IMAP и NNTP.

Обратите внимание, что при работе в почтовом клиенте Thunderbird не проверяются на вирусы почтовые сообщения, передаваемые по протоколу IMAP, в случае, если используются фильтры, перемещающие сообщения из папки **Входящие**.

В ЭТОМ РАЗДЕЛЕ

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.

Чтобы выключить использование Почтового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна снимите флажок **Включить Почтовый Антивирус**.

Формирование области защиты Почтового Антивируса

Под областью защиты подразумевается тип проверяемых почтовых сообщений, протоколы, трафик которых проверяет Kaspersky Internet Security, а также параметры интеграции Почтового Антивируса в систему.

По умолчанию Kaspersky Internet Security проверяет как входящие, так и исходящие почтовые сообщения, интегрируется в почтовые клиенты Microsoft Office Outlook и The Bat! и проверяет трафик почтовых протоколов POP3, SMTP, NNTP и IMAP.

Чтобы отключить проверку исходящей почты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Общие** в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

Если вы выбрали проверку только входящих сообщений, в самом начале работы с Kaspersky Internet Security рекомендуется проверить исходящую почту, поскольку на вашем компьютере могут быть почтовые черви, которые используют электронную почту для собственного распространения. Проверка исходящей почты позволит избежать неприятностей, связанных с неконтролируемой рассылкой зараженных почтовых сообщений с вашего компьютера.

Чтобы задать проверяемые протоколы и параметры интеграции Почтового Антивируса в систему, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Дополнительно** в блоке **Встраивание в систему** выберите нужные параметры.

Изменение и восстановление уровня безопасности почты

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности почты или настроить параметры работы Почтового Антивируса самостоятельно.

Специалисты «Лаборатории Касперского» не рекомендуют вам самостоятельно настраивать параметры работы Почтового Антивируса. В большинстве случаев достаточно выбрать другой уровень безопасности.

Настраивая параметры работы Почтового Антивируса, всегда можно вернуться к рекомендуемым значениям. Эти параметры считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

- *Чтобы изменить установленный уровень безопасности почты, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

- *Чтобы восстановить параметры защиты почты по умолчанию, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Использование эвристического анализа при работе Почтового Антивируса

При работе Почтового Антивируса всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky Internet Security сравнивает найденный объект с записями в базах.

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

- *Чтобы включить использование эвристического анализа, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Общие** в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки.

Изменение действия над зараженными почтовыми сообщениями

При обнаружении зараженных объектов программа выполняет заданное действие.

- *Чтобы изменить действие над зараженными почтовыми сообщениями, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна в блоке **Действие при обнаружении угрозы** выберите нужный вариант.

Фильтрация вложений в почтовых сообщениях

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

Чтобы настроить фильтрацию вложений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Фильтр вложений** выберите режим фильтрации вложений. При выборе последних двух режимов становится активным список типов файлов (расширений), в котором вы можете выбрать нужные типы или добавить маску нового типа.

   Чтобы добавить в список маску нового типа, перейдите по ссылке **Добавить**, откройте окно **Маска имени файла** и введите в нем нужные данные.

Проверка составных файлов Почтовым Антивирусом

Распространенная практика сокрытия вирусов – внедрение их в составные файлы, например архивы, инсталляционные пакеты, вложенные OLE-объекты, файлы почтовых форматов. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Вы можете включить или отключить проверку составных файлов, а также ограничить максимальный размер проверяемых составных файлов.

Если ваш компьютер не защищен какими-либо средствами локальной сети (выход в интернет осуществляется без участия прокси-сервера или сетевого экрана), отключать проверку составных файлов не рекомендуется.

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Общие** задайте нужные параметры.

Проверка почты в Microsoft Office Outlook

Во время установки Kaspersky Internet Security в программу Microsoft Office Outlook встраивается специальный плагин. Он позволяет быстро перейти к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook, а также определить, в какой момент (при получении, открытии или отправке) нужно проверять почтовые сообщения на присутствие вирусов и других программ, представляющих угрозу.

Настройка параметров Почтового Антивируса из программы Microsoft Office Outlook доступна в том случае, если это указано в параметрах области защиты Почтового Антивируса.

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

ПРОВЕРКА ПОЧТЫ В THE BAT!

Действия над зараженными объектами почтовых сообщений в почтовой программе The Bat! определяются средствами самой программы.

Параметры Почтового Антивируса, определяющие необходимость проверки входящей и исходящей почты, а также действия над опасными объектами писем и исключения, игнорируются. Единственное, что принимается во внимание программой The Bat!, – это проверка вложенных архивов.

Параметры защиты почты распространяются на все установленные на компьютере антивирусные компоненты, поддерживающие работу с The Bat!.

Следует помнить, что при получении почтовых сообщений они сначала проверяются Почтовым Антивирусом и только потом – плагином почтового клиента The Bat!. При обнаружении вредоносного объекта Kaspersky Internet Security обязательно уведомит вас об этом. Если при этом в окне уведомления Почтового Антивируса выбрать действие **Лечить (Удалить)**, то действия по устранению угрозы будут выполнены именно Почтовым Антивирусом. Если в окне уведомления выбрать действие **Пропустить**, то обезвреживать объект будет плагин The Bat!. При отправлении почтовых сообщений сначала осуществляется проверка плагином, а затем Почтовым Антивирусом.

Настройка параметров Почтового Антивируса из программы The Bat! доступна в том случае, если это указано в параметрах области защиты Почтового Антивируса.

Для настройки проверки почты в The Bat! вам нужно определить следующие критерии:

- какой поток почтовых сообщений (входящий, исходящий) следует подвергать проверке;
- в какой момент нужно производить проверку объектов письма (при открытии письма, перед сохранением на диске);
- какие действия будет предпринимать почтовый клиент при обнаружении опасных объектов в почтовых сообщениях. Например, вы можете выбрать:
  - **Попробовать излечить зараженные части** – при выборе этого варианта будет произведена попытка лечения зараженного объекта; если его вылечить невозможно, объект остается в письме.
  - **Удалить зараженные части** – при выборе этого варианта опасный объект письма будет удален независимо от того, является он зараженным или подозревается на заражение.

По умолчанию все зараженные объекты почтовых сообщений помещаются программой The Bat! на карантин без лечения.

Почтовые сообщения, содержащие опасные объекты, не отмечаются специальным заголовком при проверке плагином в почтовом клиенте The Bat!.

Чтобы перейти к настройке параметров проверки почты в программе The Bat!, выполните следующие действия:

1. Откройте главное окно программы The Bat!.
2. В меню **Свойства** выберите пункт **Настройка**.
3. В дереве настройки выберите объект **Защита от вирусов**.

Веб-Антивирус

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на вашем компьютере, риску заражения вирусами и другими программами, представляющими угрозу. Они могут проникать на ваш компьютер, когда вы загружаете бесплатные программы или просматриваете информацию на веб-сайтах, которые до вашего посещения подверглись атаке хакеров. Более того, сетевые черви могут проникать на ваш компьютер до открытия веб-страницы или загрузки файла, непосредственно в момент установки соединения с интернетом.

Веб-Антивирус защищает информацию, поступающую на ваш компьютер и отправляемую с него по протоколам HTTP, HTTPS и FTP, а также предотвращает запуск на компьютере опасных скриптов.

Веб-Антивирус контролирует веб-трафик, проходящий только через порты, указанные в списке контролируемых портов. Список контролируемых портов, которые чаще всего используются для передачи данных, включен в комплект поставки Kaspersky Internet Security. Если вы используете порты, отсутствующие в списке контролируемых портов, нужно добавить их в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 128), чтобы обеспечить защиту проходящего через них веб-трафика.

Веб-Антивирус проверяет веб-трафик в соответствии с определенным набором параметров, который называется уровнем безопасности. При обнаружении угроз Веб-Антивирус выполняет заданное действие. Распознавание вредоносных объектов происходит на основании баз, используемых в работе Kaspersky Internet Security, а также с помощью эвристического алгоритма.

Специалисты «Лаборатории Касперского» не рекомендуют вам самостоятельно настраивать параметры работы Веб-Антивируса. В большинстве случаев достаточно выбрать подходящий уровень безопасности.

Алгоритм проверки веб-трафика

Каждая веб-страница или файл, к которому обращаетесь вы или некоторая программа по протоколам HTTP, HTTPS или FTP, перехватывается и анализируется Веб-Антивирусом на присутствие вредоносного кода:

- Если веб-страница или файл, к которым обращается пользователь, содержат вредоносный код, доступ к ним блокируется. При этом на экран выводится уведомление о том, что запрашиваемый файл или веб-страница заражены.
- Если файл или веб-страница не содержат вредоносного кода, они сразу же становятся доступными для пользователя.

Алгоритм проверки скриптов

Каждый запускаемый скрипт перехватывается Веб-Антивирусом и анализируется на присутствие вредоносного кода:

- Если скрипт содержит вредоносный код, Веб-Антивирус блокирует скрипт и выводит на экран уведомление.
- Если в скрипте не обнаружено вредоносного кода, скрипт выполняется.

Веб-Антивирус перехватывает только скрипты, основанные на технологии Microsoft Windows Script Host.

В ЭТОМ РАЗДЕЛЕ

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.

Чтобы выключить использование Веб-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна снимите флажок **Включить Веб-Антивирус**.

ИЗМЕНЕНИЕ И ВОССТАНОВЛЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ВЕБ-ТРАФИКА

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности веб-трафика или настроить параметры работы Веб-Антивируса самостоятельно.

Настраивая параметры работы Веб-Антивируса, всегда можно вернуться к рекомендуемым значениям. Эти параметры считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

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

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

- *Чтобы восстановить уровень безопасности веб-трафика по умолчанию, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Изменение действия над опасными объектами веб-трафика

При обнаружении зараженных объектов программа выполняет заданное действие.

Что касается действий над опасными скриптами, то Веб-Антивирус всегда блокирует их исполнение и выводит на экран сообщение, уведомляющее пользователя о выполненном действии. Изменить действие над опасным скриптом нельзя, можно только отключить проверку скриптов (см. раздел «Блокирование опасных скриптов» на стр. 101).

- *Чтобы изменить действие над обнаруженными объектами, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна в блоке **Действие при обнаружении угрозы** выберите нужный вариант.

Проверка ссылок на веб-страницах

Проверка веб-страниц на наличие фишинга позволяет избежать *фишинг-атак*. Фишинг-атаки, как правило, представляют собой почтовые сообщения от якобы финансовых организаций и содержат ссылки на веб-сайты таких организаций. Почтовое сообщение предлагает воспользоваться ссылкой и ввести на открывшемся веб-сайте конфиденциальную информацию, например номер кредитной карты или имя и пароль учетной записи интернет-банка. Частным примером фишинг-атаки может служить письмо якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в почтовом сообщении, но и, например, в тексте ICQ-сообщения, Веб-Антивирус отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам.

Кроме баз Kaspersky Internet Security, для проверки веб-страниц на наличие фишинга можно использовать эвристический анализ (см. стр. 100).

В этом разделе

ВКЛЮЧЕНИЕ И ВЫКЛЮЧЕНИЕ ПРОВЕРКИ ССЫЛОК

Чтобы включить проверку ссылок по базам подозрительных веб-адресов и на наличие фишинга, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Общие** в блоке **Проверка ссылок** установите флажки **Проверять ссылки по базе подозрительных веб-адресов** и **Проверять веб-страницы на наличие фишинга**.

ИСПОЛЬЗОВАНИЕ МОДУЛЯ ПРОВЕРКИ ССЫЛОК

Модуль проверки ссылок встраивается в веб-браузеры Microsoft Internet Explorer, Mozilla Firefox и Google Chrome в виде плагина.

Модуль проверяет все ссылки на открытой веб-странице на принадлежность к подозрительным веб-адресам, а также на наличие фишинга и выделяет их цветом в окне браузера.

Можно сформировать список веб-сайтов, ссылки на которых будут проверяться, проверять ссылки на всех веб-сайтах, кроме перечисленных в списке исключений, проверять только ссылки в результатах поиска, а также указать категории веб-сайтов, ссылки на которые нужно проверять.

Настроить модуль проверки ссылок можно не только в окне настройки программы, но и в окне настройки модуля, доступном из веб-браузера.

Чтобы указать веб-сайты, на которых нужно проверять ссылки, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. Откроется окно **Веб-Антивирус**.
5. На закладке **Веб-фильтр** в блоке **Модуль проверки ссылок** установите флажок **Включить проверку ссылок**.
6. Выберите веб-сайты, на которых нужно проверять ссылки:

   a. Если вы хотите сформировать список веб-сайтов, на которых нужно проверять ссылки, выберите вариант **Только веб-сайты из списка** и нажмите на кнопку **Указать**. В открывшемся окне **Проверяемые веб-адреса** формируйте список проверяемых веб-сайтов.

   b. Если вы хотите проверять ссылки на всех веб-сайтах, кроме указанных, выберите вариант **Все, кроме исключений** и нажмите на кнопку **Исключения**. В открывшемся окне **Исключения** сформируйте список веб-сайтов, ссылки на которых не нужно проверять.

Чтобы проверять ссылки только в результатах поиска, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

4. Откроется окно **Веб-Антивирус**.

5. На закладке **Веб-фильтр** в блоке **Модуль проверки ссылок** установите флажок **Включить проверку ссылок** и нажмите на кнопку **Настройка**.

6. В открывшемся окне **Настройка модуля проверки ссылок** в блоке **Режим проверки** выберите вариант **Только ссылки в результатах поиска**.

Чтобы выбрать категории веб-сайтов, ссылки на которые нужно проверять, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.

3. В правой части окна нажмите на кнопку **Настройка**.

4. Откроется окно **Веб-Антивирус**.

5. На закладке **Веб-фильтр** в блоке **Модуль проверки ссылок** установите флажок **Включить проверку ссылок** и нажмите на кнопку **Настройка**.

6. В открывшемся окне **Настройка модуля проверки ссылок** в блоке **Категории веб-сайтов** установите флажок **Отображать информацию о категориях содержимого веб-сайтов**.

7. В списке категорий установите флажки рядом с теми категориями веб-сайтов, ссылки на которые нужно проверять.

Чтобы открыть окно настройки модуля проверки ссылок из окна веб-браузера,

нажмите на кнопку со значком Kaspersky Internet Security в панели инструментов браузера.

Блокирование доступа к опасным веб-сайтам

Вы можете заблокировать доступ к веб-сайтам, которые были определены как подозрительные или фишинговые в результате работы модуля проверки ссылок (см. раздел «Использование модуля проверки ссылок» на стр. 99).

Чтобы блокировать доступ к опасным веб-сайтам, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.

3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

4. На закладке **Веб-фильтр** в блоке **Блокирование опасных веб-сайтов** установите флажок **Блокировать опасные веб-сайты**.

Использование эвристического анализа при работе Веб-Антивируса

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

При работе Веб-Антивируса можно независимо друг от друга включить эвристический анализ для проверки веб-трафика и для проверки веб-страниц на наличие фишинга.

Чтобы включить эвристический анализ для проверки веб-трафика, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Общие** в блоке **Эвристический анализ** установите флажок **Использовать эвристический анализ** и задайте уровень детализации проверки.

Чтобы включить эвристический анализ для проверки веб-страниц на наличие фишинга, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Общие** в блоке **Проверка ссылок** нажмите на кнопку **Дополнительно**.
5. В открывшемся окне **Настройка Анти-Фишинга** установите флажок **Использовать эвристический анализ для проверки веб-страниц на наличие фишинга** и задайте уровень детализации проверки.

Блокирование опасных скриптов

Веб-Антивирус проверяет все скрипты, обрабатываемые в Microsoft Internet Explorer, а также любые WSH-скрипты (например, JavaScript, Visual Basic Script), запускаемые при работе на компьютере. Если скрипт представляет опасность для компьютера, его выполнение будет заблокировано.

Чтобы выключить блокирование опасных скриптов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Общие** в блоке **Дополнительно** снимите флажок **Блокировать опасные скрипты в Microsoft Internet Explorer**.

Оптимизация проверки

Чтобы повысить эффективность 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 компьютер.

Кеширование увеличивает продолжительность обработки объектов и передачи их для работы. Кроме того, кеширование может вызывать проблемы при загрузке и обработке больших объектов, связанные с истечением тайм-аута 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 непроверенной, а по завершении копирования объект проверяется целиком. Это позволяет уменьшить продолжительность передачи объектов и решить проблему разрыва соединения. Уровень безопасности работы в интернете при этом не снижается.

Снятие ограничения на продолжительность кеширования веб-трафика приводит к повышению эффективности антивирусной проверки, но одновременно предполагает замедление доступа к объектам.

- *Чтобы ограничить время кеширования фрагментов или снять это ограничение, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Общие** в блоке **Дополнительно** установите флажок **Ограничивать время кеширования трафика 1 сек для оптимизации проверки**.

Контроль обращения к региональным доменам

При включенном Гео-фильтре Веб-Антивирус в зависимости от вашего выбора может запрещать или разрешать доступ к веб-сайтам на основе их принадлежности к региональным доменам интернета. Это позволяет, например, запретить доступ к веб-сайтам, принадлежащим к региональным доменам с высокой степенью зараженности.

- *Чтобы разрешить или запретить доступ к веб-сайтам, принадлежащим к определенным доменам, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Гео-фильтр** установите флажок **Включить фильтрацию по региональным доменам** и ниже в списке контролируемых доменов укажите, к каким доменам следует разрешать или запрещать доступ и для каких доменов программа должна запрашивать разрешение на доступ с помощью уведомления (см. раздел «Запрос разрешения на доступ к веб-сайту из регионального домена» на стр. 211).

   Для региональных доменов, соответствующих вашему местонахождению, доступ по умолчанию разрешен. Для остальных доменов по умолчанию предусмотрен запрос разрешения на доступ.

Контроль обращения к сервисам интернет-банкинга

В процессе работы с интернет-банкингом вашему компьютеру требуется особая защита, поскольку в этом случае утечка конфиденциальной информации может привести к финансовым потерям. Веб-Антивирус может контролировать обращение к сервисам интернет-банкинга и обеспечивать безопасную работу с ними (см. раздел «О безопасном браузере» на стр. 152). Веб-Антивирус автоматически определяет, какие из интернет-ресурсов являются сервисами интернет-банкинга. Для гарантированной идентификации интернет-ресурса как сервиса интернет-банкинга вы можете указать его адрес в списке банковских веб-сайтов.

Чтобы настроить контроль обращения к сервисам интернет-банкинга, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Интернет-банкинг** установите флажок **Включить контроль**. При первой установке вам будет предложено запустить Мастер установки сертификатов, с помощью которого вы сможете установить сертификат «Лаборатории Касперского» для проверки защищенных соединений.
5. При необходимости сформируйте список ресурсов, которые Kaspersky Internet Security будет идентифицировать как сервисы интернет-банкинга.

ФОРМИРОВАНИЕ СПИСКА ДОВЕРЕННЫХ АДРЕСОВ

Веб-Антивирус не проверяет веб-трафик, полученный с доверенных адресов, на присутствие опасных объектов.

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

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. На закладке **Доверенные адреса** установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.
5. Сформируйте список веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для этого выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Маска адреса**.

   b. Введите адрес веб-сайта / веб-страницы или маску адреса веб-сайта / веб-страницы.

   c. Нажмите на кнопку **ОК**.

      В списке доверенных веб-адресов появится новая запись.
6. При необходимости повторите пункты a – c инструкции.

IM-АНТИВИРУС

IM-Антивирус предназначен для проверки трафика, передаваемого программами для быстрого обмена сообщениями (так называемых *интернет-пейджеров*).

Сообщения, переданные через интернет-пейджеры, могут содержать ссылки на подозрительные веб-сайты, а также на веб-сайты, которые используются злоумышленниками для фишинг-атак. Вредоносные программы используют интернет-пейджеры для рассылки спам-сообщений, а также ссылок на программы (или самих программ), которые крадут номера и пароли пользователей.

Kaspersky Internet Security обеспечивает безопасную работу со многими программами для быстрого обмена сообщениями, в том числе ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Агент и IRC.

Некоторые интернет-пейджеры, например Yahoo! Messenger и Google Talk, используют защищенное соединение. Чтобы проверять трафик этих программ, требуется включить проверку защищенных соединений (см. стр. 125).

IM-Антивирус перехватывает сообщения и проверяет на наличие опасных объектов или ссылок. Вы можете выбрать типы сообщений, которые нужно проверять, и задействовать различные методы проверки.

Обнаружив угрозы в сообщении, IM-Антивирус заменяет это сообщение предупреждением для пользователя.

Передаваемые через интернет-пейджеры файлы проверяются компонентом Файловый Антивирус (на стр. 83) во время попытки их сохранения.

В этом разделе

Включение и выключение IM-Антивируса

По умолчанию IM-Антивирус включен и работает в оптимальном режиме. Вы можете выключить IM-Антивирус при необходимости.

Чтобы выключить использование IM-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
3. В правой части окна снимите флажок **Включить IM-Антивирус**.

Формирование области защиты IM-Антивируса

Под областью защиты подразумевается тип сообщений, которые следует проверять. По умолчанию Kaspersky Internet Security проверяет как входящие, так и исходящие сообщения. Если вы уверены в том, что отправляемые вами сообщения не могут содержать опасных объектов, вы можете отказаться от проверки исходящего трафика.

Чтобы отключить проверку исходящих сообщений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
3. В правой части окна в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

ПРОВЕРКА ССЫЛОК В СООБЩЕНИЯХ ИНТЕРНЕТ-ПЕЙДЖЕРОВ

- *Чтобы проверять сообщения на наличие подозрительных и фишинговых ссылок, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
3. В правой части окна в блоке **Методы проверки** установите флажки **Проверять ссылки по базе подозрительных веб-адресов** и **Проверять ссылки по базе фишинговых веб-адресов**.

ИСПОЛЬЗОВАНИЕ ЭВРИСТИЧЕСКОГО АНАЛИЗА ПРИ РАБОТЕ IM-АНТИВИРУСА

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

При эвристическом анализе любой скрипт, содержащийся в сообщении интернет-пейджера, выполняется в защищенной среде. Если активность скрипта типична для вредоносных объектов, объект с достаточной долей вероятности будет признан вредоносным или подозрительным. По умолчанию эвристический анализ включен.

- *Чтобы включить использование эвристического анализа, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
3. В правой части окна в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки.

ПРОАКТИВНАЯ ЗАЩИТА

Проактивная защита обеспечивает защиту компьютера от новых угроз, информация о которых отсутствует в базах Kaspersky Internet Security.

Работа Проактивной защиты построена на использовании превентивных технологий. Превентивные технологии позволяют обезвредить новую угрозу еще до того, как она нанесет вред вашему компьютеру. В отличие от реактивных технологий, выполняющих анализ на основании записей баз Kaspersky Internet Security, превентивные технологии распознают новую угрозу на вашем компьютере по последовательности действий, производимых программой. Если в результате анализа активности последовательность действий программы вызывает подозрение, Kaspersky Internet Security блокирует активность этой программы.

Например, обнаружив такие действия, как самокопирование программы на сетевые ресурсы, в каталог автозапуска и системный реестр, с большой вероятностью можно предположить, что эта программа является червем.

К опасным последовательностям действий относятся также попытки изменения файла HOSTS, скрытая установка драйверов и другие. Вы можете отказаться от контроля (см. стр. 107) той или иной опасной активности или изменить правила контроля (см. стр. 107) для нее.

В отличие от компонента защиты Контроль программ (на стр. 109), Проактивная защита реагирует именно на определенную последовательность действий программы. Анализ активности производится для всех работающих на компьютере программ, в том числе и для программ, выделенных в группу **Доверенные** компонентом защиты Контроль программ.

Вы можете сформировать группу доверенных программ (см. стр. 106) для Проактивной защиты. Уведомления об активности таких программ отображаться не будут.

Если компьютер работает под управлением операционных систем Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 или Microsoft Windows 7 x64, то будут контролироваться не все события. Это связано с особенностями перечисленных операционных систем. Так, например, не в полном объеме будут контролироваться отправка данных посредством доверенных программ и подозрительная активность в системе.

В этом разделе

Включение и выключение Проактивной защиты

По умолчанию Проактивная защита включена и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Проактивную защиту при необходимости.

Чтобы выключить использование Проактивной защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
3. В правой части окна снимите флажок **Включить Проактивную защиту**.

Формирование группы доверенных программ

Программы, которым компонент защиты Контроль программ присвоил статус **Доверенные**, не представляют опасности для системы. Однако их активность также контролируется Проактивной защитой.

Вы можете сформировать группу доверенных программ, активность которых Проактивная защита не будет проверять. По умолчанию к числу доверенных относятся программы, имеющие проверенную цифровую подпись, и программы, являющиеся доверенными в базе Kaspersky Security Network.

Чтобы настроить параметры формирования группы доверенных программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
3. В правой части окна в блоке **Доверенные программы** выполните следующие действия:
   - Если вы хотите, чтобы в группу доверенных программ были включены программы, имеющие проверенную цифровую подпись, установите флажок **Имеющие цифровую подпись**.
   - Если вы хотите, чтобы в группу доверенных программ были включены программы, являющиеся доверенными в базе Kaspersky Security Network, установите флажок **Доверенные в базе Kaspersky Security Network**.

ИСПОЛЬЗОВАНИЕ СПИСКА ОПАСНОЙ АКТИВНОСТИ

Список действий, относящихся к опасной активности, изменить нельзя. Но можно отказаться от контроля той или иной опасной активности.

Чтобы отказаться от контроля той или иной опасной активности, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне **Проактивная защита** снимите флажок, установленный рядом с названием того вида активности, от контроля которого вы хотите отказаться.

ИЗМЕНЕНИЕ ДЕЙСТВИЯ ПО ОТНОШЕНИЮ К ОПАСНОЙ АКТИВНОСТИ ПРОГРАММ

Список действий, относящихся к опасной активности, изменить нельзя. Но можно изменить действие, которое выполняет Kaspersky Internet Security при обнаружении опасной активности программ.

Чтобы изменить действие по отношению к опасной активности программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне **Проактивная защита** в графе **Событие** выберите нужное событие, для которого необходимо изменить правило.
5. Для выбранного события, используя ссылки в блоке **Описание правила**, задайте необходимые параметры. Например:
   a. Перейдите по ссылке с установленным действием и в открывшемся окне **Выбор действия** выберите нужное действие из предложенных.
   b. Перейдите по ссылке **Вкл. / Выкл.**, чтобы указать необходимость формирования отчета о выполненной операции.

МОНИТОРИНГ АКТИВНОСТИ

Мониторинг активности собирает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты.

На основе информации, собранной Мониторингом активности, Kaspersky Internet Security может выполнять откат действий, произведенных вредоносными программами.

Откат действий вредоносной программы может быть инициирован одним из следующих компонентов защиты:

- Мониторингом активности на основе шаблонов опасного поведения;
- Проактивной защитой;

- Файловым Антивирусом;
- при проверке на вирусы.

При обнаружении подозрительных событий в системе компоненты защиты Kaspersky Internet Security могут запрашивать дополнительную информацию у Мониторинга активности. В интерактивном режиме защиты Kaspersky Internet Security (см. раздел «Выбор режима защиты» на стр. 70) вы можете просмотреть данные, собранные компонентом Мониторинг активности, в форме отчета об истории опасной активности. Эти данные помогают принять решение при выборе действия в окне уведомления. При обнаружении компонентом вредоносной программы ссылка на отчет Мониторинга активности отображается в верхней части окна уведомления (см. стр. 212) с запросом действия.

В этом разделе

Включение и выключение Мониторинга активности

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

Не рекомендуется отключать работу компонента без необходимости, так как это снизит эффективность работы Проактивной защиты и других компонентов защиты, которые могут запрашивать данные, собранные Мониторингом активности, для уточнения обнаруженной потенциальной угрозы.

Чтобы выключить использование Мониторинга активности, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Мониторинг активности**.
3. В правой части окна снимите флажок **Включить Мониторинг активности**.

Использование шаблонов опасного поведения (BSS)

Шаблоны опасного поведения программ (BSS – Behavior Stream Signatures) содержат последовательности действий программ, классифицируемые как опасные. При совпадении активности программы с одним из шаблонов опасного поведения Kaspersky Internet Security выполняет заданное действие.

Для актуальной и эффективной защиты Kaspersky Internet Security дополняет шаблоны опасного поведения, которые использует Мониторинг активности, во время обновления баз.

По умолчанию при работе Kaspersky Internet Security в автоматическом режиме, если активность программы совпадает с шаблоном опасного поведения, Мониторинг активности помещает эту программу на карантин, а в интерактивном режиме работы – запрашивает действие. Вы можете указать действие, которое нужно выполнять при совпадении активности программы с шаблоном опасного поведения.

Кроме точного совпадения активности программы с шаблонами опасного поведения, Мониторинг активности обнаруживает действия, частично совпадающие с шаблонами опасного поведения и являющиеся подозрительными на основании эвристического анализа. При обнаружении подозрительной активности Мониторинг активности запрашивает действие независимо от режима работы.

- *Чтобы выбрать действие при совпадении активности программы с шаблоном опасного поведения, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Мониторинг активности**.
  3. В правой части окна в блоке **Эвристический анализ** установите флажок **Использовать обновляемые шаблоны опасного поведения**.
  4. Выберите вариант **Выполнять действие**, а затем выберите нужное действие из раскрывающегося списка.

ОТКАТ ДЕЙСТВИЙ ВРЕДОНОСНОЙ ПРОГРАММЫ

Вы можете использовать возможность отката действий, произведенных вредоносной программой в системе. Для выполнения отката Мониторинг активности сохраняет историю активности программ. Можно ограничить объем информации, которую Мониторинг активности хранит для отката.

По умолчанию при работе Kaspersky Internet Security в автоматическом режиме откат действий выполняется автоматически при обнаружении компонентами защиты вредоносной активности. В интерактивном режиме работы Мониторинг активности запрашивает действие. Вы можете указать действие, которое нужно выполнять при обнаружении возможности отката действий вредоносной программы.

Процедура отката действий вредоносной программы затрагивает строго ограниченный набор данных. Она не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

- *Чтобы выбрать действие при обнаружении возможности отката действий вредоносной программы, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Мониторинг активности**.
  3. В правой части окна в блоке **Откат действий вредоносной программы** выберите вариант **Выполнять действие**, а затем выберите нужное действие из раскрывающегося списка.

- *Чтобы ограничить объем информации, которую Мониторинг активности сохраняет для отката, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Мониторинг активности**.
  3. В правой части окна в блоке **Откат действий вредоносной программы** установите флажок **Ограничить объем информации, хранимой для отката** и укажите максимальный объем информации, который Мониторинг активности будет сохранять для отката.

КОНТРОЛЬ ПРОГРАММ

Контроль программ предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и вашим персональным данным.

Компонент отслеживает действия, которые совершают в системе программы, установленные на компьютере, и регулирует их на основании правил Контроля программ. Эти правила регламентируют потенциально опасную активность, в том числе доступ программ к защищаемым ресурсам (например, файлам, папкам, ключам реестра, сетевым адресам).

Сетевая активность программ контролируется компонентом Сетевой экран (на стр. 118).

При первом запуске программы на компьютере компонент Контроль программ проверяет ее безопасность и помещает в одну из групп. Группа определяет правила, которые Kaspersky Internet Security будет применять для контроля активности этой программы. Правила Контроля программ представляют собой набор прав доступа к ресурсам компьютера и ограничений для различных действий программ на компьютере.

Вы можете настроить условия распределения программ по группам (см. стр. 110), переместить программу в другую группу (см. стр. 112), а также изменить правила Kaspersky Internet Security (см. стр. 112).

Для более эффективной работы Контроля программ рекомендуем вам принять участие в Kaspersky Security Network (см. раздел «Kaspersky Security Network» на стр. 187). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля программ.

При повторном запуске программы Контроль программ проверяет ее целостность. Если программа не была изменена, компонент применяет к ней текущие правила. Если программа была изменена, Контроль программ заново исследует ее, как при первом запуске.

Для контроля доступа программ к различным ресурсам компьютера вы можете использовать предустановленный список защищаемых ресурсов или дополнить список пользовательскими ресурсами (см. стр. 116).

В этом разделе

Включение и выключение Контроля программ

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

Чтобы выключить использование Контроля программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна снимите флажок **Включить Контроль программ**.

Распределение программ по группам

При первом запуске программы на компьютере компонент Контроль программ проверяет ее безопасность и помещает в одну из групп.

Программы, не представляющие опасности для системы, помещаются в группу **Доверенные**. По умолчанию в эту группу помещаются программы, имеющие цифровую подпись, а также те программы, у родительского

объекта которых присутствует цифровая подпись. Вы можете отключить автоматическое помещение программ с цифровой подписью в группу **Доверенные**.

Поведение программ, которые Контроль программ помещает в группу **Доверенные**, будет тем не менее контролироваться компонентом Проактивная защита (на стр. 105).

Для распределения по группам неизвестных программ (отсутствующих в базе Kaspersky Security Network и не имеющих цифровой подписи) по умолчанию Kaspersky Internet Security использует эвристический анализ. В процессе этого анализа определяется рейтинг опасности программы, на основании которого программа помещается в ту или иную группу. Вместо эвристического анализа вы можете указать группу, в которую Kaspersky Internet Security будет автоматически помещать все неизвестные программы.

По умолчанию Контроль программ исследует программу в течение 30 секунд. Если по истечении этого времени определение рейтинга опасности не завершено, программа помещается в группу **Слабые ограничения**, а определение рейтинга опасности продолжается в фоновом режиме. Затем программа помещается в окончательную группу. Вы можете изменить время, которое отводится для проверки запускаемых программ. Если вы уверены, что все запускаемые на вашем компьютере программы не представляют угрозы для его безопасности, то время, отведенное для проверки, можно уменьшить. Если же вы устанавливаете на компьютер программное обеспечение, в безопасности которого не уверены, время проверки рекомендуется увеличить.

Если рейтинг опасности программы высок, то Kaspersky Internet Security уведомит вас об этом и предложит выбрать группу, в которую следует поместить эту программу. Уведомление (см. стр. 210) содержит статистику использования этой программы участниками Kaspersky Security Network. На основании этой статистики, а также зная историю появления программы на вашем компьютере, вы можете принять более объективное решение о том, в какую группу следует поместить эту программу (см. раздел «Интерпретация данных об использовании программы участниками KSN» на стр. 117).

Чтобы настроить распределение программ по группам, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Установка ограничений** выполните следующие действия:
   a. Если вы хотите автоматически помещать программы с цифровой подписью в группу **Доверенные**, установите флажок **Доверять программам, имеющим цифровую подпись**.
   b. Выберите способ распределения по группам для неизвестных программ:
      - Если вы хотите использовать эвристический анализ для распределения по группам неизвестных программ, выберите вариант **Использовать эвристический анализ для определения группы**.
      - Если вы хотите помещать все неизвестные программы в указанную группу, выберите вариант **Автоматически помещать в группу** и выберите нужную группу из раскрывающегося списка.
   c. Укажите время, которое отводится для проверки запускаемой программы, в поле **Максимальное время определения группы программы**.

ПРОСМОТР АКТИВНОСТИ ПРОГРАММ

Вы можете просмотреть информацию о программах, используемых на вашем компьютере, и о выполняемых процессах.

Чтобы просмотреть активность программ, выполните следующие действия:

1. Откройте главное окно программы (см. стр. 37).
2. В нижней части окна выберите раздел **Активность программ**.

3. В открывшемся окне **Активность программ** в левом верхнем углу выберите нужную категорию программ из раскрывающегося списка.

Изменение группы и восстановление группы по умолчанию

При первом запуске программы Kaspersky Internet Security автоматически помещает ее в ту или иную группу (см. раздел «Распределение программ по группам» на стр. 110). Вы можете вручную переместить программу в другую группу. В любой момент вы можете вернуть программу в группу, заданную по умолчанию.

Специалисты «Лаборатории Касперского» не рекомендуют перемещать программы из группы, назначенной автоматически, в другую. Вместо этого при необходимости измените правила для отдельной программы.

Чтобы переместить программу в другую группу, выполните следующие действия:

1. Откройте главное окно программы (см. стр. 37).
2. В нижней части окна выберите раздел **Активность программ**.
3. В открывшемся окне **Активность программ** в левом верхнем углу выберите нужную категорию программ из раскрывающегося списка.
4. По правой клавише мыши откройте контекстное меню для нужной программы и выберите в нем пункт **Переместить в группу → <название группы>**.

Чтобы вернуть программу в группу, заданную по умолчанию, выполните следующие действия:

1. Откройте главное окно программы (см. стр. 37).
2. В нижней части окна выберите раздел **Активность программ**.
3. В открывшемся окне **Активность программ** в левом верхнем углу выберите нужную категорию программ из раскрывающегося списка.
4. По правой клавише мыши откройте контекстное меню для нужной программы и выберите пункт **Переместить в группу → Восстановить группу по умолчанию**.

Работа с правилами Контроля программ

Правила Контроля программ представляют собой набор прав доступа к ресурсам компьютера и ограничений для различных действий программ на компьютере.

По умолчанию для контроля программы применяются правила группы, в которую Kaspersky Internet Security поместил программу при первом ее запуске. Правила групп разработаны специалистами «Лаборатории Касперского» для оптимального контроля активности программ. При необходимости вы можете изменить эти правила, а также настроить их на уровне отдельной программы. Правила программы имеют более высокий приоритет, чем правила группы.

В этом разделе

ИЗМЕНЕНИЕ ПРАВИЛ ГРУППЫ

По умолчанию для разных групп заданы оптимальные наборы прав доступа к ресурсам компьютера. Вы можете изменить предустановленные правила группы.

Чтобы изменить правила группы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Настройка прав программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
4. В открывшемся окне **Программы** выберите нужную группу из списка и нажмите на кнопку **Изменить**.
5. В открывшемся окне **Правила группы** выберите закладку, соответствующую нужной категории ресурсов (**Файлы и системный реестр** или **Права**).
6. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить** или **Запросить действие**).

ИЗМЕНЕНИЕ ПРАВИЛ ПРОГРАММЫ

Вы можете изменить ограничения на уровне отдельной программы или исключить некоторые действия из правил программы. Kaspersky Internet Security не будет контролировать действия, добавленные в исключения правил программы.

Все исключения, созданные в правилах программ, доступны в окне настройки программы (см. раздел «Окно настройки параметров программы» на стр. 40) в разделе **Угрозы и исключения**.

Вы также можете выключить применение правил группы для контроля доступа к выбранным категориям защищаемых ресурсов. Доступ программы к этим ресурсам будет регулироваться правилами программы.

Чтобы изменить правило для программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Настройка прав программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
4. В открывшемся окне **Программы** выберите нужную программу в списке и нажмите на кнопку **Изменить**.
5. В открывшемся окне **Правила программы** выберите закладку, соответствующую нужной категории ресурсов (**Файлы и системный реестр** или **Права**).
6. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить** или **Запросить действие**).

Чтобы выключить применение правил группы для доступа к ресурсам, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Настройка прав программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
4. В открывшемся окне **Программы** выберите нужную программу в списке.
5. Нажмите на кнопку **Изменить**.
6. В открывшемся окне **Правила программы** выберите закладку, соответствующую нужной категории ресурсов (**Файлы и системный реестр** или **Права**).
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Наследовать** с установленным флажком.

Чтобы добавить исключение в правила программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Настройка прав программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
4. В открывшемся окне **Программы** выберите нужную программу в списке и нажмите на кнопку **Изменить**.
5. В открывшемся окне **Правила программы** выберите закладку **Исключения**.
6. Установите флажки для действий, которые не нужно контролировать.

Использование правил из Kaspersky Security Network Контролем программ

По умолчанию для программ, найденных в базе Kaspersky Security Network, применяются правила, загруженные из этой базы.

Если на момент первого запуска программа отсутствовала в базе Kaspersky Security Network, но затем информация о ней была добавлена, то по умолчанию Kaspersky Internet Security автоматически обновит правила контроля этой программы.

Вы можете выключить использование правил из Kaspersky Security Network и (или) автоматическое обновление правил для ранее неизвестных программ.

Чтобы выключить использование правил из Kaspersky Security Network, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Установка ограничений** снимите флажок **Загружать правила для программ из Kaspersky Security Network (KSN)**.

- *Чтобы выключить обновление правил Kaspersky Security Network для ранее неизвестных программ, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
  3. В правой части окна в блоке **Установка ограничений** снимите флажок **Обновлять правила для ранее неизвестных программ из KSN**.

НАСЛЕДОВАНИЕ ОГРАНИЧЕНИЙ РОДИТЕЛЬСКОГО ПРОЦЕССА

На вашем компьютере программы или процессы могут запускаться не только вами, но и другими уже запущенными программами (процессами), которые в этом случае называют *родительскими*. Если родительский процесс имеет меньшие права, чем запускаемая им программа, то к запускаемой программе Контроль программ применяет те же ограничения, что и к родительскому процессу. Таким образом, запускаемая программа *наследует* ограничения родительского процесса.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если активность программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права или отключить наследование ограничений родительского процесса.

Вносить изменения в права родительского процесса и отключать наследование ограничений следует только в том случае, если вы абсолютно уверены, что активность процесса не угрожает безопасности системы!

- *Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
  3. В правой части окна в блоке **Настройка прав программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
  4. В открывшемся окне **Программы** выберите нужную программу в списке.
  5. Нажмите на кнопку **Изменить**.
  6. В открывшемся окне **Правила программы** выберите закладку **Исключения**.
  7. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.

УДАЛЕНИЕ ПРАВИЛ ДЛЯ НЕИСПОЛЬЗУЕМЫХ ПРОГРАММ

По умолчанию правила программ, которые не запускались в течение 60 дней, автоматически удаляются. Вы можете изменить время хранения правил для неиспользуемых программ или выключить автоматическое удаление.

- *Чтобы изменить время хранения правил программ, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
  3. В правой части окна в блоке **Дополнительно** установите флажок **Удалять правила для программ, не запускавшихся более** и укажите нужное количество дней.

Чтобы выключить автоматическое удаление правил для неиспользуемых программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна в блоке **Дополнительно** снимите флажок **Удалять правила для программ, не запускавшихся более**.

Защита ресурсов операционной системы и персональных данных

Контроль программ управляет правами программ на совершение действий над различными категориями ресурсов операционной системы и персональных данных.

Специалисты «Лаборатории Касперского» выделили предустановленные категории защищаемых ресурсов. Изменять этот список нельзя. Однако вы можете дополнить этот список пользовательскими категориями и (или) отдельными ресурсами, а также отказаться от контроля выбранных ресурсов.

Кроме того, вы можете добавлять определенные ресурсы в исключения. Доступ к таким ресурсам контролироваться не будет.

Чтобы добавить защищаемые персональные данные, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна нажмите на кнопку **Защита данных**.
4. В открывшемся окне на закладке **Персональные данные** выберите нужную категорию персональных данных в раскрывающемся списке.
5. Нажмите на кнопку **Добавить** и в открывшемся меню выберите нужный тип ресурса.
6. В открывшемся окне **Пользовательский ресурс** задайте необходимые параметры в зависимости от добавляемого ресурса.

Чтобы создать категорию защищаемых персональных данных, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна нажмите на кнопку **Защита данных**.
4. В открывшемся окне на закладке **Персональные данные** нажмите на кнопку **Добавить категорию**.
5. В открывшемся окне **Категория пользовательских ресурсов** введите название новой категории ресурсов.

Чтобы добавить защищаемые параметры и ресурсы операционной системы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
3. В правой части окна нажмите на кнопку **Защита данных**.

4. В открывшемся окне на закладке **Операционная система** в раскрывающемся списке **Категория** выберите нужную категорию объектов операционной системы.

5. Нажмите на кнопку **Добавить** и в открывшемся меню выберите нужный тип ресурса.

6. В открывшемся окне **Пользовательский ресурс** задайте необходимые параметры в зависимости от добавляемого ресурса.

Чтобы добавить ресурс в исключения, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.

3. В правой части окна нажмите на кнопку **Защита данных**.

4. В открывшемся окне на закладке **Исключения** нажмите на кнопку **Добавить** и в открывшемся меню выберите нужный тип ресурса.

5. В открывшемся окне **Пользовательский ресурс** задайте необходимые параметры в зависимости от добавляемого ресурса.

ИНТЕРПРЕТАЦИЯ ДАННЫХ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММЫ УЧАСТНИКАМИ KSN

Информация об использовании программы участниками Kaspersky Security Network (см. стр. 188) поможет принять объективное решение о том, какой статус следует присвоить программе, запускаемой на вашем компьютере. Чтобы точно оценить опасность или безопасность программы на основании данных из KSN, нужно знать историю появления этой программы на вашем компьютере.

Специалисты «Лаборатории Касперского» выделяют следующие возможные источники появления новой программы на компьютере:

- загрузка из интернета и последующий запуск установочного файла пользователем;
- автоматическая загрузка и запуск установочного файла при переходе пользователя по ссылке на веб-странице;
- запуск пользователем установочного файла, находящегося на CD- / DVD-диске или скопированного оттуда на жесткий диск;
- запуск пользователем установочного файла, находящегося на USB-накопителе или скопированного оттуда на жесткий диск;
- запуск пользователем установочного файла, полученного в сообщении электронной почты, интернет-пейджера или социальной сети.

Статистика использования программы участниками Kaspersky Security Network включает частоту и давность использования данной программы. Следующие варианты статистики использования программы являются основными:

- **очень редко** (менее 100 участников KSN используют эту программу) и **недавно** (файл появился несколько дней назад);
- **редко** (менее 1000 участников KSN) и относительно **давно** (несколько месяцев назад), большинство пользователей ограничивают активность этой программы;
- **часто** (более 100 000 участников KSN) и **давно** (более полугода назад), большинство пользователей доверяют этой программе;

- **часто** (более 100 000 участников KSN) и **недавно** (несколько недель назад), большинство пользователей доверяют или ограничивают эту программу;
- **очень часто** (более 100 000 участников KSN) и **недавно**, большинство пользователей доверяют этой программе.

Защита сети

Различные компоненты защиты, инструменты и параметры настройки Kaspersky Internet Security в комплексе обеспечивают безопасность и контроль вашей работы в сети.

Следующие разделы содержат подробную информацию о принципах работы и настройке Сетевого экрана, Защиты от сетевых атак, мониторинге сетевой активности, проверке защищенных соединений, параметрах прокси-сервера, контроле сетевых портов.

В этом разделе

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и интернете.

Компонент фильтрует всю сетевую активность в соответствии с сетевыми правилами контроля программ. Сетевое правило представляет собой действие, которое Сетевой экран совершает при обнаружении попытки соединения, имеющего определенный статус. Статус присваивается каждому сетевому соединению и определяется заданными параметрами: направлением и протоколом передачи данных, адресами и портами, с которыми происходит соединение.

Сетевой экран анализирует параметры сетей, к которым вы подключаете компьютер. Если программа работает в интерактивном режиме, при первом подключении Сетевой экран запрашивает у вас статус подключенной сети (см. стр. 210). Если интерактивный режим выключен, Сетевой экран определяет статус, ориентируясь на тип сети, диапазоны адресов и другие характеристики. При необходимости можно изменить статус (см. стр. 119) сетевого соединения вручную.

В этом разделе

ВКЛЮЧЕНИЕ И ВЫКЛЮЧЕНИЕ СЕТЕВОГО ЭКРАНА

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

Чтобы выключить использование Сетевого экрана, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна снимите флажок **Включить Сетевой экран**.

ИЗМЕНЕНИЕ СТАТУСА СЕТИ

От статуса сетевого соединения зависит набор правил, применяемых для фильтрации сетевой активности данного соединения. При необходимости вы можете изменить статус сети.

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна в списке **Сети** выберите сетевое соединение и нажмите на кнопку **Изменить**, чтобы открыть окно параметров сети.
4. В открывшемся окне на закладке **Свойства** выберите нужный статус из раскрывающегося списка.

РАБОТА С ПРАВИЛАМИ СЕТЕВОГО ЭКРАНА

Сетевой экран работает на основе правил двух видов:

- *Пакетные правила.* Используются для ввода ограничений на пакеты независимо от программы. Чаще всего такие правила ограничивают входящую сетевую активность по определенным портам протоколов TCP и UDP и подвергают фильтрации ICMP-сообщения.
- *Правила программ*. Используются для ввода ограничений сетевой активности конкретной программы. Такие правила позволяют тонко настраивать фильтрацию активности, например, когда определенный тип сетевых соединений запрещен для одних программ, но разрешен для других.

Пакетные правила имеют более высокий приоритет, чем правила программ. Если для одного вида сетевой активности заданы и пакетные правила, и правила программ, эта сетевая активность будет обрабатываться по пакетным правилам. Кроме того, вы можете установить для каждого правила приоритет выполнения (см. стр. 121).

СОЗДАНИЕ ПАКЕТНОГО ПРАВИЛА

Пакетные правила состоят из набора условий и действий над пакетами, которые выполняются при соблюдении заданных условий.

При создании пакетных правил помните, что они имеют приоритет перед правилами для программ.

Чтобы создать пакетное правило, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Пакетные правила** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Сетевое правило** задайте нужные параметры и нажмите на кнопку **ОК**.
6. Назначьте приоритет нового правила, переместив его вверх или вниз с помощью кнопок **Вверх** и **Вниз**.

Изменение правил группы

Аналогично компоненту Контроль программ (на стр. 109), по умолчанию Сетевой экран применяет для фильтрации сетевой активности программы правила группы, в которую эта программа помещена.

Сетевые правила группы определяют, какими правами доступа к различным сетям будут обладать программы, помещенные в эту группу. Вы можете добавить новые и изменить предустановленные сетевые правила группы.

- *Чтобы добавить сетевое правило группы, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Правила программ** выберите нужную группу в списке и нажмите на кнопку **Изменить**.
5. В открывшемся окне **Правила группы** выберите закладку **Сетевые правила** и нажмите на кнопку **Добавить**.
6. В открывшемся окне **Сетевое правило** задайте нужные параметры и нажмите на кнопку **ОК**.
7. Назначьте приоритет нового правила, переместив его вверх или вниз по списку с помощью кнопок **Вверх** и **Вниз**.

- *Чтобы изменить сетевое правило группы, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Правила программ** выберите нужную группу в списке и нажмите на кнопку **Изменить**.
5. В открывшемся окне **Правила группы** выберите закладку **Сетевые правила**.
6. Для нужного правила в графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите в нем нужное значение: **Разрешить**, **Запретить** или **Запросить действие**.

Изменение правил программы

Вы можете создавать сетевые правила для отдельных программ. Сетевые правила программы имеют более высокий приоритет, чем сетевые правила группы.

- *Чтобы создать сетевое правило программы, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Правила программ** выберите программу и нажмите на кнопку **Изменить**, чтобы открыть окно настройки правил.

5. В открывшемся окне **Правила программы** на закладке **Сетевые правила** откройте окно создания сетевого правила для программы, нажав на кнопку **Добавить**.

6. В открывшемся окне **Сетевое правило** задайте нужные параметры и нажмите на кнопку **ОК**.

7. Назначьте приоритет нового правила, переместив его вверх или вниз по списку с помощью кнопок **Вверх** и **Вниз**.

ИЗМЕНЕНИЕ ПРИОРИТЕТА ПРАВИЛА

Приоритет выполнения правила определяется положением правила в списке. Первое правило в списке обладает самым высоким приоритетом.

Каждое создаваемое вручную пакетное правило добавляется в конец списка пакетных правил.

Правила программ сгруппированы по имени программы, и приоритет правил распространяется только на определенную группу. Созданные вручную правила программы имеют более высокий приоритет, чем наследуемые правила группы.

- *Чтобы изменить приоритет пакетного правила, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. В правой части окна нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Пакетные правила** выберите правило и переместите его на нужное место в списке, нажимая на кнопку **Вверх** или **Вниз**.

- *Чтобы изменить приоритет правил программы или группы, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. В правой части окна нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Правила программ** выберите программу или группу и откройте окно настройки правил, нажав на кнопку **Изменить**.

5. В открывшемся окне на закладке **Сетевые правила** выберите правило и переместите его на нужное место в списке, нажимая на кнопку **Вверх** или **Вниз**.

НАСТРОЙКА УВЕДОМЛЕНИЙ ОБ ИЗМЕНЕНИЯХ СЕТИ

Параметры сетевых соединений могут меняться в ходе работы. Вы можете получать уведомления об изменениях параметров сетевого соединения.

- *Чтобы настроить уведомления об изменениях параметров сетевого соединения, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. В правой части в блоке **Сети** выберите сетевое соединение и откройте окно параметров сети, нажав на кнопку **Изменить**.

4. В открывшемся окне на закладке **Дополнительно** в блоке **Информировать** установите флажки для тех событий, о которых вы хотите получать уведомления.

Дополнительные параметры работы Сетевого экрана

Дополнительно можно настроить следующие параметры работы Сетевого экрана:

- разрешение активного режима FTP;
- блокирование соединения, если нет возможности запроса действия (не загружен интерфейс программы);
- работа до полной остановки системы.

По умолчанию все параметры включены.

Чтобы настроить дополнительные параметры работы Сетевого экрана, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. В правой части окна нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Пакетные правила** откройте окно настройки дополнительных параметров, нажав на кнопку **Дополнительно**.
5. В открывшемся окне **Дополнительно** установите / снимите флажки рядом с нужными параметрами.

Защита от сетевых атак

Защита от сетевых атак отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на ваш компьютер, Kaspersky Internet Security блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

По умолчанию блокирование происходит на один час. На экран выводится уведомление о том, что была произведена попытка сетевой атаки с указанием информации об атакующем компьютере. Описания известных в настоящее время сетевых атак (см. раздел «Виды обнаруживаемых сетевых атак» на стр. 122) и методов борьбы с ними приведены в базах Kaspersky Internet Security. Пополнение списка атак, обнаруживаемых Защитой от сетевых атак, выполняется в процессе обновления (см. раздел «Обновление» на стр. 79) баз.

В этом разделе

Виды обнаруживаемых сетевых атак

В настоящее время существует множество различных видов сетевых атак. Эти атаки используют уязвимости операционной системы, а также иного установленного программного обеспечения системного и прикладного характера.

Чтобы своевременно обеспечивать безопасность компьютера, важно знать, какого рода сетевые атаки могут ему угрожать. Известные сетевые атаки можно условно разделить на три большие группы:

- *Сканирование портов* – этот вид угроз сам по себе не является атакой, но обычно предшествует ей, поскольку это один из основных способов получить сведения об удаленном компьютере. Данный способ заключается в сканировании UDP- / TCP-портов, используемых сетевыми сервисами на интересующем злоумышленника компьютере, для выяснения их состояния (закрытые или открытые порты).

  Сканирование портов позволяет понять, какие типы атак на данную систему могут оказаться удачными, а какие нет. Кроме того, полученная в результате сканирования информация («слепок» системы) даст злоумышленнику представление о типе операционной системы на удаленном компьютере. Это еще более ограничивает круг потенциальных атак и, соответственно, время, затрачиваемое на их проведение, а также позволяет использовать специфические для данной операционной системы уязвимости.

- *DoS-атаки*, или атаки, вызывающие отказ в обслуживании, – это атаки, в результате которых атакуемая система приводится в нестабильное либо полностью нерабочее состояние. Последствиями такого типа атак может стать отсутствие возможности использовать информационные ресурсы, на которые они направлены (например, невозможность доступа в интернет).

  Существует два основных типа DoS-атак:

  - отправка компьютеру-жертве специально сформированных пакетов, не ожидаемых этим компьютером, что приводит к перезагрузке или остановке системы;

  - отправка компьютеру-жертве большого количества пакетов в единицу времени, которые этот компьютер не в состоянии обработать, что приводит к исчерпанию ресурсов системы.

  Яркими примерами данной группы атак могут служить следующие:

  - Атака *Ping of death* – состоит в посылке ICMP-пакета, размер которого превышает допустимое значение в 64 КБ. Эта атака может привести к аварийному завершению работы некоторых операционных систем.

  - Атака *Land* – заключается в передаче на открытый порт вашего компьютера запроса на установление соединения с самим собой. Атака приводит к зацикливанию компьютера, в результате чего сильно возрастает загрузка процессора, а кроме того, возможно аварийное завершение работы некоторых операционных систем.

  - Атака *ICMP Flood* – заключается в отправке на ваш компьютер большого количества ICMP-пакетов. Атака приводит к тому, что компьютер вынужден отвечать на каждый поступивший пакет, в результате чего сильно возрастает загрузка процессора.

  - Атака *SYN Flood* – заключается в отправке на ваш компьютер большого количества запросов на установку соединения. Система резервирует определенные ресурсы для каждого из таких соединений, в результате чего полностью расходует свои ресурсы и перестает реагировать на другие попытки соединения.

- *Атаки-вторжения*, целью которых является «захват» системы. Это самый опасный тип атак, поскольку в случае их успешного выполнения система полностью переходит под контроль злоумышленника.

  Данный тип атак применяется, когда злоумышленнику необходимо получить конфиденциальную информацию с удаленного компьютера (например, номера кредитных карт, пароли) либо просто закрепиться в системе для последующего использования ее вычислительных ресурсов в своих целях (использование захваченной системы в зомби-сетях либо как плацдарма для новых атак).

  В эту группу входит самое большое количество атак. Их можно разделить на три подгруппы в зависимости от установленной на компьютер пользователя операционной системы: атаки на Microsoft Windows, атаки на Unix, а также общая группа для сетевых сервисов, использующихся в обеих операционных системах.

  Наиболее распространенные виды атак, использующих сетевые сервисы операционной системы:

- *Атаки на переполнение буфера*. Переполнение буфера возникает из-за отсутствия контроля (либо в случае его недостаточности) при работе с массивами данных. Это один из самых старых типов уязвимостей; он наиболее прост для эксплуатации злоумышленником.

- *Атаки, основанные на ошибках форматных строк*. Ошибки форматных строк возникают из-за недостаточного контроля значений входных параметров функций форматного ввода-вывода типа *printf()*, *fprintf()*, *scanf()* и прочих из стандартной библиотеки языка Си. Если подобная уязвимость присутствует в программном обеспечении, то злоумышленник, имеющий возможность посылать специальным образом сформированные запросы, может получить полный контроль над системой.

  Система обнаружения вторжений автоматически анализирует и предотвращает использование подобных уязвимостей в наиболее распространенных сетевых сервисах (FTP, POP3, IMAP), если они функционируют на компьютере пользователя.

- *Атаки, ориентированные на компьютеры с установленной операционной системой Microsoft Windows,* основаны на использовании уязвимостей установленного на компьютере программного обеспечения (например, таких программ, как Microsoft SQL Server, Microsoft Internet Explorer, Messenger, а также системных компонентов, доступных по сети, – DCom, SMB, Wins, LSASS, IIS5).

Кроме того, частными случаями атак-вторжений можно назвать использование различного вида вредоносных скриптов, в том числе скриптов, обрабатываемых Microsoft Internet Explorer, а также разновидности червя Helkern. Суть атаки последнего типа заключается в отправке на удаленный компьютер UDP-пакета специального вида, способного выполнить вредоносный код.

Включение и выключение Защиты от сетевых атак

По умолчанию Защита от сетевых атак включен и работает в рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Защиту от сетевых атак при необходимости.

Чтобы выключить использование Защиты от сетевых атак, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Защита от сетевых атак**.
3. В правой части окна снимите флажок **Включить Защиту от сетевых атак**.

Изменение параметров блокирования

По умолчанию Защита от сетевых атак блокирует сетевую активность атакующего компьютера в течение 60 минут. Вы можете отменить блокирование выбранного компьютера или изменить время блокирования.

Чтобы изменить время блокирования атакующего компьютера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Защита от сетевых атак**.
3. В правой части окна установите флажок **Добавить атакующий компьютер в список блокирования на** и задайте время блокирования.

Чтобы отменить блокирование атакующего компьютера, выполните следующие действия:

1. Откройте главное окно программы (см. стр. 37).
2. В нижней части окна выберите раздел **Мониторинг сети**.
3. В открывшемся окне **Мониторинг сети** на закладке **Заблокированные компьютеры** выберите заблокированный компьютер и нажмите на кнопку **Разблокировать**.

ПРОВЕРКА ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ

Соединение с использованием протоколов SSL / TLS обеспечивает защиту канала обмена данными в интернете. Протоколы SSL / TLS позволяют идентифицировать обменивающиеся данными стороны на основе электронных сертификатов, шифровать передаваемые данные и обеспечивать их целостность в процессе передачи.

Эти особенности протокола используются злоумышленниками для распространения вредоносных программ, поскольку большинство антивирусных продуктов не проверяет SSL / TLS-трафик.

Kaspersky Internet Security проверяет защищенные соединения с помощью сертификата «Лаборатории Касперского».

Если при соединении с сервером обнаружится некорректный сертификат (например, при его подмене злоумышленником), на экран будет выведено уведомление с предложением принять или отвергнуть сертификат.

Если вы уверены в том, что соединение с веб-сайтом всегда безопасно, несмотря на некорректный сертификат, вы можете добавить веб-сайт в список доверенных адресов. Kaspersky Internet Security в дальнейшем не будет проверять защищенное соединение с этим веб-сайтом.

Вы можете использовать Мастер установки сертификата, чтобы в полуинтерактивном режиме установить сертификат для проверки защищенных соединений в браузерах Microsoft Internet Explorer, Mozilla Firefox (если он не запущен) и Google Chrome, а также чтобы получить инструкции по установке сертификата «Лаборатории Касперского» для браузера Opera.

- *Чтобы включить проверку защищенных соединений и установить сертификат «Лаборатории Касперского», выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** компонент **Сеть**.
  3. В открывшемся окне установите флажок **Проверять защищенные соединения**. При первом включении этого параметра Мастер установки сертификата запускается автоматически.
  4. Если мастер не запустился, нажмите на кнопку **Установить сертификат**. Будет запущен мастер, следуя указаниям которого вы установите сертификат «Лаборатории Касперского».

В ЭТОМ РАЗДЕЛЕ

ПРОВЕРКА ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В MOZILLA FIREFOX

Браузер Mozilla Firefox не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при использовании Firefox необходимо установить сертификат «Лаборатории Касперского» вручную.

Вы также можете использовать Мастер установки сертификатов, если браузер не запущен.

- *Чтобы вручную установить сертификат «Лаборатории Касперского», выполните следующие действия:*

  1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
  2. В открывшемся окне выберите раздел **Дополнительно**.
  3. В блоке **Сертификаты** выберите закладку **Безопасность** и нажмите на кнопку **Просмотр сертификатов**.

4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Восстановить**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. В открывшемся окне установите флажки, чтобы выбрать действия, для проверки которых будет применяться установленный сертификат. Для просмотра информации о сертификате нажмите на кнопку **Просмотр**.

Чтобы вручную установить сертификат «Лаборатории Касперского» для Mozilla Firefox версии 3.x, выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.

2. В открывшемся окне выберите раздел **Дополнительно**.

3. На закладке **Шифрование** нажмите на кнопку **Просмотр сертификатов**.

4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импортировать**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. В открывшемся окне установите флажки, чтобы выбрать действия, для проверки которых будет применяться установленный сертификат. Для просмотра информации о сертификате нажмите на кнопку **Просмотреть**.

Если ваш компьютер работает под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7, то путь к файлу сертификата «Лаборатории Касперского» будет следующим: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

Проверка защищенных соединений в Opera

Браузер Opera не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при пользовании Opera необходимо установить сертификат «Лаборатории Касперского» вручную.

Чтобы установить сертификат «Лаборатории Касперского», выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.

2. В открывшемся окне выберите раздел **Дополнительно**.

3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.

4. В открывшемся окне выберите закладку **Поставщики** и нажмите на кнопку **Импорт**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен. Для просмотра информации о сертификате и выбора действий, при которых будет использоваться сертификат, выберите сертификат в списке и нажмите на кнопку **Просмотреть**.

Чтобы установить сертификат «Лаборатории Касперского» для Opera версии 9.x, выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
2. В открывшемся окне выберите раздел **Дополнительно**.
3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.
4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импорт**.
5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен.

Если ваш компьютер работает под управлением операционной системы Microsoft Windows Vista и Microsoft Windows 7, то путь к файлу сертификата «Лаборатории Касперского» будет следующим: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

МОНИТОРИНГ СЕТИ

Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности в реальном времени.

Чтобы посмотреть информацию о сетевой активности, выполните следующие действия:

1. Откройте главное окно программы (см. стр. 37).
2. В нижней части окна выберите раздел **Мониторинг сети**.

   В открывшемся окне **Мониторинг сети** на закладке **Сетевая активность** представлена информация о сетевой активности.

При работе на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вы можете открыть Мониторинг сети с помощью Kaspersky Gadget. Для этого Kaspersky Gadget должен быть настроен таким образом, чтобы одной из его кнопок была назначена функция открывания окна Мониторинга сети (см. раздел «Как использовать Kaspersky Gadget» на стр. 65).

Чтобы открыть Мониторинг сети с помощью гаджета,

нажмите на кнопку со значком **Мониторинг сети** в интерфейсе Kaspersky Gadget.

В открывшемся окне **Мониторинг сети** на закладке **Сетевая активность** представлена информация о сетевой активности.

НАСТРОЙКА ПАРАМЕТРОВ ПРОКСИ-СЕРВЕРА

Если выход в интернет осуществляется через прокси-сервер, может возникнуть необходимость настроить параметры подключения к нему. Kaspersky Internet Security использует эти параметры в работе некоторых компонентов защиты, а также для обновления баз и программных модулей.

Если в вашей сети установлен прокси-сервер, который использует нестандартный порт, необходимо добавить этот порт в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 128).

Чтобы настроить параметры подключения к прокси-серверу, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** компонент **Сеть**.
3. В блоке **Прокси-сервер** нажмите на кнопку **Настройка прокси-сервера**.
4. В открывшемся окне **Параметры прокси-сервера** задайте нужные параметры подключения к прокси-серверу.

Формирование списка контролируемых портов

При работе таких компонентов защиты, как Почтовый Антивирус, Анти-Спам, Веб-Антивирус (на стр. 96) и IM-Антивирус, контролируются потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP-порты вашего компьютера. Так, например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, а Веб-Антивирус – по протоколам HTTP, HTTPS и FTP.

Вы можете включить контроль всех или только выбранных сетевых портов. При контроле выбранных портов можно сформировать список программ, для которых требуется контроль всех портов. Рекомендуется включить в этот список программы, которые принимают или передают данные по протоколу FTP.

Чтобы добавить порт в список контролируемых портов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Сеть**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты** и нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.
4. По ссылке **Добавить**, расположенной под списком портов в верхней части окна, откройте окно **Сетевой порт** и введите номер и описание порта.

Чтобы исключить порт из списка контролируемых портов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Сеть**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты** и нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.
4. В списке портов в верхней части окна снимите флажок рядом с описанием порта, который нужно исключить.

Чтобы сформировать список программ, для которых необходимо контролировать все порты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Сеть**.

3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты** и нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.

4. Установите флажок **Контролировать все порты для указанных программ** и в списке программ, расположенном ниже, установите флажки напротив названий программ, для которых нужно контролировать все порты.

5. Если нужная программа отсутствует в списке, добавьте ее следующим образом:

   a. По ссылке **Добавить**, расположенной под списком программ, откройте меню и выберите один из пунктов:

      - Чтобы указать расположение исполняемого файла программы, выберите пункт **Обзор** и укажите расположение файла на компьютере.

      - Чтобы выбрать программу из списка программ, работающих в данный момент, выберите пункт **Программы**. В открывшемся окне **Выбор программы** выберите нужную программу.

   b. В окне **Программа** введите описание для выбранной программы.

Анти-Спам

Анти-Спам обнаруживает нежелательную корреспонденцию (спам) и обрабатывает ее в соответствии с правилами вашего почтового клиента.

Анти-Спам в виде модуля расширения встраивается в следующие почтовые клиенты:

- Microsoft Office Outlook (на стр. 143);
- Microsoft Outlook Express (Windows Mail) (на стр. 143);
- The Bat! (на стр. 144);
- Thunderbird (на стр. 145).

Списки запрещенных и разрешенных отправителей позволяют указать, письма с каких адресов следует считать полезными, а с каких – спамом. К спаму могут быть отнесены письма, адресованные не вам (см. стр. 139). Кроме того, Анти-Спам может анализировать сообщение на наличие разрешенных и запрещенных фраз, а также фраз из списка нецензурных выражений.

Чтобы Анти-Спам эффективно распознавал спам и полезную почту, его следует обучить (см. раздел «Обучение Анти-Спама» на стр. 132).

Анти-Спам использует самообучающийся алгоритм, позволяющий компоненту с течением времени более точно различать спам и полезную почту. Источником данных для алгоритма является содержимое письма.

Работа компонента Анти-Спам разделена на два этапа:

1. Применение к сообщению жестких критериев фильтрации. Эти критерии позволяют быстро определить, является ли сообщение спамом. Анти-Спам присваивает сообщению статус *спам* или *не спам*, проверка останавливается, и сообщение передается для обработки почтовому клиенту (см. ниже шаги алгоритма 1–5).

2. Изучение почтовых сообщений, прошедших фильтрацию. Такие сообщения уже нельзя однозначно оценивать как спам. Поэтому Анти-Спам вычисляет *вероятность* их принадлежности к спаму.

Алгоритм работы Анти-Спама состоит из следующих шагов:

1. Адрес отправителя почтового сообщения проверяется на присутствие в списках разрешенных и запрещенных отправителей.

   - Если адрес отправителя находится в списке разрешенных отправителей, сообщению присваивается статус *не спам*.

   - Если адрес отправителя находится в списке запрещенных отправителей, почтовому сообщению присваивается статус *спам*.

2. Если сообщение было отправлено с помощью Microsoft Exchange Server и проверка таких сообщений выключена, то сообщению присваивается статус *не спам*.

3. Сообщение анализируется на наличие строк из списка разрешенных фраз. Если найдена хотя бы одна строка из этого списка, сообщению присваивается статус *не спам*. По умолчанию этот шаг пропускается.

4. Сообщение анализируется на наличие строк из списка запрещенных фраз и списка нецензурных фраз. При обнаружении в сообщении слов из этих списков их весовые коэффициенты суммируются. Если сумма коэффициентов превысит 100, сообщению будет присвоен статус *спам*. По умолчанию данный шаг пропускается.

5. Если текст сообщения содержит адрес, входящий в базу фишинговых или подозрительных веб-адресов, письму присваивается статус *спам*.

6. Сообщение анализируется с помощью эвристических правил. Если в результате этого анализа в сообщении найдены признаки, характерные для спама, вероятность того, что сообщение является спамом, увеличивается.

7. Сообщение анализируется с помощью технологии GSG. При этом Анти-Спам анализирует изображения в составе почтового сообщения. Если в них найдены признаки, характерные для спама, вероятность того, что сообщение является спамом, увеличивается.

8. Анализируются вложенные в сообщение документы в формате RTF. Анти-Спам ищет во вложенных документах признаки, характерные для спама. По окончании анализа Анти-Спам вычисляет, насколько увеличилась вероятность того, что сообщение является спамом. По умолчанию использование этой технологии выключено.

9. Выполняются проверки на наличие дополнительных признаков, характерных для спама. Обнаружение каждого признака увеличивает вероятность того, что проверяемое сообщение является спамом.

10. Если Анти-Спам был обучен, сообщение проверяется с помощью технологии iBayes. Самообучающийся алгоритм iBayes вычисляет вероятность того, что сообщение является спамом, на основе частоты употребления в его тексте фраз, характерных для спама.

> Обучение выполняется, только если в вашем Kaspersky Internet Security включена функция самообучающегося алгоритма анализа текста iBayes. Наличие этой функции зависит от языка локализации программы.

В результате анализа сообщения определяется вероятность того, что почтовое сообщение является спамом, выражаемая значением *фактора спама*. Сообщению присваивается статус *спам* или *потенциальный спам* в зависимости от пороговых значений фактора спама (см. раздел «Регулировка пороговых значений фактора спама» на стр. 141). Кроме того, по умолчанию для спама и потенциального спама в поле **Тема** добавляется метка **[!! SPAM]** или **[?? Probable Spam]** (см. раздел «**Добавление метки к теме сообщения**» на стр. 142). Затем сообщение обрабатывается по заданным вами правилам для почтовых клиентов (см. раздел «Настройка обработки спама почтовыми клиентами» на стр. 143).

В ЭТОМ РАЗДЕЛЕ

ВКЛЮЧЕНИЕ И ВЫКЛЮЧЕНИЕ АНТИ-СПАМА

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

Чтобы выключить использование Анти-Спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна снимите флажок **Включить Анти-Спам**.

ИЗМЕНЕНИЕ И ВОССТАНОВЛЕНИЕ УРОВНЯ ЗАЩИТЫ ОТ СПАМА

В зависимости от того, насколько часто вы получаете спам, можно выбрать один из предустановленных уровней защиты от спама или настроить параметры работы Анти-Спама самостоятельно. Уровням защиты от спама соответствуют уровни безопасности, сформированные специалистами «Лаборатории Касперского»:

- **Высокий**. Данный уровень безопасности следует использовать, если вы получаете спам слишком часто, например при использовании бесплатного почтового сервиса. При выборе этого уровня может возрасти частота распознавания полезной почты как спама.
- **Рекомендуемый**. Данный уровень безопасности следует использовать в большинстве случаев.
- **Низкий**. Данный уровень безопасности следует использовать, если вы редко получаете спам, например при работе в защищенной среде системы корпоративной почты. При выборе этого уровня может снизиться частота распознавания полезной почты как спама и потенциального спама.

Настраивая параметры работы Анти-Спама, всегда можно вернуться к рекомендуемым значениям. Эти параметры считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень защиты от спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

   В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

   При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить параметры защиты от спама по умолчанию, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Обучение Анти-Спама

Один из инструментов распознавания спама – самообучающийся алгоритм iBayes. В результате выполнения этого алгоритма выносится решение о присвоении сообщению того или иного статуса на основе входящих в него фраз. До начала работы алгоритма iBayes необходимо предоставить Анти-Спаму образцы строк, входящих в полезные и спам-сообщения, то есть *обучить* его.

Обучение выполняется, если в Kaspersky Internet Security включена функция самообучающегося алгоритма анализа текста iBayes. Наличие этой функции зависит от языка локализации программы.

Существует несколько подходов к обучению Анти-Спама:

- Обучение Анти-Спама на исходящих сообщениях.
- Обучение в процессе работы с электронной почтой с помощью почтового клиента, в окне которого предусмотрены специальные кнопки и пункты меню для обучения.
- Обучение при работе с отчетами Анти-Спама.

В этом разделе

Обучение на исходящих сообщениях

Вы можете обучить Анти-Спам на примере 50 исходящих сообщений. После включения обучения Анти-Спам будет анализировать каждое из отправляемых вами писем, используя его в качестве образца полезного сообщения. После отправки пятидесятого сообщения обучение будет завершено.

Чтобы включить обучение Анти-Спама на исходящих сообщениях, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Дополнительно** в блоке **Исходящие сообщения** установите флажок **Обучаться на исходящих сообщениях**.

При обучении на исходящих сообщениях адреса получателей этих сообщений автоматически добавляются в список разрешенных отправителей. Вы можете отключить эту функцию (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 133).

ОБУЧЕНИЕ ЧЕРЕЗ ИНТЕРФЕЙС ПОЧТОВОГО КЛИЕНТА

Обучить Анти-Спам в процессе непосредственной работы с электронной почтой можно с помощью кнопок панели инструментов и пунктов меню вашего почтового клиента.

Кнопки и пункты меню, предназначенные для обучения Анти-Спама, появляются в интерфейсе почтовых клиентов только после установки Kaspersky Internet Security.

Чтобы обучить Анти-Спам через интерфейс почтового клиента, выполните следующие действия:

1. Запустите почтовый клиент.
2. Выберите письмо, с помощью которого вы хотите обучить Анти-Спам.
3. В зависимости от того, каким почтовым клиентом вы пользуетесь, выполните следующие действия:
   - нажмите на кнопку **Спам** или **Не Спам** в панели инструментов Microsoft Office Outlook;
   - нажмите на кнопку **Спам** или **Не Спам** в панели инструментов Microsoft Outlook Express (Windows Mail);
   - воспользуйтесь специальными пунктами **Пометить как спам** и **Пометить как НЕ спам** в меню **Специальное** почтового клиента The Bat!;
   - воспользуйтесь кнопкой **Спам / Не спам** в панели инструментов почтового клиента Mozilla Thunderbird.

После выбора одного из перечисленных выше действий Анти-Спам проводит обучение на выбранном письме. Если вы выделите несколько писем, обучение будет происходить на всех выделенных письмах.

Если письмо отмечено как полезное, адрес отправителя письма автоматически добавляется в список разрешенных отправителей. Вы можете отключить эту функцию (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 133).

ДОБАВЛЕНИЕ АДРЕСА В СПИСОК РАЗРЕШЕННЫХ ОТПРАВИТЕЛЕЙ

При обучении Анти-Спама в окне почтового клиента адреса отправителей полезных писем автоматически добавляются в список разрешенных отправителей (см. раздел «Запрещенные и разрешенные отправители» на стр. 138). В этот же список добавляются адреса получателей исходящих сообщений при обучении на исходящих сообщениях.

Вы можете отключить эту функцию, чтобы список разрешенных отправителей не пополнялся автоматически в результате обучения.

Чтобы отключить добавление адреса в список разрешенных отправителей, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Точные методы** в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**.

   Откроется окно **Разрешенные отправители**.
5. Снимите флажок **Добавлять адреса разрешенных отправителей при обучении Анти-Спама**.

Обучение с помощью отчетов

Предусмотрена возможность обучать Анти-Спам на основе его отчетов, в которых отображается информация о письмах, отнесенных к категории «потенциальный спам». Обучение заключается в присвоении письмам меток **спам** или **не спам**, а также в добавлении их отправителей в списки разрешенных или запрещенных отправителей (см. раздел «Запрещенные и разрешенные отправители» на стр. 138).

Метки **спам** и **не спам** присваиваются письмам, если в Kaspersky Internet Security включена функция самообучающегося алгоритма анализа текста iBayes. Наличие этой функции зависит от языка локализации программы.

Чтобы провести обучение Анти-Спама на основе отчета, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна нажмите на кнопку **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.
4. В левой части окна выберите раздел **Анти-Спам**.
5. В правой части окна по записи в графе **Объект** выберите письма, на основе которых вы хотите обучить Анти-Спам. Для каждого из таких писем по правой клавише мыши откройте контекстное меню и выберите один из пунктов меню в соответствии с тем, какое действие нужно выполнить с письмом:
   - Отметить как спам.
   - Отметить как не спам.
   - Добавить в список разрешенных отправителей.
   - Добавить в список запрещенных отправителей.

Проверка ссылок в почтовых сообщениях

Анти-Спам может проверять содержащиеся в почтовых сообщениях ссылки на принадлежность к списку подозрительных веб-адресов и к списку фишинговых веб-адресов. Эти списки включены в комплект поставки Kaspersky Internet Security. Если вы участвуете в Kaspersky Security Network (на стр. 187), то для проверки ссылок Kaspersky Internet Security также обращается в Kaspersky Security Network. Если в письме обнаруживается

фишинговая или подозрительная ссылка, а также если элементы фишинга обнаруживаются в тексте письма, то это письмо идентифицируется как спам.

Для проверки ссылок в почтовых сообщениях можно дополнительно использовать эвристический анализ.

Чтобы включить проверку ссылок по базам подозрительных и фишинговых адресов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Точные методы** в блоке **Считать спамом следующие сообщения** установите флажки **Со ссылками из базы подозрительных веб-адресов** и **С элементами фишинга**.

Чтобы включить использование эвристического анализа, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Точные методы** в блоке **Считать спамом следующие сообщения** нажмите на кнопку **Дополнительно**.
5. В открывшемся окне **Настройка Анти-Фишинга** установите флажок **Использовать эвристический анализ для проверки почты на наличие фишинга** и задайте уровень детализации проверки с помощью ползунка.

ОПРЕДЕЛЕНИЕ СПАМА ПО ФРАЗАМ И АДРЕСАМ. ФОРМИРОВАНИЕ СПИСКОВ

Вы можете составить списки разрешенных, запрещенных и нецензурных ключевых фраз, а также списки разрешенных и запрещенных адресов отправителей и список ваших адресов. Если эти списки используются, Анти-Спам проверяет содержимое письма на наличие в нем словосочетаний, внесенных в списки фраз, а адреса отправителя и получателей – на соответствие записям в списках адресов. Обнаружив искомые фразу или адрес, Анти-Спам идентифицирует письмо как полезное или как спам в зависимости от того, в каком из списков присутствует найденные фраза или адрес.

Спамом считаются следующие письма:

- содержащие запрещенные или нецензурные фразы с суммарным весовым коэффициентом, превышающим 100;
- отправленные с запрещенного адреса или адресованные не вам.

Полезными считаются следующие письма:

- содержащие разрешенные фразы;
- отправленные с разрешенного адреса.

В этом разделе

Использование масок фраз и адресов

В списках разрешенных, запрещенных и нецензурных фраз вы можете использовать маски фраз. В списках разрешенных и запрещенных адресов отправителей, а также в списке доверенных адресов вы можете использовать маски адресов.

Маска представляет собой строку-шаблон, с которой сверяется фраза или адрес. Некоторые символы в маске используются для замены других символов: * заменяет любую последовательность символов, а ? – любой один символ. Если в маске используются такие символы, то ей могут соответствовать несколько фраз или несколько адресов (см. примеры ниже).

Если символ * или ? входит в состав фразы (например, Который час?), перед ним нужно использовать символ \, чтобы Анти-Спам корректно его распознал. Таким образом, вместо символа * в маске нужно использовать сочетание *, вместо символа ? – сочетание \? (например, Который час\?).

Примеры масок фраз:

- Посетите наш *! – этой маске соответствует письмо, содержащее фразу, которая начинается словами Посетите наш, имеет любое продолжение и завершается символом !.
- Предлагаем – этой маске соответствует письмо, содержащее фразу, которая начинается словом Предлагаем и имеет любое продолжение.

Примеры масок адресов:

- admin@test.com – этой маске соответствует только адрес admin@test.com.
- admin@* – этой маске соответствует адрес отправителя с именем admin, например: admin@test.com, admin@example.org.
- *@test* – этой маске соответствует адрес любого отправителя письма с почтового домена, начинающегося с test, например: admin@test.com, info@test.org.
- info.*@test.??? – этой маске соответствует адрес любого отправителя письма, имя которого начинается с info. и имя почтового домена которого начинается с test. и оканчивается последними тремя любыми символами, например: info.product@test.com, info.company@test.org, но не info.product@test.ru.

Запрещенные и разрешенные фразы

В список *запрещенных фраз* вы можете внести фразы, которые, согласно вашим наблюдениям, характерны для спама, и задать для каждой фразы весовой коэффициент. *Весовой коэффициент* позволяет указать, насколько характерна фраза для спам-писем: чем выше коэффициент, тем более вероятно, что письмо с этой фразой является спамом. Весовой коэффициент фразы может принимать значения от 0 до 100. Если сумма весовых коэффициентов всех фраз, обнаруженных в письме, превысит 100, письмо будет идентифицировано как спам.

Ключевые фразы, характерные для полезных писем, можно внести в список *разрешенных фраз*. Обнаружив такую фразу в письме, Анти-Спам идентифицирует его как полезное (не спам).

В списки запрещенных и разрешенных фраз вы можете вносить как фразы целиком, так и их маски (см. раздел «Использование масок фраз и адресов» на стр. 136).

Чтобы сформировать список запрещенных или разрешенных фраз, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Точные методы** выполните следующие действия:

   - Если нужно сформировать список запрещенных фраз, в блоке **Считать спамом следующие сообщения** установите флажок **С запрещенными фразами** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Запрещенные фразы**.

   - Если нужно сформировать список разрешенных фраз, в блоке **Считать полезными следующие сообщения** установите флажок **С разрешенными фразами** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Разрешенные фразы**.
5. По ссылке **Добавить** откройте окно **Запрещенная фраза** (или окно **Разрешенная фраза**).
6. Введите фразу целиком или маску фразы, для запрещенной фразы укажите весовой коэффициент, а затем нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

НЕЦЕНЗУРНЫЕ ФРАЗЫ

Специалистами «Лаборатории Касперского» сформирован список нецензурных фраз, который входит в поставку Kaspersky Internet Security. В списке хранятся нецензурные фразы, наличие которых в сообщении с большой долей вероятности указывает на то, что сообщение является спамом. Вы можете дополнить данный список и внести в него как фразы целиком, так и их маски (см. раздел «Использование масок фраз и адресов» на стр. 136).

Если для пользователя включен Родительский контроль (см. стр. 155) и установлен пароль (см. стр. 69) для изменения параметров Родительского контроля, то для просмотра списка нецензурных фраз потребуется ввести пароль.

Чтобы изменить список нецензурных фраз, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Точные методы** в блоке **Считать спамом следующие сообщения** установите флажок **С запрещенными фразами** и нажмите на кнопку **Выбрать**.

   Откроется окно **Запрещенные фразы**.

5. Установите флажок **Считать запрещенными нецензурные фразы** и по ссылке **нецензурные фразы** откройте окно **Соглашение**.

6. Ознакомьтесь с текстом соглашения и, если вы согласны с условиями, изложенными в окне, установите флажок в нижней части окна и нажмите на кнопку **ОК**.

   Откроется окно **Нецензурная лексика**.

7. По ссылке **Добавить** откройте окно **Запрещенная фраза**.

8. Введите фразу целиком или маску фразы, укажите весовой коэффициент фразы и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

Запрещенные и разрешенные отправители

В список *запрещенных отправителей* вы можете внести адреса отправителей, письма от которых Анти-Спам будет идентифицировать как спам. Адреса отправителей писем, от которых не ожидается спама, хранятся в списке *разрешенных отправителей*. Этот список создается автоматически во время обучения компонента Анти-Спам (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 133). Кроме того, вы можете пополнить список самостоятельно.

В списки разрешенных и запрещенных отправителей вы можете внести как адреса полностью, так и маски адресов (см. раздел «Использование масок фраз и адресов» на стр. 136).

Чтобы сформировать список запрещенных или разрешенных отправителей, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Точные методы** выполните следующие действия:

   - Если нужно сформировать список запрещенных отправителей, в блоке **Считать спамом следующие сообщения** установите флажок **От запрещенных отправителей** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Запрещенные отправители**.

   - Если нужно сформировать список разрешенных отправителей, в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Разрешенные отправители**.

5. По ссылке **Добавить** откройте окно **Маска адреса электронной почты**.

6. Введите маску адреса и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

ВАШИ АДРЕСА

Вы можете сформировать список ваших адресов электронной почты, чтобы Анти-Спам отмечал как спам письма, адресованные не вам.

Чтобы сформировать список ваших адресов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Точные методы** установите флажок **Адресованные не мне** и нажмите на кнопку **Мои адреса**.

   Откроется окно **Мои адреса**.
5. По ссылке **Добавить** откройте окно **Маска адреса электронной почты**.
6. Введите маску адреса и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

ЭКСПОРТ И ИМПОРТ СПИСКОВ ФРАЗ И АДРЕСОВ

Создав списки фраз и адресов, вы можете затем многократно использовать их: например, переносить адреса в аналогичный список на другом компьютере с установленным Kaspersky Internet Security.

Последовательность действий при этом такова:

1. Выполните *экспорт* – скопируйте записи из списка в файл.
2. Перенесите сохраненный файл на другой компьютер (например, перешлите по почте или переместите на съемном носителе).
3. Выполните *импорт* – внесите записи из файла в аналогичный список на другом компьютере.

При экспорте списка вам будет предложено копировать только выбранный элемент списка или весь список целиком. При импорте можно добавить новые элементы в список или заменить существующий список импортируемым.

Для адресов из списка разрешенных отправителей предусмотрена возможность импорта адресов из адресной книги Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail).

Чтобы экспортировать записи из списка, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Точные методы** установите флажок в строке, содержащей название списка, из которого нужно экспортировать записи, и нажмите на соответствующую ему кнопку справа.

5. В открывшемся окне со списком установите флажки напротив тех записей, которые нужно включить в файл.

6. Нажмите на ссылку **Экспорт**.

   Откроется окно с предложением экспортировать только выделенные элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если в файл нужно включить только выбранные записи;
   - нажмите на кнопку **Нет**, если нужно включить список полностью.

7. В открывшемся окне укажите тип и имя сохраняемого файла и подтвердите сохранение.

Чтобы импортировать записи из файла в список, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Точные методы** установите флажок в строке, содержащей название списка, в который нужно импортировать записи, и нажмите на кнопку справа.

5. В окне со списком перейдите по ссылке **Импорт**. Если вы импортируете список разрешенных отправителей, то откроется меню, в котором нужно выбрать пункт **Импортировать из файла**. Для остальных списков выбор пункта меню не требуется.

   Если список не пуст, откроется окно с предложением добавить импортируемые элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если нужно добавить к списку записи из файла;
   - нажмите на кнопку **Нет**, если нужно заменить существующие записи списком из файла.

6. В открывшемся окне выберите файл со списком записей, которые нужно импортировать.

Чтобы импортировать список разрешенных отправителей из адресной книги, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Точные методы** в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**.

   Откроется окно **Разрешенные отправители**.

5. Перейдите по ссылке **Импорт**, откройте меню выбора источника и выберите в нем пункт **Импортировать из адресной книги**.

6. В открывшемся окне выберите нужную адресную книгу.

РЕГУЛИРОВКА ПОРОГОВЫХ ЗНАЧЕНИЙ ФАКТОРА СПАМА

Распознавание спама основано на использовании современных технологий фильтрации, позволяющих научить (см. раздел «Обучение Анти-Спама» на стр. 132) Анти-Спам отличать спам и потенциальный спам от полезной почты. При этом каждому отдельному элементу полезной почты или спама присваивается коэффициент.

Когда в ваш почтовый ящик поступает почтовое сообщение, Анти-Спам проверяет письмо на наличие элементов спама и полезной почты. Коэффициенты каждого элемента спама (полезной почты) суммируются, в результате чего вычисляется *фактор спама*. Чем больше значение фактора спама, тем выше вероятность того, что сообщение является спамом. По умолчанию сообщение считается полезным, если фактор спама не превышает 60. Если фактор спама выше 60, то сообщение считается потенциальным спамом. Если же значение превышает 90, сообщение считается спамом. Вы можете изменить пороговые значения фактора спама.

Чтобы изменить пороговые значения фактора спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Экспертные методы** в блоке **Фактор спама** отрегулируйте значения фактора спама с помощью ползунков или полей ввода с прокруткой.

ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ ПРИЗНАКОВ, ВЛИЯЮЩИХ НА ФАКТОР СПАМА

На результат вычисления фактора спама могут влиять дополнительные признаки сообщений: например, отсутствие адреса получателя в поле «Кому» или слишком длинная тема сообщения (более 250 символов). При наличии этих признаков в сообщении вероятность того, что оно является спамом, увеличивается. Соответственно, увеличивается значение фактора спама. Вы можете выбрать, какие из дополнительных признаков должны учитываться при анализе сообщения.

Чтобы использовать дополнительные признаки, увеличивающие фактор спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Экспертные методы** нажмите на кнопку **Дополнительно**.
5. В открывшемся окне **Дополнительно** установите флажки рядом с теми признаками, которые должны дополнительно учитываться при анализе сообщения, увеличивая фактор спама.

Выбор алгоритма распознавания спама

Анти-Спам анализирует почтовые сообщения, используя алгоритмы распознавания спама.

Чтобы включить использование какого-либо алгоритма распознавания спама при анализе почтовых сообщений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Экспертные методы** в блоке **Алгоритмы распознавания** установите соответствующие флажки.

Добавление метки к теме сообщения

Анти-Спам может добавлять в поле **Тема** сообщений, которые при проверке были признаны спамом или потенциальным спамом, соответствующие метки:

- **[!! SPAM]** – для сообщений, идентифицированных как спам;
- **[?? Probable Spam]** – для сообщений, идентифицированных как потенциальный спам.

Наличие таких меток в теме сообщения может вам помочь визуально отличать спам и потенциальный спам при просмотре списков сообщений.

Чтобы настроить добавление метки к теме сообщений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.
4. На закладке **Дополнительно** в блоке **Действия** установите флажки напротив названий тех меток, которые нужно добавлять к теме сообщения. При необходимости измените текст метки.

Проверка сообщений Microsoft Exchange Server

По умолчанию Анти-Спам не проверяет сообщения Microsoft Exchange Server. Вы можете включить проверку почтовых сообщений, пересылаемых в рамках внутренней сети (например, корпоративная почта).

Сообщения будут считаться внутренней почтой в том случае, если в качестве почтового клиента на всех компьютерах сети используется Microsoft Office Outlook, а почтовые ящики пользователей расположены на одном Exchange-сервере либо на соединенных серверах.

Чтобы включить проверку сообщений Microsoft Exchange Server, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

3. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Анти-Спам**.

4. На закладке **Дополнительно** в блоке **Исключения** снимите флажок **Не проверять сообщения Microsoft Exchange Server**.

НАСТРОЙКА ОБРАБОТКИ СПАМА ПОЧТОВЫМИ КЛИЕНТАМИ

Если в результате проверки выясняется, что письмо является спамом или потенциальным спамом, дальнейшие действия Анти-Спама зависят от статуса письма и от выбранного действия. По умолчанию электронные сообщения, являющиеся спамом или потенциальным спамом, модифицируются: в поле **Тема** письма добавляется метка **[!! SPAM]** или **[?? Probable Spam]** соответственно (см. раздел «Добавление метки к теме сообщения» на стр. 142).

Вы можете выбрать дополнительные действия над спамом и потенциальным спамом. В почтовых клиентах Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail) для этого предусмотрены специальные модули расширения. Для почтовых клиентов The Bat! и Thunderbird вы можете настроить правила фильтрации почты.

В ЭТОМ РАЗДЕЛЕ

MICROSOFT OFFICE OUTLOOK

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Microsoft Office Outlook. Окно настройки обработки спама открывается автоматически при первой загрузке почтового клиента после установки Kaspersky Internet Security. Кроме того, параметры обработки спама и потенциального спама в Microsoft Office Outlook приведены на специальной закладке **Анти-Спам** в меню **Сервис** → **Параметры**.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Microsoft Outlook Express (Windows Mail).

Окно настройки обработки спама открывается при первом запуске почтового клиента после установки программы. Его также можно открыть, нажав на кнопку **Настройка**, расположенную в панели инструментов почтового клиента рядом с кнопками **Спам** и **Не Спам**.

СОЗДАНИЕ ПРАВИЛА ОБРАБОТКИ СООБЩЕНИЙ НА СПАМ

Ниже приведена инструкция по созданию правила обработки сообщений на спам с применением Анти-Спама в почтовом клиенте Microsoft Office Outlook. Вы можете воспользоваться этой инструкцией и на ее основе создать собственное правило.

Чтобы создать правило обработки сообщений на спам, выполните следующие действия:

1. Запустите программу Microsoft Office Outlook и воспользуйтесь командой **Сервис** → **Правила и оповещения** главного меню программы. Способ вызова мастера зависит от используемой вами версии Microsoft Office Outlook. В данной справке приведено описание создания правила с помощью Microsoft Office Outlook 2003.

2. В окне **Правила и оповещения** перейдите на закладку **Правила для электронной почты** и нажмите на кнопку **Новое**. В результате будет запущен мастер создания нового правила. Его работа состоит из последовательности окон / шагов:

   a. Вам предлагается выбрать создание правила с нуля либо по шаблону. Выберите вариант **Создать новое правило** и в качестве условия проверки выберите **Проверка сообщений после получения**. Нажмите на кнопку **Далее**.

   b. В окне выбора условий отбора сообщений, не устанавливая флажков, нажмите на кнопку **Далее**. Подтвердите применение данного правила ко всем получаемым сообщениям в окне запроса подтверждения.

   c. В окне выбора действий над сообщениями установите в списке действий флажок **выполнить дополнительное действие**. В нижней части окна нажмите на ссылку **дополнительное действие**. В открывшемся окне выберите из раскрывающегося списка элемент **Kaspersky Anti-Spam**, нажмите на кнопку **ОК**.

   d. В окне выбора исключений из правила, не устанавливая флажков, нажмите на кнопку **Далее**.

   e. В окне завершения создания правила вы можете изменить его имя (по умолчанию установлено Kaspersky Anti-Spam). Проверьте, что флажок **Включить правило** установлен, и нажмите на кнопку **Готово**.

3. Новое правило по умолчанию будет добавлено первым в список правил окна **Правила и оповещения**. Переместите это правило в конец списка, если хотите, чтобы оно применялось к сообщению последним.

Все сообщения, поступающие в почтовый ящик, обрабатываются на основе правил. Очередность применения правил зависит от приоритета, который задан для каждого правила. Правила начинают применяться с начала списка: приоритет каждого последующего правила ниже, чем предыдущего. Вы можете понижать или повышать приоритет применения правила к сообщению, перемещая правило вниз или вверх в списке. Если вы не хотите, чтобы после выполнения какого-либо правила сообщение дополнительно обрабатывалось правилом Анти-Спама, в параметрах этого правила требуется установить флажок **остановить дальнейшую обработку правил** (см. Шаг 3 окна создания правил).

The Bat!

Действия над спамом и потенциальным спамом в почтовом клиенте The Bat! определяются средствами самого клиента.

Чтобы перейти к настройке правил обработки спама в The Bat!, выполните следующие действия:

1. В меню **Свойства** почтового клиента выберите пункт **Настройка**.

2. В дереве настройки выберите объект **Защита от спама**.

Представленные параметры защиты от спама распространяются на все установленные на компьютере модули Анти-Спама, поддерживающие работу с The Bat!.

Вам нужно определить уровень рейтинга и указать, как поступать с сообщениями, которым присвоен тот или иной рейтинг (в случае Анти-Спама – вероятность того, что письмо является спамом):

- удалять сообщения с рейтингом, превышающим указанную величину;
- перемещать сообщения с определенным рейтингом в специальную папку для спам-сообщений;

- перемещать спам-сообщения, отмеченные специальным заголовком, в папку спама;
- оставлять спам-сообщения в папке **Входящие**.

В результате обработки почтового сообщения Kaspersky Internet Security присваивает письму статус спама и потенциального спама на основании фактора, значение которого вы можете регулировать. В почтовом клиенте The Bat! реализован собственный алгоритм рейтинга сообщений на предмет спама, также основанный на факторе спама. Чтобы исключить расхождения между фактором спама в Kaspersky Internet Security и в The Bat!, всем проверенным Анти-Спамом письмам присваивается рейтинг, соответствующий статусу письма: полезная почта – 0%, потенциальный спам – 50%, спам – 100%. Таким образом, рейтинг письма в почтовом клиенте The Bat! соответствует не фактору спама, заданному в Анти-Спаме, а фактору соответствующего статуса.

Подробнее о рейтинге спама и правилах обработки см. в документации к почтовому клиенту The Bat!.

THUNDERBIRD

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Thunderbird, вызвав окно настройки с помощью команды меню **Инструменты** → **Фильтры сообщений** (подробнее о работе с почтовым клиентом см. справку Mozilla Thunderbird).

Модуль расширения Анти-Спама для Thunderbird позволяет проводить обучение на письмах, полученных и отправленных с помощью этого почтового клиента, а также проверять почтовую корреспонденцию на содержание спама. Модуль встраивается в Thunderbird и перенаправляет письма компоненту Анти-Спам для их проверки при выполнении команды меню **Инструменты** → **Запустить в папке антиспам-фильтры**. Таким образом, вместо Thunderbird проверку сообщений производит Kaspersky Internet Security. При этом функциональность Thunderbird не изменяется.

Статус модуля расширения Анти-Спама отображается в виде значка в строке состояния Thunderbird. Серый цвет значка информирует вас о том, что в работе плагина возникла проблема или компонент Анти-Спам отключен. Двойным щелчком мыши на значке вы можете открыть окно настройки параметров Kaspersky Internet Security. Чтобы перейти к настройке параметров Анти-Спама, нажмите на кнопку **Настройка** в блоке **Анти-Спам**.

АНТИ-БАННЕР

Анти-Баннер предназначен для блокирования показа баннеров на просматриваемых вами веб-страницах и в интерфейсе некоторых компьютерных программ. Рекламная информация на баннерах может отвлекать вас от дел, а загрузка баннеров увеличивает объем загружаемого трафика.

Прежде чем отобразиться на веб-странице или в окне компьютерной программы, баннер должен быть загружен из интернета. Анти-Баннер проверяет адрес, с которого загружается баннер. Если адрес соответствует какой-либо маске из списка, включенного в поставку Kaspersky Internet Security, либо из составленного вами списка запрещенных адресов баннеров, Анти-Баннер блокирует баннер. Для блокирования баннеров, маски адресов которых отсутствуют в упомянутых списках, используется эвристический анализатор.

Кроме того, можно сформировать список разрешенных адресов, на основании которого показ баннеров будет разрешен.

В ЭТОМ РАЗДЕЛЕ

Включение и выключение Анти-Баннера

После установки Kaspersky Internet Security Анти-Баннер выключен и не блокирует показ баннеров. Для блокирования баннеров нужно включить Анти-Баннер.

Для отображения всех баннеров нужно выключить Анти-Баннер. Для отображения некоторых баннеров нужно добавить их адреса в список разрешенных адресов баннеров (см. раздел «Формирование списков запрещенных и разрешенных адресов баннеров» на стр. 146).

Чтобы включить Анти-Баннер, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
3. В правой части окна установите флажок **Включить Анти-Баннер**.

Выбор методов проверки

Вы можете указать, какие из методов должен использовать Анти-Баннер для проверки адресов, с которых могут быть загружены баннеры. В дополнение к этим методам Анти-Баннер проверяет адреса баннеров на соответствие маскам из списков разрешенных и запрещенных адресов, если они используются.

Чтобы выбрать методы проверки адресов Анти-Баннером, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
3. В правой части окна в группе **Методы проверки** установите флажки напротив названий методов, которые нужно использовать.

Формирование списков запрещенных и разрешенных адресов баннеров

С помощью списков запрещенных и разрешенных адресов баннеров можно указать, с каких адресов загрузка и показ баннеров запрещены, а с каких – разрешены. Составьте список из масок запрещенных адресов, и Анти-Баннер заблокирует загрузку и показ баннеров с адресов, соответствующих этим маскам. Составьте список из масок разрешенных адресов, и Анти-Баннер будет загружать и показывать баннеры с адресов, соответствующих этим маскам.

При использовании браузеров Microsoft Internet Explorer, Mozilla Firefox и Google Chrome можно добавлять маски в список запрещенных адресов непосредственно из окна браузера.

Чтобы добавить маску в список запрещенных или разрешенных адресов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
3. В правой части окна в блоке **Дополнительно** установите флажок **Использовать список запрещенных веб-адресов** (или **Использовать список разрешенных веб-адресов**) и нажмите на кнопку **Настройка**, расположенную под флажком.

   Откроется окно **Запрещенные адреса** (или **Разрешенные адреса**).

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Маска адреса (URL)**.

5. Введите маску адреса баннера и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять, достаточно в списке снять флажок рядом с маской.

- *Чтобы добавить маску в список запрещенных адресов из окна браузера,*

  по правой клавише мыши на изображении в окне браузера откройте контекстное меню и выберите пункт **Добавить в Анти-Баннер**.

ЭКСПОРТ И ИМПОРТ СПИСКОВ АДРЕСОВ

Списки разрешенных и запрещенных адресов баннеров можно использовать многократно (например, переносить адреса баннеров в аналогичный список на другом компьютере с установленным Kaspersky Internet Security).

Последовательность действий при этом такова:

1. Выполните *экспорт* – скопируйте записи из списка в файл.

2. Перенесите сохраненный файл на другой компьютер (например, перешлите по почте или переместите на съемном носителе).

3. Выполните *импорт* – внесите записи из файла в аналогичный список на другом компьютере.

При экспорте списка вам будет предложено копировать только выбранный элемент списка или весь список целиком. При импорте можно добавить новые элементы в список или заменить существующий список импортируемым.

- *Чтобы экспортировать адреса баннеров из списка разрешенных или запрещенных адресов баннеров, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.

3. В правой части окна в блоке **Дополнительно** нажмите на кнопку **Настройка**, расположенную в строке с названием списка, адреса из которого следует копировать в файл.

4. В открывшемся окне **Разрешенные адреса** (или окне **Запрещенные адреса**) установите флажки напротив тех адресов, которые нужно включить в файл.

5. Нажмите на кнопку **Экспорт**.

   Откроется окно с предложением экспортировать только выделенные элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если в файл нужно включить только выбранные адреса;

   - нажмите на кнопку **Нет**, если в файл нужно включить список полностью.

6. В открывшемся окне введите имя для сохраняемого файла и подтвердите сохранение.

Чтобы импортировать адреса баннеров из файла в список разрешенных или запрещенных адресов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
3. В правой части окна в блоке **Дополнительно** нажмите на кнопку **Настройка**, расположенную в строке с названием списка, в который нужно добавить адреса из файла.
4. В открывшемся окне **Разрешенные адреса** (или окне **Запрещенные адреса**) нажмите на кнопку **Импорт**.

   Если список не пуст, откроется окно с предложением добавить импортируемые элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если нужно добавить к списку записи из файла;
   - нажмите на кнопку **Нет**, если нужно заменить существующие записи списком из файла.
5. В открывшемся окне выберите файл со списком записей, которые нужно импортировать.

Безопасная среда и безопасный браузер

Kaspersky Internet Security позволяет выполнить потенциально опасные действия изолированно от основной операционной системы. Для этого в Kaspersky Internet Security предусмотрены следующие возможности:

- запуск отдельной программы в безопасном режиме на основном рабочем столе (см. стр. 57);
- работа в безопасной среде (см. стр. 149);
- работа в безопасном браузере (см. стр. 152).

Изоляция от основной операционной системы обеспечивает дополнительную защиту вашего компьютера, так как реальные объекты операционной системы не подвергаются изменениям.

Подозрительные файлы, обнаруженные при работе в изолированном режиме, помещаются на карантин в обычном режиме. При восстановлении файлов из карантина файлы восстанавливаются в исходную папку. Если исходную папку найти не удается, то Kaspersky Internet Security предлагает указать место восстановления объекта в той среде (обычной или безопасной), в которой была запущена процедура восстановления.

На компьютерах под управлением Microsoft Windows XP x64 безопасная среда и безопасный браузер недоступны.

На компьютерах под управлением Microsoft Windows Vista x64 и Microsoft Windows 7 x64 функциональность некоторых программ при работе в безопасной среде ограничена. При запуске таких программ на экран будет выведено соответствующее сообщение, если включены уведомления (см. стр. 185) о событии **Функциональность программы в безопасной среде ограничена**. Кроме того, полностью недоступен безопасный рабочий стол для запуска программ.

В этом разделе

О БЕЗОПАСНОЙ СРЕДЕ

Безопасная среда представляет собой изолированную от основной операционной системы среду для запуска программ, в безопасности которых вы не уверены. При работе в безопасной среде реальные объекты операционной системы не подвергаются изменениям. Поэтому, даже если вы запускаете в безопасной среде зараженную программу, все ее действия будут ограничены виртуальной средой и не окажут воздействия на операционную систему.

В ЭТОМ РАЗДЕЛЕ

ЗАПУСК И ЗАВЕРШЕНИЕ РАБОТЫ В БЕЗОПАСНОЙ СРЕДЕ

Запустить безопасную среду можно следующими способами:

- из главного окна Kaspersky Internet Security (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- из контекстного меню Kaspersky Internet Security (см. раздел «Контекстное меню» на стр. 36);
- с помощью кнопки в интерфейсе Kaspersky Gadget, если для нее назначена функция запуска безопасного рабочего стола (см. раздел «Как использовать Kaspersky Gadget» на стр. 65);
- с помощью ярлыка на рабочем столе (см. раздел «Создание ярлыка безопасной среды на рабочем столе» на стр. 152).

Завершить работу в безопасной среде можно следующими способами:

- через меню **Пуск** операционной системы;
- из всплывающей панели (см. раздел «Использование всплывающей панели в безопасной среде» на стр. 151);
- с помощью комбинации клавиш **CTRL+ALT+SHIFT+K**.

Чтобы запустить безопасную среду из главного окна Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасная среда**.
3. В открывшемся окне нажмите на кнопку **Перейти в безопасную среду**.

Чтобы запустить безопасную среду из контекстного меню Kaspersky Internet Security,

по правой клавише мыши откройте контекстное меню для значка Kaspersky Internet Security в области уведомлений и выберите пункт **Безопасная среда**.

Чтобы запустить безопасную среду из Kaspersky Gadget,

нажмите на кнопку со значком **Безопасная среда** в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

Чтобы завершить работу в безопасной среде через меню Пуск,

в меню **Пуск** операционной системы выберите пункт **Безопасная среда – завершение работы**.

Чтобы завершить работу в безопасной среде из всплывающей панели, выполните следующие действия:

1. Наведите курсор мыши на верхнюю часть экрана.
2. Во всплывающей панели нажмите на кнопку .
3. В открывшемся окне выбора действия выберите пункт **Выключить**.

Автоматический запуск программ в безопасной среде

Вы можете сформировать список программ, которые будут запускаться автоматически при запуске безопасной среды.

Формирование списка автозапуска доступно только при работе в безопасной среде.

Чтобы сформировать список автозапуска для безопасной среды, выполните следующие действия:

1. В меню **Пуск** операционной системы выберите пункт **Программы** → **Автозапуск** → **Безопасная среда**.
2. По правой клавише мыши откройте контекстное меню и выберите в нем пункт **Открыть**.
3. В открывшуюся папку скопируйте ярлыки программ, которые нужно запускать автоматически при запуске безопасной среды.

Переключение между основным рабочим столом и безопасной средой

Вы можете переключаться на основной рабочий стол, не завершая работу в безопасной среде, а затем переключаться обратно. Переключение между безопасной средой и основным рабочим столом можно выполнить следующими способами:

- из главного окна Kaspersky Internet Security (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);
- из контекстного меню Kaspersky Internet Security (см. раздел «Контекстное меню» на стр. 36);
- из всплывающей панели (см. раздел «Использование всплывающей панели в безопасной среде» на стр. 151) (доступно только в безопасной среде);
- с помощью гаджета.

Чтобы переключиться на основной рабочий стол из главного окна Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасная среда**.
3. В открывшемся окне нажмите на кнопку **Основной рабочий стол**.

Чтобы переключиться на основной рабочий стол из контекстного меню Kaspersky Internet Security,

по правой клавише мыши откройте контекстное меню для значка Kaspersky Internet Security в области уведомлений и выберите в нем пункт **Вернуться на основной рабочий стол**.

Чтобы переключиться на основной рабочий стол из всплывающей панели, выполните следующие действия:

1. Наведите курсор мыши на верхнюю часть экрана.
2. Во всплывающей панели нажмите на кнопку  .

Использование всплывающей панели в безопасной среде

Всплывающая панель в безопасной среде позволяет выполнить следующие действия:

- завершить работу в безопасной среде (см. раздел «Запуск и завершение работы в безопасной среде» на стр. 149);
- переключиться на основной рабочий стол (см. раздел «Переключение между основным рабочим столом и безопасной средой» на стр. 150).

Чтобы отобразить всплывающую панель в безопасной среде,

наведите курсор мыши на верхнюю часть экрана.

Чтобы зафиксировать всплывающую панель, выполните следующие действия:

1. Наведите курсор мыши на верхнюю часть экрана.
2. Во всплывающей панели нажмите на кнопку  .

Очистка безопасной среды

В процессе очистки Kaspersky Internet Security удаляет данные, которые были сохранены при работе в безопасной среде, и восстанавливает измененные параметры.

Очистка производится из главного окна Kaspersky Internet Security на основном рабочем столе и только при завершенной работе в безопасной среде.

Перед очисткой убедитесь в том, что вся информация, которая может понадобиться вам для дальнейшей работы, сохранена в общую папку безопасной среды. В противном случае данные будут удалены без возможности восстановления.

Чтобы очистить данные безопасной среды, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасная среда**.
3. В открывшемся окне нажмите на кнопку  .
4. В открывшемся меню выберите пункт **Очистить безопасную среду**.

Создание ярлыка безопасной среды на рабочем столе

Для быстрого запуска безопасной среды вы можете создать ярлык на рабочем столе.

Чтобы создать на рабочем столе ярлык для запуска безопасной среды, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасная среда**.
3. В открывшемся окне нажмите на кнопку  .
4. В открывшемся меню выберите пункт **Создать ярлык на рабочем столе**.

О безопасном браузере

Безопасный браузер предназначен для доступа к системам интернет-банкинга и другим веб-сайтам, работающим с конфиденциальными данными.

Вы можете включить контроль доступа к сервисам интернет-банкинга (см. раздел «Контроль обращения к сервисам интернет-банкинга» на стр. 102) для автоматического определения банковских веб-сайтов, а также запускать безопасный браузер вручную (см. раздел «Защита конфиденциальных данных, вводимых на веб-сайтах» на стр. 56).

При работе в безопасном браузере введенные данные и сделанные изменения (например, сохраненные файлы cookies, журнал посещенных веб-сайтов) не попадают в операционную систему, а значит, не могут быть использованы злоумышленниками.

Браузер, работающий в режиме безопасного просмотра веб-сайтов, обозначен зеленой рамкой вокруг окна программы.

В этом разделе

Выбор браузера для безопасного просмотра веб-сайтов

В качестве безопасного браузера используется браузер, установленный по умолчанию. Вы можете выбрать другой браузер, установленный на вашем компьютере.

Kaspersky Internet Security позволяет использовать один из следующих браузеров:

- Microsoft Internet Explorer версии 6, 7, 8, 9;
- Mozilla Firefox версии 3.x, 4.x;
- Google Chrome версии 7.x, 8.x.

Чтобы выбрать браузер для безопасного просмотра веб-сайтов, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасный браузер**.
3. В открывшемся окне нажмите на кнопку  .
4. В открывшемся меню выберите пункт **Настроить**.
5. Откроется окно **Настройка безопасного браузера**.
6. В открывшемся окне в списке **Выберите браузер для безопасного просмотра веб-сайтов** выберите нужный браузер.
7. Нажмите на кнопку **Сохранить**.

ОЧИСТКА БЕЗОПАСНОГО БРАУЗЕРА

По умолчанию при работе в безопасном браузере Kaspersky Internet Security сохраняет изменения параметров браузера и данные, вводимые на веб-сайтах. Для защиты данных рекомендуется регулярно выполнять очистку безопасного браузера.

В процессе очистки Kaspersky Internet Security удаляет данные, которые были сохранены при работе в безопасном браузере, и восстанавливает измененные параметры.

Перед очисткой убедитесь в том, что вся информация, которая может понадобиться вам для дальнейшей работы, сохранена в общую папку безопасной среды. В противном случае данные будут удалены без возможности восстановления.

Вместо очистки вручную вы можете включить автоматическую очистку безопасного браузера. При этом Kaspersky Internet Security будет выполнять очистку автоматически по завершении работы в безопасном браузере, а очистка вручную будет недоступна.

Чтобы очистить данные безопасного браузера вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасный браузер**.
3. В открывшемся окне нажмите на кнопку  .
4. В открывшемся меню выберите пункт **Очистить безопасный браузер**.

Чтобы включить автоматическую очистку безопасного браузера, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Безопасный браузер**.
3. В открывшемся окне нажмите на кнопку  .
4. В открывшемся меню выберите пункт **Настроить**.
5. Откроется окно **Настройка безопасного браузера**.

6. В открывшемся окне в блоке **Дополнительные параметры** выберите вариант **Включить автоматическую очистку данных**.

7. Нажмите на кнопку **Сохранить**.

Создание ярлыка безопасного браузера на рабочем столе

Для быстрого запуска безопасного браузера вы можете создать ярлык на рабочем столе.

Чтобы создать на рабочем столе ярлык для запуска безопасного браузера, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Безопасный браузер**.

3. В открывшемся окне нажмите на кнопку  .

4. В открывшемся меню выберите пункт **Создать ярлык на рабочем столе**.

Использование общей папки

Общая папка служит для обмена файлами между основной операционной системой, безопасной средой и безопасным браузером. Все файлы, сохраненные в эту папку при работе в безопасной среде и безопасном браузере, будут доступны из основного рабочего стола.

Общая папка создается при установке программы. Расположение общей папки различается в зависимости от операционной системы:

- для операционной системы Microsoft Windows XP – C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\SandboxShared;

- для операционных систем Microsoft Windows Vista и Microsoft Windows 7 – C:\ProgramData\Kaspersky Lab\SandboxShared.

Расположение общей папки изменять нельзя.

Можно открыть общую папку двумя способами:

- из главного окна программы (см. раздел «Главное окно Kaspersky Internet Security» на стр. 37);

- с помощью ярлыка, обозначенного значком  . В зависимости от параметров программы, заданных разработчиками, ярлык может быть расположен в разделе Мой компьютер или Мои документы Проводника Microsoft Windows.

Чтобы открыть общую папку из главного окна Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Безопасная среда** или **Безопасный браузер**.

3. В открывшемся окне нажмите на кнопку **Открыть общую папку**.

Родительский контроль

Родительский контроль позволяет контролировать действия разных пользователей на компьютере и в сети. Понятие контроля включает возможность ограничивать доступ к интернет-ресурсам и программам, а также просматривать отчеты о действиях пользователей.

В настоящее время доступ к компьютеру и интернет-ресурсам получает все большее количество детей и подростков. При этом возникает проблема обеспечения безопасности, так как работа и общение в интернете связаны с рядом угроз. Назовем наиболее распространенные среди них:

- посещение веб-сайтов, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы);
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- загрузка файлов, зараженных вредоносными программами;
- чрезмерно длительное нахождение за компьютером, что может нанести вред здоровью;
- контакты с незнакомыми людьми, которые под видом сверстников могут получить личную информацию о пользователе (например, настоящее имя, адрес, время, когда никого нет дома).

Родительский контроль позволяет снизить риски, связанные с работой на компьютере и в интернете. Для этого используются следующие функции модуля:

- ограничение использования компьютера и интернета по времени;
- создание списков разрешенных и запрещенных для запуска приложений, а также временное ограничение запуска разрешенных приложений;
- создание списков разрешенных и запрещенных для доступа веб-сайтов, выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов;
- включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на веб-сайты с сомнительным содержимым не отображаются в результатах поиска);
- ограничение загрузки файлов из интернета;
- создание списков контактов, запрещенных или разрешенных для общения через интернет-пейджеры и в социальных сетях;
- просмотр текста переписки через интернет-пейджеры и в социальных сетях;
- запрет пересылки определенных персональных данных;
- поиск заданных ключевых слов в тексте переписки.

Все ограничения включаются по отдельности, что позволяет гибко настраивать Родительский контроль для разных пользователей. Для каждой учетной записи можно просматривать отчеты, в которых регистрируются события контролируемых категорий за выбранный период.

Для настройки и просмотра отчетов Родительского контроля требуется ввести имя и пароль. Если вы еще не задали пароль для управления Kaspersky Internet Security (см. раздел «Ограничение доступа к Kaspersky Internet Security» на стр. 69), при первом запуске Родительского контроля вам будет предложено это сделать.

В этом разделе

Настройка Родительского контроля пользователя

Вы можете включить и настроить Родительский контроль индивидуально для каждой учетной записи вашего компьютера, задав разные ограничения для разных пользователей, например в зависимости от возраста. Для пользователей, действия которых контролировать не нужно, вы можете отключить Родительский контроль.

В этом разделе

Включение и выключение контроля пользователя

Вы можете включать и выключать Родительский контроль отдельно для каждой учетной записи. Например, действия взрослого пользователя с учетной записью администратора компьютера контролировать не нужно – для него Родительский контроль можно отключить. Для остальных пользователей, действия которых нужно контролировать, Родительский контроль следует включить, а затем настроить (например, загрузив стандартные параметры настройки из шаблона).

Включить и выключить Родительский контроль можно следующими способами:

- из главного окна программы (см. стр. 37);
- из окна настройки Родительского контроля;
- из окна настройки программы (см. стр. 40);

- из контекстного меню значка программы (см. стр. 36).

Из контекстного меню можно включить / выключить Родительский контроль только для текущей учетной записи.

Чтобы включить Родительский контроль для учетной записи из главного окна, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Включить**.

Чтобы включить Родительский контроль для учетной записи из окна Родительский контроль, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.
5. В правой части окна установите флажок **Включить контроль пользователя**, если нужно включить Родительский контроль для учетной записи.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Чтобы включить Родительский контроль для учетной записи из окна настройки программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Родительский контроль**.
3. В правой части окна выберите учетную запись пользователя, для которого нужно включить Родительский контроль.
4. Над списком пользователей нажмите на кнопку **Контролировать**.

Чтобы включить Родительский контроль для текущей учетной записи из контекстного меню,

выберите пункт **Включить Родительский контроль** в контекстном меню значка программы.

Экспорт и импорт параметров Родительского контроля

Если вы настроили параметры Родительского контроля для учетной записи, их можно сохранить в отдельный файл (выполнить *экспорт*). В дальнейшем можно будет загрузить параметры из этого файла для быстрой настройки (выполнить *импорт*). Кроме того, вы можете применить параметры контроля другой учетной записи или использовать шаблон настройки (предустановленный набор правил для разных типов пользователей в зависимости от их возраста, опыта и других характеристик).

После применения набора параметров к учетной записи вы можете изменить их значения. Это не повлияет на значения в файле, из которого вы импортировали параметры.

- *Чтобы сохранить параметры контроля в файле, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Родительский контроль**.
  3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

     Откроется окно **Родительский контроль**.
  4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.
  5. В правой части окна в блоке **Управление параметрами** нажмите на кнопку **Сохранить** и сохраните файл настройки.

- *Чтобы загрузить параметры контроля из файла, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Родительский контроль**.
  3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Включить**.

     Откроется окно **Родительский контроль**.
  4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.
  5. В правой части окна в блоке **Управление параметрами** нажмите на кнопку **Загрузить**.
  6. В открывшемся окне **Загрузка параметров Родительского контроля** выберите вариант **Файл конфигурации** и укажите расположение файла.

- *Чтобы применить параметры другой учетной записи, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Родительский контроль**.
  3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Включить**.

     Откроется окно **Родительский контроль**.
  4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.
  5. В правой части окна в блоке **Управление параметрами** нажмите на кнопку **Загрузить**.
  6. В открывшемся окне **Загрузка параметров Родительского контроля** выберите вариант **Другой пользователь** и укажите учетную запись, параметры которой нужно использовать.

- *Чтобы использовать шаблон настройки, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Родительский контроль**.
  3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Включить**.

     Откроется окно **Родительский контроль**.

4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.

5. В правой части окна в блоке **Управление параметрами** нажмите на кнопку **Загрузить**.

6. В открывшемся окне **Загрузка параметров Родительского контроля** выберите вариант **Шаблон** и укажите шаблон, параметры которого нужно использовать.

ОТОБРАЖЕНИЕ УЧЕТНОЙ ЗАПИСИ В KASPERSKY INTERNET SECURITY

Вы можете выбрать, под каким псевдонимом и с каким изображением будет отображаться учетная запись пользователя в Kaspersky Internet Security.

Чтобы указать псевдоним и изображение для учетной записи, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Родительский контроль**.

3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.

4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Параметры учетной записи**.

5. В правой части окна укажите псевдоним пользователя в поле **Псевдоним**.

6. Выберите изображение для учетной записи пользователя в блоке **Изображение**.

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

ВРЕМЯ РАБОТЫ НА КОМПЬЮТЕРЕ

Вы можете настроить расписание доступа пользователя к компьютеру (дни недели и время в течение дня), а также ограничить суммарное время работы на компьютере в сутки.

Чтобы ограничить время работы на компьютере, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Родительский контроль**.

3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.

4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Использование компьютера**.

5. В правой части окна установите флажок **Включить контроль**.

6. Задайте временные ограничения на использование компьютера.

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

Время работы в интернете

Вы можете ограничить время пребывания пользователя в интернете. Для этого можно настроить расписание доступа в интернет (дни недели и время в течение дня, когда доступ разрешен или запрещен), а также ограничить суммарное время пребывания в интернете в сутки.

Чтобы ограничить время работы в интернете, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Использование интернета**.
5. В правой части окна установите флажок **Включить контроль**.
6. Задайте временные ограничения на использование интернета.
7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Запуск программ

Вы можете разрешить или запретить запуск определенных программ, а также ограничить запуск разрешенных программ по времени.

Чтобы ограничить запуск программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Запуск программ**.
5. В правой части окна установите флажок **Включить контроль**.
6. Создайте списки разрешенных и запрещенных для запуска программ, установите расписание использования разрешенных программ.
7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Посещение веб-сайтов

Вы можете установить ограничения на доступ к веб-сайтам в зависимости от их содержимого. Для этого можно выбрать категории веб-сайтов, доступ к которым должен быть заблокирован, и при необходимости сформировать список исключений.

Вы можете также включить режим *безопасного поиска*, который будет применяться во время работы пользователя с поисковыми системами. Некоторые поисковые системы стремятся защитить пользователей от неприемлемого содержимого веб-ресурсов. Для этого при индексации веб-сайтов анализируются ключевые слова и фразы, адреса и категории ресурсов. При включенном режиме безопасного поиска из результатов поиска

исключаются веб-сайты, относящиеся к нежелательным категориям (порнография, наркотики, насилие и другие материалы, не рекомендуемые для несовершеннолетних).

Родительский контроль позволяет включать режим безопасного поиска одновременно для следующих поисковых систем:

- Google;
- Bing.

Чтобы ограничить посещаемые веб-сайты, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Посещение веб-сайтов**.
5. В правой части окна установите флажок **Включить контроль**.
6. В блоке **Запрет веб-сайтов** выберите режим доступа к веб-сайтам:
   - Если вы хотите запретить доступ к веб-сайтам определенных категорий, выберите вариант **Запретить следующие категории веб-сайтов** и установите флажки для тех категорий веб-сайтов, доступ к которым нужно блокировать.

     При необходимости разрешить доступ к некоторым веб-сайтам, которые входят в категорию блокируемых, нажмите на кнопку **Исключения**, добавьте нужные веб-адреса в список исключений и назначьте им статус **Разрешено**.
   - Если вы хотите сформировать список веб-сайтов, доступ к которым разрешен, и запретить доступ ко всем остальным веб-сайтам, выберите вариант **Запретить посещение всех веб-сайтов, кроме разрешенных в списке исключений**, нажмите на кнопку **Исключения**, добавьте нужные веб-адреса в список исключений и назначьте им статус **Разрешено**.
   - Если вы хотите запретить доступ к определенным веб-сайтам, нажмите на кнопку **Исключения**, добавьте нужные веб-адреса в список исключений и назначьте им статус **Запрещено**.
7. Установите флажок **Включить безопасный поиск**, чтобы включить режим безопасного поиска.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

ЗАГРУЗКА ФАЙЛОВ ИЗ ИНТЕРНЕТА

Вы можете указать типы файлов, которые пользователю разрешено загружать из интернета.

Чтобы ограничить загрузку файлов из интернета, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Загрузка файлов**.

5. В правой части окна установите флажок **Включить контроль**.

6. Выберите категории файлов, загрузка которых разрешена.

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

Переписка через интернет-пейджеры

Контроль переписки через программы мгновенного обмена сообщениями (интернет-пейджеры) заключается в контроле контактов, с которыми разрешено общение, в блокировке переписки с контактами, с которыми запрещено общение, а также в контроле содержания переписки. Вы можете сформировать списки разрешенных и запрещенных контактов, задать ключевые слова, наличие которых будет проверяться в сообщениях, а также указать персональную информацию, пересылка которой будет запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные данному контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. В отчете можно просмотреть также текст переписки с каждым контактом.

Контроль переписки имеет следующие ограничения:

- Если интернет-пейджер был запущен до включения Родительского контроля, то контроль переписки не будет осуществляться до перезапуска интернет-пейджера.

- При использовании HTTP-прокси контроль переписки осуществляться не будет.

Текущая версия Родительского контроля обеспечивает контроль общения через следующие интернет-пейджеры:

- ICQ;
- QIP;
- Windows Live Messenger (MSN);
- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Агент;
- Psi;
- Miranda;
- Digsby;
- Pidgin;
- Qnext;
- SIM;
- Trilian;
- Xchat;
- Instantbird;
- RnQ;

- MSN;
- Jabber.

Некоторые интернет-пейджеры, например Yahoo! Messenger и Google Talk, используют защищенное соединение. Чтобы проверять трафик этих программ, требуется включить проверку защищенных соединений (см. стр. 125).

Чтобы ограничить переписку через интернет-пейджеры, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **IM-переписка**.
5. В правой части окна установите флажок **Включить контроль**.
6. Создайте список разрешенных и запрещенных контактов:
   a. В списке **Контакты** нажмите на кнопку **Добавить контакт**.
   b. В открывшемся окне **Новый контакт** выберите контакт из списка или добавьте его вручную.
7. Если вы хотите разрешить общение только с теми контактами, для которых в списке назначен статус **Разрешен**, установите флажок **Запретить переписку с контактами, не добавленными в список**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

ПЕРЕПИСКА В СОЦИАЛЬНЫХ СЕТЯХ

Контроль переписки через социальные сети заключается в контроле контактов, с которыми разрешено общение, в блокировке переписки с контактами, с которыми запрещено общение, а также в контроле содержания переписки. Вы можете сформировать списки разрешенных и запрещенных контактов, задать ключевые слова, наличие которых будет проверяться в сообщениях, а также указать персональную информацию, пересылка которой будет запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные данному контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. В отчете можно просмотреть также текст переписки с каждым контактом.

Некоторые социальные сети, например Twitter, используют защищенное соединение. Чтобы проверять трафик этих сетей, требуется включить проверку защищенных соединений (см. стр. 125).

Чтобы ограничить переписку через социальные сети, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Социальные сети**.

5. В правой части окна установите флажок **Включить контроль**.

6. Создайте список разрешенных и запрещенных контактов:

   Формирование списка недоступно, если Kaspersky Internet Security еще не собрал достаточно данных об использовании социальных сетей.

   a. В списке **Контакты** нажмите на кнопку **Добавить контакт**.

   b. В открывшемся окне **Новый контакт** выберите контакт из списка или добавьте его вручную.

7. Если вы хотите разрешить общение только с теми контактами, для которых в списке назначен статус **Разрешен**, установите флажок **Запретить переписку с контактами, не добавленными в список**.

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

Пересылка конфиденциальной информации

Вы можете запретить пересылку данных, содержащих персональную информацию, через интернет-пейджеры, социальные сети и при отправке данных на веб-сайты. Для этого требуется сформировать список записей, которые содержат конфиденциальные данные (например, домашний адрес, номер телефона).

Попытки пересылки данных из списка блокируются, а информация о заблокированных сообщениях выводится в отчет.

Чтобы запретить пересылку конфиденциальной информации, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Родительский контроль**.

3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.

4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Личные данные**.

5. В правой части окна установите флажок **Включить контроль**.

6. Сформируйте список личных данных, запрещенных к пересылке:

   a. В списке **Личные данные** нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Личные данные** введите информацию, пересылку которой вы хотите запретить.

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

Поиск ключевых слов

Вы можете отслеживать наличие определенных слов и словосочетаний в переписке пользователя через интернет-пейджеры, социальные сети и при отправке данных на веб-сайты.

Наличие в пересылаемых сообщениях ключевых слов, входящих в список, отражается в отчете.

Если отключен контроль переписки через интернет-пейджеры, социальные сети или контроль посещения веб-сайтов, поиск ключевых слов не производится.

- *Чтобы отслеживать наличие определенных слов в переписке и отправляемых данных, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Настройка**, а затем в левой части окна выберите раздел **Ключевые слова**.
5. В правой части окна установите флажок **Включить контроль**.
6. Сформируйте список ключевых слов, которые нужно отслеживать в переписке и отправляемых данных:
   a. В списке **Ключевые слова** нажмите на кнопку **Добавить**.
   b. В открывшемся окне **Ключевое слово** введите слова или фразы, которые нужно отслеживать.
7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

ПРОСМОТР ОТЧЕТОВ О ДЕЙСТВИЯХ ПОЛЬЗОВАТЕЛЯ

Вы можете просмотреть отчеты о действиях каждого пользователя, для которого настроен Родительский контроль, отдельно для каждой категории контролируемых событий.

- *Чтобы просмотреть отчет о действиях контролируемого пользователя, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Родительский контроль**.
3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку **Настройка**.

   Откроется окно **Родительский контроль**.
4. Выберите закладку **Отчеты**.
5. В левой части окна выберите раздел с названием категории контролируемых действий или содержимого (например **Использование интернета** или **Личные данные**).

   В правой части окна отобразится отчет о контролируемых действиях и содержимом.

ДОВЕРЕННАЯ ЗОНА

Доверенная зона – это перечень объектов, которые не контролируются программой в процессе работы. Иначе говоря, это набор исключений из защиты Kaspersky Internet Security.

Доверенная зона формируется на основе списка доверенных программ (см. раздел «Формирование списка доверенных программ» на стр. 166) и правил исключений (см. раздел «Создание правил исключений» на стр. 167) в зависимости от особенностей объектов, с которыми вы работаете, а также от программ, установленных на компьютере. Включение объектов в доверенную зону может потребоваться, например, если Kaspersky Internet Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект / программа абсолютно безвредны.

Например, если вы считаете объекты, используемые стандартной программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, добавьте программу Блокнот в список доверенных программ, чтобы исключить проверку объектов, используемых этим процессом.

Кроме того, некоторые действия, классифицируемые как опасные, могут быть безопасны в рамках функциональности ряда программ. Так, перехват текста, вводимого вами с клавиатуры, – штатное действие программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных.

При добавлении программы в список доверенных не будет контролироваться файловая и сетевая активность этой программы (в том числе и подозрительная), а также ее обращения к системному реестру. В то же время исполняемый файл и процесс доверенной программы по-прежнему будут проверяться на вирусы. Для полного исключения программы из проверки следует пользоваться правилами исключений.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Internet Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Internet Security и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В свою очередь, правила исключений доверенной зоны обеспечивают возможность работы с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным. Такие программы сами по себе не имеют вредоносных функций, но они могут быть использованы в качестве вспомогательного компонента вредоносной программы. К этой категории относятся программы удаленного администрирования, IRC-клиенты, FTP-серверы, различные утилиты для остановки процессов или сокрытия их работы, клавиатурные шпионы, программы вскрытия паролей, программы автоматического дозвона и другие. В результате работы Kaspersky Internet Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ можно настроить правила исключения из проверки.

Правило исключения – это набор условий, при которых объект не будет проверяться Kaspersky Internet Security. Во всех остальных случаях проверка данного объекта будет осуществляться всеми компонентами защиты в соответствии с установленными для них параметрами защиты.

Правила исключений доверенной зоны могут использоваться некоторыми компонентами программы (например, Файловым Антивирусом (см. раздел «Файловый Антивирус» на стр. 83), Почтовым Антивирусом (см. раздел «Почтовый Антивирус» на стр. 90), Веб-Антивирусом (см. раздел «Веб-Антивирус» на стр. 96)), а также при выполнении задач проверки на вирусы.

В этом разделе

Формирование списка доверенных программ

По умолчанию Kaspersky Internet Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. При добавлении программы в список доверенных Kaspersky Internet Security исключает ее из проверки.

Чтобы добавить программу в список доверенных, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Угрозы и исключения**.
3. В блоке **Исключения** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Доверенные программы** откройте меню выбора программы, нажав на кнопку **Добавить**.

5. В раскрывшемся меню выберите программу в списке **Программы** или выберите пункт **Обзор**, чтобы указать путь к исполняемому файлу нужной программы.

6. В открывшемся окне **Исключения для программы** установите флажки для тех видов активности программы, которые не нужно проверять.

СОЗДАНИЕ ПРАВИЛ ИСКЛЮЧЕНИЙ

Если вы используете в своей работе программы, классифицируемые Kaspersky Internet Security как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или вашим данным, рекомендуем вам настроить для них правила исключений.

Чтобы создать правило исключения, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Угрозы и исключения**.

3. В блоке **Исключения** нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Правила исключений** нажмите на кнопку **Добавить**.

5. В открывшемся окне **Правило исключения** задайте параметры правила исключения.

ПРОИЗВОДИТЕЛЬНОСТЬ И СОВМЕСТИМОСТЬ С ДРУГИМИ ПРОГРАММАМИ

Под производительностью Kaspersky Internet Security подразумевается спектр обнаруживаемых угроз, а также потребление энергии и ресурсов компьютера.

Kaspersky Internet Security позволяет выбирать различные категории угроз (см. раздел «Выбор категорий обнаруживаемых угроз» на стр. 168), которые программа будет обнаруживать в ходе работы.

При работе на портативных компьютерах потребление программами энергоресурсов имеет особое значение. Зачастую проверка компьютера на вирусы и обновление баз Kaspersky Internet Security требуют значительного количества ресурсов. Специальный режим работы Kaspersky Internet Security на портативном компьютере (см. раздел «Энергосбережение при работе от аккумулятора» на стр. 168) позволяет автоматически откладывать задачи проверки и обновления по расписанию при питании от аккумулятора и экономить тем самым его заряд, а режим Проверки во время простоя компьютера (см. раздел «Запуск задач в фоновом режиме» на стр. 169) позволяет запускать ресурсоемкие задачи в то время, когда компьютер не используется.

Потребление ресурсов компьютера Kaspersky Internet Security может сказываться на производительности других программ. Для решения проблем совместной работы при увеличении нагрузки на центральный процессор и дисковые подсистемы Kaspersky Internet Security может приостанавливать выполнение задач проверки и уступать ресурсы другим программам (см. раздел «Распределение ресурсов компьютера при проверке на вирусы» на стр. 169), работающим на компьютере.

В режиме игрового профиля (см. стр. 170) автоматически отключается показ уведомлений о работе Kaspersky Internet Security при запуске других программ в полноэкранном режиме.

Процедура расширенного лечения в случае активного заражения системы требует обязательной перезагрузки компьютера, что также может влиять на работу других программ. При необходимости вы можете отключить применение технологии лечения активного заражения (см. стр. 168), чтобы избежать нежелательной перезагрузки компьютера.

В этом разделе

Выбор категорий обнаруживаемых угроз

Угрозы, обнаруживаемые Kaspersky Internet Security, подразделяются на категории по различным признакам. Программа всегда ищет вирусы, троянские программы и вредоносные утилиты. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера можно расширить список обнаруживаемых угроз, включив контроль за действиями легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или вашим данным.

Чтобы выбрать категории обнаруживаемых угроз, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Угрозы и исключения**.
3. В правой части окна нажмите на кнопку **Настройка**, расположенную под списком **Включено обнаружение угроз следующих типов**.
4. В открывшемся окне **Угрозы** установите флажки для категорий угроз, которые необходимо обнаруживать.

Энергосбережение при работе от аккумулятора

В целях экономии заряда аккумулятора портативного компьютера вы можете отложить выполнение задач проверки на вирусы и обновления по расписанию. По мере необходимости можно обновлять Kaspersky Internet Security или запускать проверку на вирусы вручную.

Чтобы включить режим энергосбережения при работе от аккумулятора, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Энергосбережение**.
3. В правой части окна установите флажок **Не запускать задачи проверки по расписанию при работе от аккумулятора**.

Лечение активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. При обнаружении вредоносной активности в системе Kaspersky Internet Security предлагает использовать технологию лечения активного заражения, в результате которой угроза будет обезврежена и удалена с компьютера.

По окончании лечения активного заражения программа выполняет обязательную перезагрузку компьютера. После перезагрузки компьютера рекомендуется запускать полную проверку на вирусы (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 53).

- *Чтобы Kaspersky Internet Security применял технологию лечения активного заражения, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Совместимость**.
  3. Установите флажок **Применять технологию лечения активного заражения**.

РАСПРЕДЕЛЕНИЕ РЕСУРСОВ КОМПЬЮТЕРА ПРИ ПРОВЕРКЕ НА ВИРУСЫ

Выполнение задач проверки увеличивает нагрузку на центральный процессор и дисковые подсистемы, тем самым замедляя работу других программ. По умолчанию при возникновении такой ситуации Kaspersky Internet Security приостанавливает выполнение задач проверки и высвобождает ресурсы системы для программ пользователя.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы системы.

- *Чтобы Kaspersky Internet Security откладывал выполнение задач проверки при замедлении работы других программ, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Совместимость**.
  3. Установите флажок **Уступать ресурсы другим программам**.

ЗАПУСК ЗАДАЧ В ФОНОВОМ РЕЖИМЕ

Для оптимизации нагрузки на ресурсы компьютера Kaspersky Internet Security выполняет периодический поиск руткитов в фоновом режиме, а также запускает ресурсоемкие задачи во время простоя компьютера.

Периодический поиск руткитов выполняется в то время, когда вы работаете за компьютером. Поиск выполняется не более 5 минут и использует минимальные ресурсы компьютера.

К задачам, которые могут выполняться во время простоя компьютера, относятся следующие:

- автоматическое обновление антивирусных баз и программных модулей;
- проверка системной памяти, объектов автозапуска и системного раздела.

Задачи во время простоя компьютера запускаются, если компьютер был заблокирован пользователем, а также если в течение 5 минут на экране работает экранная заставка.

При работе компьютера от аккумулятора задачи во время простоя компьютера запускаться не будут.

После запуска задач в фоновом режиме процесс их выполнения отображается в Менеджере задач (см. раздел «Управление задачами проверки. Менеджер задач» на стр. 78).

В этом разделе

Поиск руткитов в фоновом режиме

По умолчанию Kaspersky Internet Security выполняет периодический поиск руткитов. При необходимости вы можете выключить поиск руткитов.

Чтобы выключить регулярный поиск руткитов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** подраздел **Основные параметры**.
3. В правой части окна снимите флажок **Выполнять регулярный поиск руткитов**.

Проверка во время простоя компьютера

Первым этапом запуска задач во время простоя компьютера является проверка актуальности баз и программных модулей. Если по результатам проверки требуется обновление, то запускается задача автоматического обновления. На втором этапе проверяется дата и статус последнего выполнения задачи во время простоя компьютера. Если задача во время простоя компьютера не запускалась, была выполнена в последний раз более 7 дней назад или прервана, то запускается задача проверки системной памяти, объектов автозапуска и системного реестра.

Проверка во время простоя компьютера выполняется с глубоким уровнем эвристического анализа, который повышает вероятность обнаружения скрытых угроз.

При возвращении пользователя к работе задача во время простоя компьютера автоматически прерывается. При этом сохраняется этап, на котором задача была прервана, и в следующий раз она возобновится с этого этапа.

Если выполнение задач во время простоя компьютера было прервано во время загрузки обновления, то в следующий раз обновление запустится с начала.

Чтобы выключить выполнение задач во время простоя компьютера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Проверка компьютера** подраздел **Основные параметры**.
3. В правой части окна снимите флажок **Выполнять проверку во время простоя компьютера**.

Работа в полноэкранном режиме. Игровой профиль

Использование некоторых программ (особенно компьютерных игр) в полноэкранном режиме плохо совместимо с некоторыми функциями Kaspersky Internet Security: например, в этом режиме неуместны окна уведомлений. Зачастую такие программы требуют также значительных системных ресурсов, поэтому выполнение некоторых задач Kaspersky Internet Security может привести к замедлению работы этих программ.

Чтобы вручную не отключать уведомления и не приостанавливать задачи каждый раз при переходе в полноэкранный режим, в Kaspersky Internet Security предусмотрена возможность временного изменения параметров с помощью игрового профиля. Когда игровой профиль используется, при переходе в полноэкранный режим автоматически изменяются параметры всех компонентов таким образом, чтобы обеспечить оптимальную

работу в этом режиме. При выходе из полноэкранного режима параметрам программы возвращаются значения, которые были установлены до перехода в полноэкранный режим.

Чтобы включить использование игрового профиля, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Игровой профиль**.
3. Установите флажок **Использовать Игровой профиль** и в блоке **Параметры профиля** ниже укажите необходимые параметры использования игрового профиля.

САМОЗАЩИТА KASPERSKY INTERNET SECURITY

Поскольку Kaspersky Internet Security обеспечивает безопасность компьютера от вредоносных программ, попадающее на компьютер вредоносное программное обеспечение пытается заблокировать работу Kaspersky Internet Security или удалить программу с компьютера.

Стабильность защиты вашего компьютера обеспечивают реализованные в Kaspersky Internet Security механизмы самозащиты и защиты от внешнего управления.

Самозащита Kaspersky Internet Security предотвращает изменение и удаление собственных файлов на диске, процессов в памяти, записей в системном реестре. Защита от внешнего управления позволяет блокировать все попытки удаленного управления сервисами программы.

Под управлением 64-разрядных операционных систем и Microsoft Windows Vista доступно только управление механизмом самозащиты Kaspersky Internet Security от изменения или удаления собственных файлов на диске, а также от изменения или удаления записей в системном реестре.

В ЭТОМ РАЗДЕЛЕ

ВКЛЮЧЕНИЕ И ВЫКЛЮЧЕНИЕ САМОЗАЩИТЫ

По умолчанию самозащита Kaspersky Internet Security включена. При необходимости вы можете выключить самозащиту.

Чтобы выключить самозащиту Kaspersky Internet Security, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Самозащита**.
3. В правой части окна снимите флажок **Включить самозащиту**.

Защита от внешнего управления

По умолчанию защита от внешнего управления включена. При необходимости вы можете отключить защиту.

Нередко возникают ситуации, когда при использовании защиты от внешнего управления возникает необходимость применить программы удаленного администрирования (например, RemoteAdmin). Для обеспечения работы этих программ необходимо добавить их в список доверенных программ (см. раздел «Доверенная зона» на стр. 165) и включить для них параметр **Не контролировать активность программы**.

Чтобы отключить защиту от внешнего управления, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Самозащита**.
3. В блоке **Внешнее управление** снимите флажок **Отключить возможность внешнего управления системной службой**.

Карантин и резервное хранилище

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Возможно зараженный файл может быть обнаружен и помещен на карантин в процессе проверки на вирусы, а также Файловым Антивирусом, Почтовым Антивирусом и Проактивной защитой.

Файлы помещаются на карантин в следующих случаях:

- Код файла похож на известную угрозу, но частично изменен или напоминает по структуре вредоносную программу, однако не зафиксирован в базе. В этом случае файл помещается на карантин в результате эвристического анализа в ходе работы Файлового Антивируса и Почтового Антивируса, а также в процессе проверки на вирусы. Механизм эвристического анализа редко приводит к ложным срабатываниям.
- Последовательность совершаемых объектом действий является подозрительной. В этом случае файл помещается на карантин в результате анализа его поведения компонентом Проактивная защита.

Файлы на карантине не представляют опасности. С течением времени появляется информация о новых угрозах и способах их лечения, и возможна ситуация, когда Kaspersky Internet Security сможет вылечить файл, находящийся на карантине.

Резервное хранилище предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

В этом разделе

ХРАНЕНИЕ ФАЙЛОВ НА КАРАНТИНЕ И В РЕЗЕРВНОМ ХРАНИЛИЩЕ

По умолчанию максимальный срок хранения объектов составляет 30 дней. По истечении этого времени объекты удаляются. Вы можете отменить ограничение по времени или изменить максимальный срок хранения объектов.

Кроме того, вы можете указать максимальный размер карантина и резервного хранилища. При достижении максимального размера содержимое карантина и резервного хранилища заменяется новыми объектами. По умолчанию ограничение максимального размера выключено.

Чтобы настроить максимальный срок хранения объектов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.
3. В правой части окна в блоке **Хранение объектов карантина и резервного хранилища** установите флажок **Хранить объекты не более** и укажите максимальный срок хранения объектов на карантине.

Чтобы настроить максимальный размер карантина и резервного хранилища, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.
3. В правой части окна в блоке **Хранение объектов карантина и резервного хранилища** установите флажок **Максимальный размер** и укажите максимальный размер карантина и резервного хранилища.

РАБОТА С ФАЙЛАМИ НА КАРАНТИНЕ

Карантин Kaspersky Internet Security позволяет выполнять следующие операции:

- помещать на карантин файлы, подозреваемые вами на присутствие вируса;
- проверять файлы на карантине, используя текущую версию баз Kaspersky Internet Security;
- восстанавливать файлы в исходные папки, откуда они были перенесены на карантин;
- удалять выбранные файлы из карантина;
- отправлять файлы на карантине на исследование в «Лабораторию Касперского».

Поместить файл на карантин можно следующими способами:

- с помощью кнопки **Поместить на карантин** в окне **Карантин**;
- с помощью контекстного меню файла.

Чтобы поместить файл на карантин из окна Карантин, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.
3. На закладке **Карантин** нажмите на кнопку **Поместить на карантин**.
4. В открывшемся окне выберите файл, который нужно поместить на карантин.

- *Чтобы поместить файл на карантин с помощью контекстного меню, выполните следующие действия:*

  1. Откройте окно Проводника Microsoft Windows и перейдите в папку с файлом, который нужно поместить на карантин.
  2. По правой клавише мыши откройте контекстное меню файла и выберите пункт **Поместить на карантин**.

- *Чтобы проверить файл на карантине, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Карантин**.
  3. На закладке **Карантин** выберите файл, который нужно проверить.
  4. Нажмите на кнопку **Проверить**.

- *Чтобы восстановить файл из карантина, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Карантин**.
  3. На закладке **Карантин** выберите файл, который нужно восстановить.
  4. Нажмите на кнопку **Восстановить**.

- *Чтобы удалить файл из карантина, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Карантин**.
  3. На закладке **Карантин** выберите файл, который нужно удалить.
  4. По правой клавише мыши откройте контекстное меню файла и выберите пункт **Удалить**.

- *Чтобы отправить объект из карантина на исследование в «Лабораторию Касперского», выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В нижней части окна выберите раздел **Карантин**.
  3. На закладке **Карантин** выберите файл, который нужно отправить на исследование.
  4. По правой клавише мыши откройте контекстное меню файла и выберите пункт **Отправить на исследование**.

Работа с объектами в резервном хранилище

Резервное хранилище Kaspersky Internet Security позволяет выполнять следующие операции:

- восстанавливать файлы в указанную или в исходные папки, где находился файл до его обработки Kaspersky Internet Security;
- удалять выбранные файлы или все файлы в резервном хранилище.

Чтобы восстановить файл из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.
3. На закладке **Хранилище** выберите файл, который нужно восстановить.
4. Нажмите на кнопку **Восстановить**.

Чтобы удалить файл из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.
3. На закладке **Хранилище** выберите файл, который нужно удалить.
4. По правой клавише мыши откройте контекстное меню файла и выберите пункт **Удалить**.

Чтобы удалить все файлы из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.
3. На закладке **Хранилище** нажмите на кнопку **Очистить хранилище**.

ПРОВЕРКА ФАЙЛОВ НА КАРАНТИНЕ ПОСЛЕ ОБНОВЛЕНИЯ

Если при проверке файла не удалось точно определить, какими вредоносными программами он заражен, такой файл помещается на карантин. Возможно, после обновления баз Kaspersky Internet Security сможет однозначно определить угрозу и обезвредить ее. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

Рекомендуем вам периодически просматривать файлы на карантине. В результате проверки их статус может измениться. Ряд файлов можно будет восстановить в прежнее расположение и продолжить работу с ними.

Чтобы включить проверку файлов на карантине после обновления, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Обновление** компонент **Параметры обновления**.
3. В блоке **Дополнительно** установите флажок **Проверять файлы на карантине после обновления**.

ИНСТРУМЕНТЫ ДЛЯ ДОПОЛНИТЕЛЬНОЙ ЗАЩИТЫ

Для решения специфических задач по обеспечению безопасности компьютера используются мастеры и инструменты, включенные в состав Kaspersky Internet Security:

- Мастер создания Kaspersky Rescue Disk – предназначен для создания образа диска и записи на съемный носитель программы Kaspersky Rescue Disk, которая позволяет восстановить работоспособность системы после вирусной атаки с помощью загрузки со съемных носителей. Kaspersky Rescue Disk применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения.

- Мастер устранения следов активности – предназначен для поиска и устранения следов активности пользователя в системе, а также параметров операционной системы, способствующих накоплению информации об активности пользователя.

- Мастер восстановления системы – предназначен для устранения повреждений системы и следов пребывания вредоносных объектов в системе.

- Мастер настройки браузера – предназначен для анализа и настройки параметров браузера Microsoft Internet Explorer с целью устранения его потенциальных уязвимостей.

Все проблемы, обнаруживаемые мастерами (кроме Мастера создания Kaspersky Rescue Disk), группируются в зависимости от опасности, которую они представляют для системы. Для каждой группы проблем специалисты «Лаборатории Касперского» предлагают набор действий, выполнение которых поможет устранить уязвимости и проблемные места в системе. Всего выделено три группы проблем и, соответственно, действий при их обнаружении:

- *Настоятельно рекомендуемые действия* помогут избавиться от проблем, представляющих серьезную угрозу безопасности. Рекомендуем вам своевременно выполнять все действия этой группы для устранения угрозы.

- *Рекомендуемые действия* направлены на устранение проблем, которые могут представлять потенциальную опасность. Действия этой группы также рекомендуется выполнять для обеспечения оптимальной защиты.

- *Дополнительные действия* предназначены для устранения неопасных в данный момент проблем, которые в будущем могут поставить безопасность компьютера под угрозу. Выполнение этих действий обеспечивает полноценную защиту вашего компьютера, но в некоторых случаях может привести к удалению пользовательских параметров (например, файлов cookie).

В этом разделе

Устранение следов активности

При работе на компьютере действия пользователя регистрируются в системе. При этом сохраняются данные о введенных пользователем поисковых запросах и посещенных им сайтах, о запуске программ и открытии и сохранении файлов, записи в системном журнале Microsoft Windows, временные файлы и многое другое.

Все эти источники информации об активности пользователя могут содержать конфиденциальные данные (в том числе пароли) и могут оказаться доступными для анализа злоумышленниками. В то же время пользователь зачастую не обладает достаточными знаниями для того, чтобы предотвратить хищение информации из этих источников.

В состав Kaspersky Internet Security входит Мастер устранения следов активности. Этот мастер производит поиск как следов активности пользователя в системе, так и параметров операционной системы, способствующих накоплению информации об этой активности.

Следует помнить о том, что накопление информации об активности пользователя в системе происходит постоянно. Запуск любого файла или открытие документа фиксируется в истории, системный журнал Microsoft Windows регистрирует множество событий, происходящих в системе. Это приводит к тому, что повторный запуск Мастера устранения следов активности может обнаружить следы активности, удаленные во время предыдущего запуска мастера. Некоторые файлы, например файл журнала Microsoft Windows, могут оказаться активно используемыми системой в момент их удаления мастером. Чтобы удалить эти файлы, мастер предложит перезагрузить систему. Однако в ходе перезагрузки такие файлы могут быть созданы заново, что приведет к их повторному обнаружению как следов активности.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы удалить следы активности пользователя в системе, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Инструменты**.
3. В открывшемся окне в блоке **Устранение следов активности** нажмите на кнопку **Выполнить**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Провести диагностику следов активности пользователя**, и нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Поиск следов активности

Мастер осуществляет поиск следов активности на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для устранения следов активности

По завершении поиска мастер сообщает о найденных следах активности и предлагаемых действиях для их устранения.

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение следов активности

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

После устранения следов активности мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Если вы хотите, чтобы устранение следов активности в дальнейшем выполнялось автоматически при завершении работы Kaspersky Internet Security, на завершающем шаге работы мастера установите флажок **Выполнять устранение следов активности при каждом завершении работы Kaspersky Internet Security**. Если вы планируете самостоятельно устранять следы активности с помощью мастера, не устанавливайте этот флажок.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Настройка браузера для безопасной работы

Браузер Microsoft Internet Explorer в некоторых случаях требует специального анализа и настройки, поскольку некоторые значения параметров, заданные пользователем или установленные по умолчанию, могут приводить к возникновению проблем в безопасности.

Приведем примеры объектов и параметров, используемых браузером и представляющих собой потенциальные угрозы безопасности:

- **Кеш работы Microsoft Internet Explorer**. В кеше хранятся данные, загруженные из интернета, что позволяет в дальнейшем не загружать их повторно. Это сокращает время загрузки веб-страниц и уменьшает интернет-трафик. Вместе с тем кеш содержит конфиденциальные данные и предоставляет возможность узнать, какие ресурсы посещал пользователь. Многие вредоносные объекты при сканировании диска сканируют также и кеш, в результате чего злоумышленники могут получить, например, почтовые адреса пользователей. Для усиления защиты рекомендуется очищать кеш после завершения работы браузера.

- **Отображение расширений для файлов известных форматов**. Для удобства редактирования имен файлов можно не отображать их расширения. Однако для пользователя иногда полезно видеть реальное расширение файла. В именах файлов многих вредоносных объектов используются сочетания символов, имитирующие дополнительное расширение перед реальным расширением (например, example.txt.com). Если реальное расширение файла не отображается, пользователь видит только часть названия файла с имитацией расширения и может принять вредоносный объект за безопасный файл. Для усиления защиты рекомендуется включать отображение расширений для файлов известных форматов.

- **Список доверенных сайтов**. Для корректной работы некоторых веб-сайтов их нужно добавлять в список доверенных. В то же время вредоносные объекты могут добавлять в такой список ссылки на веб-сайты, созданные злоумышленниками.

Настройка браузера для безопасной работы может привести к проблемам в отображении некоторых веб-сайтов (например, если они используют ActiveX-элементы). Решить проблему поможет включение подобных веб-сайтов в доверенную зону.

Анализ и настройка браузера выполняются Мастером настройки браузера. В ходе работы мастер проверяет, установлены ли последние обновления для браузера и не делают ли установленные значения параметров браузера систему уязвимой для действий злоумышленников. По окончании работы мастера формируется отчет, который может быть отправлен в «Лабораторию Касперского» для анализа.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Перед началом диагностики закройте все окна браузера Microsoft Internet Explorer.

Чтобы настроить браузер для безопасной работы, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Инструменты**.

3. В открывшемся окне в блоке **Настройка браузера** нажмите на кнопку **Выполнить**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Провести диагностику Microsoft Internet Explorer**, и нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Анализ параметров Microsoft Internet Explorer

Мастер анализирует параметров браузера Microsoft Internet Explorer. Поиск проблем в параметрах браузера может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для настройки браузера

По завершении поиска мастер сообщает о найденных проблемах и предлагаемых действиях для их устранения.

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Настройка браузера

Мастер выполняет действия, выбранные на предыдущем шаге. Настройка браузера может занять некоторое время. После выполнения настройки мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

ОТМЕНА ИЗМЕНЕНИЙ, ВЫПОЛНЕННЫХ МАСТЕРАМИ

Некоторые изменения, выполненные при запуске Мастера устранения следов активности (см. раздел «Устранение следов активности» на стр. 176), Мастера восстановления системы (см. раздел «Что делать, если вы подозреваете, что ваш компьютер заражен» на стр. 58), Мастера настройки браузера (см. раздел «Настройка браузера для безопасной работы» на стр. 178), можно отменить.

Чтобы отменить изменения, выполненные мастерами, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна выберите раздел **Инструменты**.

2. В правой части окна нажмите на кнопку **Выполнить** в блоке с названием мастера, для которого нужно отменить выполненные изменения:

   - **Устранение следов активности** – для отмены изменений, выполненных Мастером устранения следов активности;

- **Восстановление после заражения** – для отмены изменений, выполненных Мастером восстановления системы;
- **Настройка браузера** – для отмены изменений, выполненных Мастером настройки браузера.

Рассмотрим подробнее шаги мастеров при отмене изменений.

Шаг 1. Начало работы мастера

Выберите вариант **Отменить изменения** и нажмите на кнопку **Далее**.

Шаг 2. Поиск изменений

Мастер осуществляет поиск изменений, выполненных им ранее, для которых возможен откат. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор изменений для отката

По завершении поиска мастер сообщает о найденных изменениях.

Чтобы мастер отменил ранее выполненное действие, установите флажок слева от названия действия.

Выбрав действия, которые нужно отменить, нажмите на кнопку **Далее**.

Шаг 4. Отмена изменений

Мастер отменяет действия, выбранные на предыдущем шаге. После отмены изменений мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Отчеты

События, происходящие в ходе работы компонентов защиты или выполнения задач Kaspersky Internet Security, фиксируются в отчетах.

В этом разделе

ФОРМИРОВАНИЕ ОТЧЕТА ДЛЯ ВЫБРАННОГО КОМПОНЕНТА ЗАЩИТЫ

Вы можете получить подробный отчет о событиях, произошедших в ходе работы каждого компонента защиты или задачи Kaspersky Internet Security.

Для удобства работы с отчетами вы можете изменять представление данных на экране: группировать события по различным параметрам, выбирать отчетный период, сортировать события по каждой графе или по важности, а также скрывать графы таблицы.

- *Чтобы получить отчет для компонента защиты или задачи, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.
4. В левой части открывшегося окна **Подробный отчет** выберите компонент или задачу, для которой нужно сформировать отчет. При выборе пункта **Центр защиты** отчет будет сформирован для всех компонентов защиты.

ФИЛЬТРАЦИЯ ДАННЫХ

В отчетах Kaspersky Internet Security вы можете отфильтровать события по одному или нескольким значениям в графах таблицы, а также задать сложные условия фильтрации данных.

- *Чтобы отфильтровать события по значениям, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.
4. В правой части открывшегося окна **Подробный отчет** наведите курсор на верхний левый угол заголовка графы таблицы и по левой клавише мыши откройте меню фильтра.
5. В меню фильтра выберите значение, по которому нужно отфильтровать данные.
6. При необходимости повторите процедуру для другой графы таблицы.

- *Чтобы задать сложное условие фильтрации, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Отчеты** в верхней части окна откройте окно отчетов.
3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.
4. В правой части открывшегося окна **Подробный отчет** по правой клавише мыши откройте контекстное меню для нужной графы отчета и выберите в нем пункт **Фильтр**.
5. В открывшемся окне **Сложный фильтр** задайте условия фильтрации:
   a. В правой части окна задайте границу выборки.
   b. В левой части окна в раскрывающемся списке **Условие** выберите условие выборки (например, больше или меньше, равно или не равно значению, указанному в качестве границы выборки).

c. При необходимости добавьте второе условие, используя логические операции конъюнкции (логическое И) и дизъюнкции (логическое ИЛИ). Если вы хотите, чтобы выборка данных удовлетворяла обоим заданным условиям, выберите **И**. Если достаточно хотя бы одного условия, выберите **ИЛИ**.

Поиск событий

Вы можете выполнить поиск нужного события в отчете по ключевому слову через поисковую строку или с помощью специального окна поиска.

Чтобы найти событие с помощью поисковой строки, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.
4. В правой части открывшегося окна **Подробный отчет** введите ключевое слово в поисковой строке.

Чтобы найти событие с помощью окна поиска, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.
4. В правой части открывшегося окна **Подробный отчет** по правой клавише мыши откройте контекстное меню для заголовка нужной графы и выберите в нем пункт **Поиск**.
5. В открывшемся окне **Поиск** задайте критерии поиска:
   a. В поле **Строка** введите ключевое слово для поиска.
   b. В раскрывающемся списке **Графа** выберите название графы, в которой нужно искать заданное ключевое слово.
   c. При необходимости установите флажки для дополнительных параметров поиска.
6. Запустите поиск одним из следующих способов:
   - Если вы хотите искать следующее событие, совпадающее с заданными критериями поиска, после выделенного в списке, нажмите на кнопку **Искать дальше**.
   - Если вы хотите найти все события, совпадающие с заданными критериями поиска, нажмите на кнопку **Отметить все**.

Сохранение отчета в файл

Полученный отчет можно сохранить в текстовом файле.

Чтобы сохранить отчет в файле, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку **Подробный отчет**.

4. В открывшемся окне **Подробный отчет** сформируйте необходимый отчет и по ссылке **Сохранить** откройте окно для выбора расположения сохраняемого файла.

5. В открывшемся окне укажите папку, в которую следует сохранить файл отчета, и введите название файла.

ХРАНЕНИЕ ОТЧЕТОВ

По умолчанию максимальный срок хранения отчетов о событиях составляет 30 дней. По истечении этого времени данные удаляются. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

Кроме того, вы можете указать максимальный размер файла отчета. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера содержимое файла заменяется новыми записями. Вы можете отменить ограничение размера отчета или установить другое значение.

- *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Хранение отчетов** установите флажок **Хранить отчеты не более** и укажите максимальный срок хранения отчетов.

- *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Хранение отчетов** установите флажок **Максимальный размер файла** и укажите максимальный размер файла отчета.

ОЧИСТКА ОТЧЕТОВ

Вы можете очистить отчеты, данные которых вам больше не нужны.

- *Чтобы очистить отчеты, выполните следующие действия*:

1. Откройте окно настройки программы.

2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Очистка отчетов** нажмите на кнопку **Очистить**.

4. В открывшемся окне **Удаление информации из отчетов** установите флажки для тех отчетов, которые вы хотите очистить.

ЗАПИСЬ НЕКРИТИЧЕСКИХ СОБЫТИЙ В ОТЧЕТ

По умолчанию записи о некритических событиях, событиях реестра и файловой системы не добавляются в отчет. Вы можете включить запись таких событий в отчет.

Чтобы записывать некритические события в отчет, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Отчеты и хранилища**.
3. В правой части окна установите флажок **Включить запись некритических событий**.

Настройка уведомления о готовности отчета

Вы можете сформировать расписание, согласно которому Kaspersky Internet Security будет напоминать вам о готовности отчета.

Чтобы настроить напоминание о готовности отчета, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Отчеты**.
3. В открывшемся окне **Отчеты** нажмите на кнопку  .
4. В открывшемся окне **Уведомления** задайте параметры расписания.

Внешний вид программы. Управление активными элементами интерфейса

Kaspersky Internet Security позволяет настраивать параметры отображения текста на экране приветствия Microsoft Windows и активных элементов интерфейса (значка программы в области уведомлений, окон уведомлений и всплывающих сообщений).

В этом разделе

Полупрозрачность окон уведомлений

Чтобы включить полупрозрачность окон уведомлений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Вид**.
3. В блоке **Значок в панели задач** установите флажок **Использовать полупрозрачность окон уведомлений**.

АНИМАЦИЯ ЗНАЧКА ПРОГРАММЫ В ОБЛАСТИ УВЕДОМЛЕНИЙ

Анимация значка программы в области уведомлений отображается при выполнении обновления или проверки.

По умолчанию анимация значка программы в области уведомлений включена.

Чтобы выключить анимацию значка программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Вид**.
3. В блоке **Значок в панели задач** снимите флажок **Использовать анимацию значка при выполнении задач**.

ТЕКСТ НА ЭКРАНЕ ПРИВЕТСТВИЯ MICROSOFT WINDOWS

По умолчанию, если Kaspersky Internet Security включен и защищает ваш компьютер, при загрузке Microsoft Windows на экране приветствия отображается текст «Protected by Kaspersky Lab».

Текст «Protected by Kaspersky Lab» отображается только в операционной системе Microsoft Windows XP.

Чтобы выключить отображение текста при загрузке Microsoft Windows, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Вид**.
3. В блоке **Значок в панели задач** снимите флажок **Показывать «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows**.

УВЕДОМЛЕНИЯ

По умолчанию при возникновении событий в процессе работы Kaspersky Internet Security уведомляет вас об этом. Если от вас требуется выбор дальнейших действий, то на экран выводятся окна уведомлений (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 38). О событиях, не требующих выбора действий, программа уведомляет с помощью звукового оповещения, почтовых сообщений и всплывающих сообщений в области уведомлений панели задач (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 38).

В состав Kaspersky Internet Security включен новостной агент (на стр. 41), с помощью которого «Лаборатория Касперского» уведомляет вас о новостях. Если вы не хотите получать новости, вы можете выключить доставку новостей.

В ЭТОМ РАЗДЕЛЕ

Включение и выключение уведомлений

По умолчанию Kaspersky Internet Security уведомляет вас о значимых событиях, связанных с работой программы, различными способами (см. раздел «Настройка способа уведомления» на стр. 186). Вы можете отключить доставку уведомлений.

Вне зависимости от того, включена или выключена доставка уведомлений, информация о событиях, возникающих в ходе работы Kaspersky Internet Security, записывается в отчет о работе программы (см. стр. 180).

Когда вы выключаете доставку уведомлений, это не влияет на отображение окон уведомлений. Чтобы на экране отображалось минимальное количество окон уведомлений, используйте автоматический режим защиты (см. раздел «Выбор режима защиты» на стр. 70).

Чтобы выключить доставку уведомлений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Уведомления**.
3. В правой части окна снимите флажок **Уведомлять о событиях**.

Настройка способа уведомления

Программа уведомляет вас о событиях следующими способами:

- всплывающими сообщениями в области уведомлений панели задач;
- звуковым оповещением;
- сообщениями электронной почты.

Вы можете настроить способы доставки уведомлений индивидуально для каждого типа событий.

По умолчанию критические уведомления и уведомления о нарушениях в работе программы сопровождаются звуковым сигналом. В качестве звукового сопровождения используется звуковая схема Microsoft Windows. Вы можете изменить использующуюся схему или отключить звуковое оповещение.

Чтобы Kaspersky Internet Security мог уведомлять вас о событиях по почте, необходимо настроить параметры электронной почты для доставки уведомлений.

Чтобы выбрать способы доставки уведомлений для разных типов событий, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Уведомления**.
3. В правой части окна установите флажок **Уведомлять о событиях** и нажмите на кнопку **Настройка**, расположенную под флажком.
4. В открывшемся окне **Уведомления** установите флажки в соответствии с тем, какими способами вы хотите получать уведомления о различных событиях: по электронной почте, в виде всплывающего сообщения или с помощью звукового оповещения.

- *Чтобы настроить параметры электронной почты для доставки уведомлений, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Уведомления**.
  3. В правой части окна установите флажок **Отправлять почтовые сообщения о событиях** и нажмите на кнопку **Настройка**.
  4. В открывшемся окне **Настройка почтовых уведомлений** задайте параметры доставки уведомлений по электронной почте.

- *Чтобы настроить звуковую схему уведомлений, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Уведомления**.
  3. В правой части окна установите флажок **Включить звуковое сопровождение уведомлений**.

     Если вы хотите использовать звуковую схему Microsoft Windows для уведомления о событиях Kaspersky Internet Security, установите флажок **Использовать стандартную звуковую схему Windows Default**. Если этот флажок снят, для звукового сопровождения будет использоваться звуковая схема предыдущих версий Kaspersky Internet Security.

ВЫКЛЮЧЕНИЕ ДОСТАВКИ НОВОСТЕЙ

- *Чтобы выключить получение новостей из окна настройки программы, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Вид**.
  3. В правой части окна снимите флажок **Уведомлять о новостях**.

KASPERSKY SECURITY NETWORK

Чтобы повысить эффективность защиты вашего компьютера, Kaspersky Internet Security использует данные, полученные от пользователей во всем мире. Для сбора этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Internet Security на новые виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет «Лаборатории Касперского» оперативно собирать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний.

Кроме того, участие в Kaspersky Security Network обеспечивает вам доступ к данным о репутации программ и веб-сайтов.

При участии в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Internet Security на вашем компьютере, автоматически отправляется в «Лабораторию Касперского».

Сбор, обработка и хранение ваших персональных данных не производится.

Участие в Kaspersky Security Network добровольное. Решение об участии вы принимаете на этапе установки Kaspersky Internet Security, но можете изменить его в любой момент.

В этом разделе

Включение и выключение участия в Kaspersky Security Network

Чтобы участвовать в Kaspersky Security Network, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Обратная связь**.
3. В правой части окна установите флажок **Я согласен участвовать в Kaspersky Security Network**.

Проверка подключения к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- ваш компьютер не подключен к интернету;
- вы не участвуете в Kaspersky Security Network;
- ваша лицензия на использование Kaspersky Internet Security ограничена.

Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна нажмите на кнопку **Защита из облака**.
3. В левой части открывшегося окна отображается статус подключения к Kaspersky Security Network.

ПРОВЕРКА РАБОТЫ ПРОГРАММЫ

Этот раздел содержит сведения о том, как проверить работу программы – убедиться в том, что программа обнаруживает вирусы и их модификации и выполняет над ними действия.

В ЭТОМ РАЗДЕЛЕ

О ТЕСТОВОМ ФАЙЛЕ EICAR

Вы можете убедиться в том, что программа обнаруживает вирусы и выполняет лечение зараженных файлов, при помощи *тестового файла EICAR*. Тестовый файл EICAR разработан организацией European Institute for Computer Antivirus Research (EICAR) для проверки работы антивирусных программ.

Тестовый файл EICAR не является вирусом. В состав тестового файла EICAR не входит программный код, который может нанести ущерб вашему компьютеру. Тем не менее большинство антивирусных программ идентифицируют тестовый файл EICAR как вирус.

Тестовый файл EICAR не предназначен для проверки работы эвристического анализатора и поиска вредоносных программ на системном уровне (руткитов).

Не используйте для проверки работоспособности антивирусных программ настоящие вирусы! Это может нанести ущерб вашему компьютеру.

Не забудьте возобновить антивирусную защиту интернет-трафика и антивирусную защиту файлов после завершения работы с тестовым файлом EICAR.

ПРОВЕРКА РАБОТЫ ПРОГРАММЫ С ИСПОЛЬЗОВАНИЕМ ТЕСТОВОГО ФАЙЛА EICAR

Вы можете проверить с помощью тестового файла EICAR, как работает защита интернет-трафика, антивирусная защита файлов и проверка вашего компьютера.

Не забудьте возобновить антивирусную защиту интернет-трафика и антивирусную защиту файлов после завершения работы с тестовым файлом EICAR.

Чтобы проверить защиту интернет-трафика с использованием тестового файла EICAR, выполните следующие действия:

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

2. Попытайтесь сохранить тестовый файл EICAR в любой папке на вашем компьютере.

   Kaspersky Internet Security сообщит вам об обнаружении угрозы по запрашиваемому URL-адресу и заблокирует сохранение объекта на компьютере.

3. Если требуется, используйте виды тестового файла EICAR (см. раздел «О видах тестового файла EICAR» на стр. 191).

Чтобы проверить антивирусную защиту файлов с использованием тестового файла EICAR или его вида, выполните следующие действия:

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов на вашем компьютере.

   Когда защита приостановлена, не рекомендуется подключать компьютер к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб вашему компьютеру.

2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

3. Сохраните тестовый файл EICAR в любой папке на вашем компьютере.

4. Добавьте в начало строки тестового файла EICAR один из префиксов (см. раздел «О видах тестового файла EICAR» на стр. 191).

   Для этого вы можете использовать любой текстовый или гипертекстовый редактор, например, Блокнот. Чтобы запустить Блокнот, выберите **Пуск** → **Программы** → **Стандартные** → **Блокнот**.

5. Сохраните полученный файл под именем, соответствующим виду файла EICAR: например, добавив префикс DELE-, сохраните полученный файл под именем eicar_dele.com.

6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов на вашем компьютере.

7. Попробуйте запустить сохраненный файл.

   Kaspersky Internet Security сообщит вам об обнаружении угрозы на жестком диске вашего компьютера и выполнит над ней действие, настроенное в параметрах антивирусной защиты файлов.

Чтобы проверить, как работает поиск вирусов, с использованием тестового файла EICAR или его вида, выполните следующие действия:

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов на вашем компьютере.

   Когда защита приостановлена, не рекомендуется подключать компьютер к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб вашему компьютеру.

2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

3. Добавьте в начало строки тестового файла EICAR один из префиксов (см. раздел «О видах тестового файла EICAR» на стр. 191).

   Для этого вы можете использовать любой текстовый или гипертекстовый редактор, например, Блокнот. Чтобы запустить Блокнот, выберите **Пуск** → **Программы** → **Стандартные** → **Блокнот**.

4. Сохраните полученный файл под именем, соответствующим виду тестового файла EICAR: например, добавив префикс DELE-, сохраните полученный файл под именем eicar_dele.com.

5. Запустите проверку сохраненного файла.

   Kaspersky Internet Security сообщит вам об обнаружении угрозы на жестком диске вашего компьютера и выполнит над ней действие, настроенное в параметрах проверки компьютера.

6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов на вашем компьютере.

О видах тестового файла EICAR

Вы можете проверить функции программы, создав разные виды тестового файла EICAR. Программа обнаруживает тестовый файл EICAR (его вид) и присваивает ему статус в зависимости от результатов проверки. Программа выполняет над тестовым файлом EICAR те действия, которые настроены в параметрах компонента, обнаружившего тестовый файл EICAR.

В первой графе таблицы (см. таблицу ниже) приведены префиксы, которые вы можете использовать для создания видов тестового файла EICAR. Во второй графе перечислены все возможные значения статуса, присваиваемого файлу по результатам проверки программой. Третья графа содержит информацию об обработке программой файлов с указанным статусом.

Таблица 2. Виды тестового файла EICAR

Префикс	Статус файла	Информация об обработке файла
Префикс отсутствует, стандартный тестовый вирус.	**Зараженный**. Файл содержит код известного вируса. Лечение файла невозможно.	Программа идентифицирует этот файл, как содержащий вирус, который невозможно вылечить. При попытке лечения файла применяется действие, установленное для зараженных файлов. По умолчанию программа выводит на экран уведомление о том, что лечение зараженного файла невозможно.
CURE-	**Зараженный**. Файл содержит код известного вируса. Лечение файла возможно.	Файл содержит вирус, который может быть вылечен или удален. Программа выполняет лечение файла, при этом текст тела вируса изменяется на CURE. Программа выводит на экран уведомление об обнаружении зараженного файла.
DELE-	**Зараженный**. Файл содержит код известного вируса. Лечение файла невозможно.	Программа идентифицирует этот файл как вирус, не подлежащий лечению, и удаляет его. Программа выводит на экран уведомление об удалении зараженного файла.
WARN-	**Возможно зараженный**. Файл содержит код неизвестного вируса. Лечение файла невозможно.	Файл признан возможно зараженным. Программа выполняет над файлом действие, установленное для возможно зараженных файлов. По умолчанию программа выводит на экран уведомление об обнаружении возможно зараженного файла.
SUSP-	**Возможно зараженный.** Файл содержит модифицированный код известного вируса. Лечение файла невозможно.	Программа обнаружила частичное совпадение участка кода файла с участком кода известного вируса. На момент обнаружения возможно зараженного файла базы программы не содержат описания полного кода этого вируса. Программа выполняет над файлом действие, установленное для возможно зараженных файлов. По умолчанию программа выводит на экран уведомление об обнаружении возможно зараженного файла.

Префикс	Статус файла	Информация об обработке файла
CORR-	**Поврежденный**.	Программа не проверяет файл этого типа, поскольку его структура повреждена (например, неверный формат файла). Информацию о том, что файл был обработан, вы можете найти в отчете о работе программы.
ERRO-	**Ошибка проверки**.	При проверке файла возникла ошибка. Программа не смогла получить доступ к файлу: нарушена целостность файла (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется файл на сетевом диске). Информацию о том, что файл был обработан, вы можете найти в отчете о работе программы.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит сведения о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

В ЭТОМ РАЗДЕЛЕ

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. 14), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы. Если компьютер заражен, специалисты Службы технической поддержки помогут устранить последствия работы вредоносных программ.

Прежде чем обращаться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или международной Службы технической поддержки.
- Отправить запрос из Личного кабинета на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Для получения технической поддержки вы должны быть зарегистрированным пользователем коммерческой версии Kaspersky Internet Security. Техническая поддержка пользователей пробных версий программы не осуществляется.

Использование файла трассировки и скрипта AVZ

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на

наличие вредоносного кода, проверять систему на наличие вредоносного кода, лечить / удалять зараженные файлы и создавать отчеты о результатах проверки системы.

Создание отчета о состоянии системы

Чтобы создать отчет о состоянии системы, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** нажмите на кнопку **Создать отчет о состоянии системы**.

Отчет о состоянии системы формируется в форматах HTML и XML и сохраняется в архиве sysinfo.zip. По окончании процесса сбора информации о системе вы можете просмотреть отчет.

Чтобы просмотреть отчет, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** нажмите на кнопку **Просмотр**.
4. Откройте архив sysinfo.zip, содержащий файлы отчета.

Создание файла трассировки

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** в блоке **Трассировка** выберите уровень трассировки в раскрывающемся списке.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. При отсутствии указаний Службы технической поддержки рекомендуется устанавливать уровень трассировки **500**.
4. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.
5. Воспроизведите ситуацию, в которой у вас возникает проблема.
6. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

Вы можете перейти к загрузке результатов трассировки (см. раздел «Отправка файлов данных» на стр. 195) на сервер «Лаборатории Касперского».

Отправка файлов данных

После создания файлов трассировки и отчета о состоянии системы их необходимо отправить специалистам Службы технической поддержки «Лаборатории Касперского».

Чтобы загрузить файлы данных на сервер Службы технической поддержки, вам понадобится номер запроса. Этот номер доступен в вашем Личном кабинете на веб-сайте Службы технической поддержки при наличии активного запроса.

Чтобы загрузить файлы данных на сервер Службы технической поддержки, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

   Откроется окно **Загрузка информации для поддержки на сервер**.
4. Установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

   Откроется окно **Номер запроса**.
5. Укажите номер, присвоенный вашему запросу при обращении в Службу технической поддержки через Личный кабинет, и нажмите на кнопку **ОК**.

Выбранные файлы данных будут упакованы и отправлены на сервер Службы технической поддержки.

Если связаться со Службой технической поддержки по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их из Личного кабинета.

Чтобы сохранить файлы данных на диске, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

   Откроется окно **Загрузка информации для поддержки на сервер**.
4. Установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

   Откроется окно **Номер запроса**.
5. Нажмите на кнопку **Отмена** и в открывшемся окне подтвердите сохранение файлов на диске, нажав на кнопку **Да**.

   Откроется окно сохранения архива.
6. Задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через Личный кабинет.

Выполнение скрипта AVZ

Не рекомендуется вносить изменения в текст скрипта, присланного вам специалистами «Лаборатории Касперского». В случае возникновения проблем в ходе выполнения скрипта обращайтесь в Службу технической поддержки (см. раздел «Способы получения технической поддержки» на стр. 193).

Чтобы выполнить скрипт AVZ, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка** и перейдите в нем по ссылке **Трассировки**.
3. В открывшемся окне **Трассировки** нажмите на кнопку **Выполнить скрипт AVZ**.

В случае успешного выполнения скрипта работа мастера завершается. Если во время выполнения скрипта возникнет сбой, мастер выведет на экран соответствующее сообщение.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или интернациональной технической поддержки (http://support.kaspersky.ru/support/support_local).

Перед обращением в Службу технической поддержки вам требуется собрать информацию (http://support.kaspersky.ru/support/details) о компьютере и установленных на нем антивирусных программах. Это позволит нашим специалистам быстрее помочь вам.

Получение технической поддержки через Личный кабинет

Личный кабинет – это ваш персональный раздел https://my.kaspersky.ru на сайте Службы технической поддержки.

Для доступа к Личному кабинету вам требуется зарегистрироваться на странице регистрации (https://my.kaspersky.com/ru/registration). Вам нужно указать адрес электронной почты и пароль для доступа в Личный кабинет.

В Личном кабинете вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Вирусную лабораторию;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших запросов в Службу технической поддержки;
- получать копию файла ключа в случае, если файл ключа был утерян или удален.

Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском, немецком, французском или испанском языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса;
- номер клиента и пароль;
- электронный адрес.

Специалист Службы технической поддержки направляет ответ на ваш вопрос в ваш Личный кабинет и по адресу электронной почты, который вы указали в электронном запросе.

Электронный запрос в Вирусную лабораторию

Некоторые запросы требуется направлять не в Службу технической поддержки, а в Вирусную лабораторию.

Вы можете направлять в Вирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Kaspersky Internet Security не обнаруживает его в качестве зараженного.

  Специалисты Вирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.

- *Ложное срабатывание антивируса* – Kaspersky Internet Security определяет файл как содержащий вирус, но вы уверены, что файл не является вирусом.

- *Запрос на описание вредоносной программы* – вы хотите получить описание вируса, обнаруженного Kaspersky Internet Security, на основе названия этого вируса.

Вы также можете направлять запросы в Вирусную лабораторию со страницы с формой запроса (http://support.kaspersky.ru/virlab/helpdesk.html), не регистрируясь в Личном кабинете. При этом вам не требуется указывать код активации программы.

ПРИЛОЖЕНИЯ

Этот раздел содержит информацию, которая дополняет основной текст документа.

В ЭТОМ РАЗДЕЛЕ

РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Kaspersky Internet Security с помощью командной строки. При этом предусмотрена возможность выполнения следующих операций:

- активация программы;
- запуск и остановка программы;
- запуск и остановка работы компонентов программы;
- запуск и остановка задач;
- получение информации о текущем статусе компонентов и задач и их статистики;
- запуск и остановка выполнения задач проверки на вирусы;
- проверка выбранных объектов;
- обновление баз и программных модулей, откат обновления;
- экспорт и импорт параметров защиты;
- вызов справки по синтаксису командной строки в целом и отдельных команд.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Обращаться к программе через командную строку следует из каталога установки продукта либо с указанием полного пути к avp.com.

Перечень команд, используемых для управления программой и ее компонентами, приведен в таблице ниже.

START	Запуск компонента или задачи.
STOP	Остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс Kaspersky Internet Security).
STATUS	Вывод на экран текущего статуса компонента или задачи.
STATISTICS	Вывод на экран статистики работы компонента или задачи.
HELP	Вывод на экран списка команд, а также информации о синтаксисе команды.

SCAN	Проверка объектов на присутствие вирусов.
UPDATE	Запуск обновления программы.
ROLLBACK	Откат последнего произведенного обновления Kaspersky Internet Security (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
EXIT	Завершение работы с программой (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
IMPORT	Импорт параметров защиты Kaspersky Internet Security (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
EXPORT	Экспорт параметров защиты программы.

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента программы.

В этом разделе

Активация программы

Активировать Kaspersky Internet Security можно с помощью файла ключа.

Синтаксис команды:

```
avp.com ADDKEY <имя_файла>
```

Описание параметров выполнения команды приведено в таблице ниже.

<имя_файла>	Имя файла ключа к программе с расширением key.

Пример:

```
avp.com ADDKEY 1AA111A1.key
```

Запуск программы

Синтаксис команды:

```
avp.com
```

Остановка программы

Синтаксис команды:

```
avp.com EXIT /password=<ваш_пароль>
```

Описание параметров приведено в таблице ниже.

<ваш_пароль>	Пароль к программе, заданный в интерфейсе.

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Управление компонентами и задачами программы

Синтаксис команды:

```
avp.com <команда> <профайл|имя_задачи> [/R[A]:<файл_отчета>]
avp.com STOP <профайл|имя_задачи> /password=<ваш_пароль> [/R[A]:<файл_отчета>]
```

Описание команд и параметров приведено в таблице ниже.

<команда>	Управление компонентами и задачами Kaspersky Internet Security из командной строки выполняется с помощью следующего набора команд: START – запуск компонента защиты или задачи. STOP – остановка работы компонента защиты или задачи. STATUS – вывод на экран текущего статуса компонента защиты или задачи. STATISTICS – вывод на экран статистики по работе компонента защиты или задачи. Обратите внимание, что без ввода пароля команда STOP выполняться не будет.
<профайл|имя_задачи>	В качестве значений для параметра **<профайл>** вы можете указать любой из компонентов защиты Kaspersky Internet Security, а также модули, входящие в состав компонентов, сформированные задачи проверки по требованию или обновления (используемые программой стандартные значения приводятся в таблице ниже). В качестве значений для параметра **<имя_задачи>** может быть указано имя любой сформированной пользователем задачи проверки по требованию либо обновления.
<ваш_пароль>	Пароль к программе, заданный в интерфейсе.
/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

В качестве параметра **<профайл>** указывается одно из значений, приведенных в следующей таблице.

RTP	Все компоненты защиты. Команда **avp.com START RTP** запускает все компоненты защиты, если защита была полностью отключена. В случае если компонент был выключен командой **STOP** командной строки, он не будет запущен командой **avp.com START RTP**. Для этого необходимо выполнить команду **avp.com START <профайл>**, где для параметра **<профайл>** используется значение для конкретного компонента защиты, например, **avp.com START FM**.
FW	Сетевой экран.
HIPS	Контроль программ.
pdm	Проактивная защита.
FM	Файловый Антивирус.
EM	Почтовый Антивирус.
WM	Веб-Антивирус. Значения для подкомпонентов Веб-Антивируса: **httpscan (HTTP)** – проверка HTTP-трафика; **sc** – проверка скриптов.
IM	IM-Антивирус.
AB	Анти-Баннер.
AS	Анти-Спам.
PC	Родительский контроль.
AP	Анти-Фишинг.
ids	Защита от сетевых атак.
Updater	Обновление.
Rollback	Откат последнего обновления.
Scan_My_Computer	Проверка компьютера.
Scan_Objects	Проверка объектов.
Scan_Quarantine	Проверка карантина.
Scan_Startup (STARTUP)	Проверка объектов автозапуска.
Scan_Vulnerabilities (SECURITY)	Поиск уязвимостей.

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе программы.

Примеры:

- *Чтобы включить Файловый Антивирус, введите команду:*

```
avp.com START FM
```

- *Чтобы остановить проверку компьютера, введите команду:*

```
avp.com STOP Scan_My_Computer /password=<ваш_пароль>
```

Проверка на вирусы

Командная строка запуска проверки некоторой области на присутствие вирусов, а также запуска обработки вредоносных объектов имеет следующий общий вид:

```
avp.com SCAN [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>]
[<конфигурационный файл>] [<параметры отчета>] [<дополнительные параметры>]
```

Для проверки объектов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки. При этом задача будет выполнена с параметрами, установленными в интерфейсе Kaspersky Internet Security.

Описание параметров приведено в таблице ниже.

<объект проверки> – параметр задает перечень объектов, которые будут проверены на присутствие вредоносного кода. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
<files>	Список путей к файлам и папкам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элементов списка – пробел. Замечания: • если имя объекта содержит пробел, оно должно быть заключено в кавычки; • если указан конкретный каталог, проверяются все содержащиеся в нем файлы.
/MEMORY	Объекты оперативной памяти.
/STARTUP	Объекты автозапуска.
/MAIL	Почтовые ящики.
/REMDRIVES	Все съемные диски.
/FIXDRIVES	Все локальные диски.
/NETDRIVES	Все сетевые диски.
/QUARANTINE	Объекты на карантине.
/ALL	Полная проверка компьютера.

/@:<filelist.lst>	Путь к файлу со списком объектов и каталогов, включаемых в проверку. Допускается ввод абсолютного или относительного пути к файлу со списком. Путь указывается без кавычек, даже если в нем содержится символ пробела. Файл со списком объектов должен иметь текстовый формат. Каждый объект проверки необходимо указывать с новой строки. Рекомендуется указывать в файле абсолютные пути к объектам проверки. При указании относительного пути указывается путь относительно исполняемого файла программы, а не относительно файла со списком проверяемых объектов.
<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i8**. Если вы работаете в автоматическом режиме, то Kaspersky Internet Security будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов. Действие, соответствующее значению параметра **<действие>**, будет игнорироваться.	
/i0	Не совершать над объектом никаких действий, фиксировать информацию о нем в отчете.
/i1	Лечить зараженные объекты; если лечение невозможно – пропустить.
/i2	Лечить зараженные объекты; если лечение невозможно – удалять; не удалять зараженные объекты из контейнеров (составных объектов); удалять контейнеры с исполняемым заголовком (sfx-архивы).
/i3	Лечить зараженные объекты; если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i4	Удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i8	Запрашивать действие у пользователя при обнаружении зараженного объекта.
/i9	Запрашивать действие у пользователя по окончании проверки.
<типы файлов> – параметр определяет типы файлов, которые будут подвергаться антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому.	
/fe	Проверять только заражаемые файлы по расширению.
/fi	Проверять только заражаемые файлы по содержимому.
/fa	Проверять все файлы.
<исключения> – параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
-e:a	Не проверять архивы.
-e:b	Не проверять почтовые базы.
-e:m	Не проверять почтовые сообщения в формате plain text.
-e:<filemask>	Не проверять объекты по маске.
-e:<seconds>	Пропускать объекты, которые проверяются дольше указанного параметром **<seconds>** времени.
-es:<size>	Пропускать объекты, размер которых (в мегабайтах) превышает значение, заданное параметром **<size>**. Параметр применим только к составным файлам (например, архивам).

<конфигурационный файл> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при проверке. Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для антивирусной проверки. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.	
/C:<имя_файла>	Использовать значения параметров, заданные в конфигурационном файле **<имя_файла>**.
<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.	
/R:<файл_отчета>	Записывать в указанный файл отчета только важные события.
/RA:<файл_отчета>	Записывать в указанный файл отчета все события.
<дополнительные параметры> – параметр, определяющий использование технологий антивирусной проверки.	
/iChecker=<on|off>	Включить / отключить использование технологии iChecker.
/iSwift=<on|off>	Включить / отключить использование технологии iSwift.

Примеры:

- *Запустить проверку оперативной памяти, объектов автозапуска, почтовых ящиков, а также каталогов My Documents, Program Files и файла test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_settings.txt. По результатам проверки сформировать отчет, в котором зафиксировать все события:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Пример конфигурационного файла:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Обновление программы

Команда для обновления модулей Kaspersky Internet Security и программных баз имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>] [/R[A]:<файл_отчета>] [/C:<имя_файла>]
```

Описание параметров приведено в таблице ниже.

<источник_обновлений>	HTTP-, FTP-сервер или сетевой каталог для загрузки обновлений. В качестве значения для данного параметра может быть указан полный путь к источнику обновлений либо URL-адрес. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.
/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран; отображаются все события.

/C:<имя_файла>	Путь к конфигурационному файлу, содержащему параметры работы Kaspersky Internet Security при обновлении. Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для обновления программы. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения параметров, установленные в интерфейсе программы.

Примеры:

- *Обновить базы программы, зафиксировав все события в отчете:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Обновить модули Kaspersky Internet Security, используя параметры конфигурационного файла updateapp.ini:*

```
avp.com UPDATE /C:updateapp.ini
```

Пример конфигурационного файла:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

Откат последнего обновления

Синтаксис команды:

```
avp.com ROLLBACK [/R[A]:<файл_отчета>][/password=<ваш_пароль>]
```

Описание параметров приведено в таблице ниже.

/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран; отображаются все события.
<ваш_пароль>	Пароль к программе, заданный в интерфейсе.

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt /password=<ваш_пароль>
```

Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл> <имя_файла>
```

Описание параметров выполнения команды приведено в таблице ниже.

<профайл>	Компонент или задача, для которых выполняется экспорт параметров. В качестве значения параметра **<профайл>** может быть использовано любое значение, указанное в разделе справки «Управление компонентами программы и задачами».
<имя_файла>	Путь к файлу, в который экспортируются параметры Kaspersky Internet Security. Может быть указан абсолютный или относительный путь. Конфигурационный файл сохраняется в бинарном формате (dat), если не указан иной формат либо формат не задан, и далее может использоваться для переноса параметров программы на другие компьютеры. Кроме того, вы можете сохранить конфигурационный файл в текстовом формате, для этого в имени файла укажите расширение txt. Обратите внимание, что импорт параметров защиты из текстового файла не поддерживается, данный файл может использоваться только для просмотра основных параметров работы Kaspersky Internet Security.

Пример:

```
avp.com EXPORT RTP c:\settings.dat
```

Импорт параметров защиты

Синтаксис команды:

```
avp.com IMPORT <имя_файла> [/password=<ваш_пароль>]
```

Описание параметров выполнения команды приведено в таблице ниже.

<имя_файла>	Путь к файлу, из которого импортируются параметры Kaspersky Internet Security. Может быть указан абсолютный или относительный путь.
<ваш_пароль>	Пароль к Kaspersky Internet Security, заданный в интерфейсе программы. Импорт параметров защиты возможен только из файла в бинарном формате.

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Пример:

```
avp.com IMPORT c:\settings.dat /password=<ваш_пароль>
```

Получение файла трассировки

Создание файла трассировки может потребоваться при возникновении проблем в работе Kaspersky Internet Security. Это поможет специалистам Службы технической поддержки более точно диагностировать проблемы.

Рекомендуется включать создание файлов трассировки только для диагностики конкретной проблемы. Постоянное включение трассировки может привести к потере производительности работы компьютера и переполнению жесткого диска.

Синтаксис команды:

```
avp.com TRACE [file] [on|off] [<уровень_трассировки>]
```

Описание параметров приведено в таблице ниже.

[on|off]	Включить / отключить создание файла трассировки.
[file]	Получить трассировку в виде файла.
<уровень_трассировки>	Для данного параметра допустимо указывать числовое значение в диапазоне от 0 (минимальный уровень, только критические сообщения) до 700 (максимальный уровень, все сообщения). При обращении в Службу технической поддержки специалист должен указать необходимый уровень трассировки. Если уровень не был указан, рекомендуется устанавливать значение 500.

Примеры:

- *Отключить создание файлов трассировки:*

```
avp.com TRACE file off
```

- *Создать файл трассировки для отправки в Службу технической поддержки с максимальным уровнем трассировки, равным 500:*

```
avp.com TRACE file on 500
```

Просмотр справки

Для просмотра справочной информации о синтаксисе командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Для получения справочной информации о синтаксисе конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

Коды возврата командной строки

В этом разделе приведено описание кодов возврата командной строки (в таблице ниже). Общие коды могут быть возвращены любой командой командной строки. К кодам возврата задач относятся общие коды, а также коды, специфичные для конкретного типа задачи.

Общие коды возврата	
0	Операция выполнена успешно.
1	Неверное значение параметра.
2	Неизвестная ошибка.
3	Ошибка выполнения задачи.
4	Выполнение задачи отменено.
Коды возврата задач проверки на вирусы	
101	Все опасные объекты обработаны.
102	Обнаружены опасные объекты.

Список уведомлений Kaspersky Internet Security

Этот раздел содержит информацию об уведомлениях, которые могут выводиться на экран в процессе работы Kaspersky Internet Security.

В этом разделе

Уведомления в любом режиме защиты

В этом разделе содержится информация об уведомлениях, которые появляются как в автоматическом, так и в интерактивном режиме защиты (см. раздел «Выбор режима защиты» на стр. 70).

В этом разделе

Требуется специальная процедура лечения

При обнаружении угрозы, которая в данный момент активна в системе (например, вредоносного процесса в оперативной памяти или в объектах автозапуска), на экран выводится уведомление с запросом на проведение специальной расширенной процедуры лечения.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Тип угрозы и наименование вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием вредоносного объекта отображается значок. При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе, представляемой объектом.
- Имя файла вредоносного объекта, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Да, лечить с перезагрузкой** – выполнить специальную процедуру лечения (рекомендуется).

  В процессе лечения блокируется запуск всех приложений, кроме доверенных. По окончании лечения операционная система перезагрузится, поэтому перед лечением рекомендуется сохранить результаты текущей работы и закрыть все программы. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы.
- **Не выполнять** – найденный объект или процесс будет обработан в соответствии с выбранным ранее действием.

Чтобы выбранное действие всегда применялось при возникновении подобной ситуации, установите флажок **Применить ко всем объектам**.

Скрытая загрузка драйвера

Некоторые вредоносные программы загружают драйверы на компьютер пользователя скрытым способом, после чего активность вредоносной программы невозможно контролировать с помощью Kaspersky Internet Security. Полезные программы редко используют подобный способ загрузки драйверов.

Когда Контроль программ обнаруживает попытку загрузить драйвер скрытым способом, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Имя файла драйвера, включая путь к нему.

  Рядом с именем файла отображается значок. При нажатии на значок открывается окно с информацией о драйвере.

Вы можете выбрать одно из следующих действий:

- **Разрешить сейчас** – разрешить загрузку драйвера и добавить драйвер в список исключений.
- **Запретить сейчас** – запретить загрузку драйвера.
- **Карантин** – запретить загрузку драйвера и поместить файл драйвера на карантин.

Запускается программа без цифровой подписи

Когда Контроль программ обнаруживает, что на компьютере запущена программа, у которой отсутствует цифровая подпись и которой по результатам эвристического анализа был присвоен высокий рейтинг опасности, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Наименование запускаемой программы.

  Рядом с наименованием программы отображается значок  . При нажатии на значок открывается окно с информацией о программе.
- Сведения о количестве пользователей, использующих программу и доверяющих ей.

Вы можете выбрать одно из следующих действий:

- **Да, доверяю** – разрешить запуск и выполнение программы без ограничений.
- **Ограничить программу** – разрешить запуск программы, но запретить выполнение опасных операций.
- **Заблокировать** – запретить запуск и выполнение программы сейчас и в дальнейшем.

Подключен съемный диск

При подключении к компьютеру съемного диска на экране открывается уведомление об этом.

Вы можете выбрать одно из следующих действий:

- **Быстрая проверка** – проверить на съемном диске файлы, которые могут представлять потенциальную опасность.
- **Полная проверка** – проверить все файлы на съемном диске.
- **Не проверять** – не проверять съемный диск.

Чтобы в дальнейшем выбранное действие применялось ко всем подключаемым съемным дискам, установите флажок **Применять всегда в подобных случаях**.

Обнаружена новая сеть

При каждом подключении компьютера к новой зоне (сети) на экран выводится уведомление.

В верхней части окна уведомления приведена информация о сети:

- сетевой адаптер, используемый для подключения к сети;
- тип сети (например, «беспроводная»);
- название сети.

В нижней части окна уведомления вы можете присвоить обнаруженной сети статус, на основании которого будет разрешена та или иная сетевая активность:

- **Да, это доверенная сеть**. Этот статус рекомендуется применять только для безопасной сети, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным.

- **Локальная сеть**. Рекомендуется применять этот статус для сетей со средней степенью риска работы в них (например, для внутренней корпоративной сети).

- **Нет, это публичная сеть**. Сеть с высокой степенью риска, при работе в которой компьютер подвержен любым возможным типам угроз. Этот статус также рекомендуется выбирать для сетей, не защищенных антивирусными программами, сетевыми экранами, фильтрами. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в сети.

Обнаружен ненадежный сертификат

Kaspersky Internet Security проверяет безопасность соединения по протоколу SSL с помощью установленного сертификата. При попытке соединения с сервером с использованием некорректного сертификата (что может происходить, например, в случае подмены сертификата злоумышленниками) на экран выводится уведомление.

В уведомлении содержится следующая информация:

- описание угрозы;
- ссылка на просмотр сертификата;
- возможные причины ошибки;
- веб-адрес ресурса.

Вы можете выбрать одно из следующих действий:

- **Да, принять ненадежный сертификат** – продолжить соединение с веб-ресурсом.
- **Отвергнуть сертификат** – разорвать соединение с веб-ресурсом.

Запрос разрешения на доступ к веб-сайту из регионального домена

При обращении к веб-сайту из регионального домена, который не относится к запрещенным или разрешенным, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- описание причины, по которой заблокировано обращение к веб-сайту;
- название региона, к которому относится веб-сайт;
- домен, характеристика степени зараженности веб-сайтов в домене;
- адрес веб-сайта;
- наименование программы, выполнившей обращение к веб-сайту.

Вы можете выбрать одно из следующих действий:

- **Да, разрешить обращение** – загрузить веб-сайт.
- **Нет, запретить обращение** – отказаться от загрузки веб-сайта.

Чтобы выбранное действие применялось ко всем веб-сайтам из этого регионального домена, установите флажок **Запомнить для данного региона**.

Обнаружена программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя

Когда Мониторинг активности обнаруживает программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Тип и наименование программы, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Рядом с наименованием программы отображается значок . При нажатии на значок открывается окно с информацией о программе.
- Идентификатор процесса и имя файла программы, включая путь к нему.
- Ссылка на окно с историей появления программы.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – разрешить выполнение программы.
- **Карантин** – завершить программу; поместить файл программы на карантин, где он не будет представлять угрозы безопасности вашего компьютера.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  > Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.

- **Завершить программу** – прервать выполнение программы.
- **Добавить в исключения** – разрешить программе всегда выполнять подобные действия.

Файл на карантине не заражен

Kaspersky Internet Security по умолчанию проверяет файлы на карантине после каждого обновления баз. Если в результате проверки файла на карантине программа определяет, что он не заражен, то на экран выводится уведомление.

В уведомлении содержится следующая информация:

- рекомендация восстановить файл, находящийся на карантине;
- имя файла, включая путь к папке, в которой файл находился до помещения на карантин.

Вы можете выбрать одно из следующих действий:

- **Восстановить** – восстановить файл, удалив его из карантина и поместив в папку, в которой файл находился до помещения на карантин.
- **Отмена** – оставить файл на карантине.

Вышла новая версия продукта

При появлении новой версии Kaspersky Internet Security, доступной для загрузки с серверов «Лаборатории Касперского», на экран выводится уведомление.

В уведомлении содержится следующая информация:

- ссылка на окно с подробной информацией о вышедшей версии программы;
- размер установочного дистрибутива.

Вы можете выбрать одно из следующих действий:

- **Да, загрузить** – загрузить дистрибутив новой версии программы в указанную папку.
- **Нет** – отказаться от загрузки дистрибутива.

Чтобы уведомление о новой версии программы больше не выводилось на экран, установите флажок **Не информировать меня об этом обновлении**.

Вышло техническое обновление

При выходе технического обновления Kaspersky Internet Security, доступного для загрузки с серверов «Лаборатории Касперского», на экран выводится уведомление.

В уведомлении содержится следующая информация:

- номер версии программы, установленной на компьютере;
- номер версии программы после предлагаемого технического обновления;
- ссылка на окно с подробной информацией о техническом обновлении;
- размер файла обновления.

Вы можете выбрать одно из следующих действий:

- **Да, загрузить** – загрузить файл обновления в указанную папку.
- **Нет** – отказаться от загрузки обновления. Этот вариант действия доступен, если установлен флажок **Не информировать меня об этом обновлении** (см. далее).
- **Нет, напомнить позже** – отказаться от загрузки обновления сейчас и получить напоминание об обновлении позже. Этот вариант действия доступен, если снят флажок **Не информировать меня об этом обновлении** (см. далее).

Чтобы уведомление об этом обновлении больше не выводилось на экран, установите флажок **Не информировать меня об этом обновлении**.

Техническое обновление загружено

По завершении загрузки технического обновления Kaspersky Internet Security с серверов «Лаборатории Касперского» на экран выводится уведомление.

В уведомлении содержится следующая информация:

- номер версии программы после технического обновления;
- ссылка на файл обновления.

Вы можете выбрать одно из следующих действий:

- **Да, установить** – установить обновление.

  После установки обновления понадобится перезагрузка операционной системы.

- **Отложить установку** – отказаться от установки, чтобы выполнить ее позднее.

Загруженное техническое обновление не установлено

При наличии на вашем компьютере ранее загруженного технического обновления Kaspersky Internet Security, которое не было установлено, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- номер версии программы после технического обновления;
- ссылка на файл обновления.

Вы можете выбрать одно из следующих действий:

- **Да, установить** – установить обновление.

  После установки обновления понадобится перезагрузка операционной системы.

- **Отложить установку** – отказаться от установки, чтобы выполнить ее позднее.

Чтобы уведомление об этом обновлении больше не выводилось на экран, установите флажок **Не спрашивать до появления новой версии**.

Срок действия лицензии истек

По истечении срока действия пробной лицензии Kaspersky Internet Security выводит на экран уведомление об этом.

В уведомлении содержится следующая информация:

- длительность пробного периода;
- информация о результатах работы программы (может включать ссылку на просмотр более подробных сведений).

Вы можете выбрать одно из следующих действий:

- **Да, приобрести** – при выборе этого варианта открывается окно веб-браузера и загружается страница интернет-магазина, где вы можете приобрести коммерческую лицензию на использование программы.
- **Отмена** – отказаться от использования программы. При выборе этого варианта программа перестает выполнять все основные функции (проверка на вирусы, обновление, функции постоянной защиты и так далее).

Рекомендуется обновить базы перед проверкой

При запуске задач проверки до или во время первого обновления баз, на экран выводится уведомление.

В уведомлении содержится рекомендация обновить базы или дождаться окончания обновления перед проверкой.

Вы можете выбрать одно из следующих действий:

- **Обновить базы перед проверкой** – запустить обновление баз, после чего автоматически запустится задача проверки. Этот вариант действия доступен, если вы запустили задачу проверки до первого обновления баз.
- **Запустить проверку после обновления** – дождаться окончания обновления баз и запустить задачу проверки автоматически. Этот вариант действия доступен, если вы запустили задачу проверки во время первого обновления баз.
- **Запустить проверку сейчас** – запустить задачу проверки, не дожидаясь обновления баз.

Уведомления в интерактивном режиме защиты

В этом разделе содержится информация об уведомлениях, которые появляются в интерактивном режиме защиты (см. раздел «Выбор режима защиты» на стр. 70).

В этом разделе

Обнаружена сетевая активность программы

При обнаружении сетевой активности программы (по умолчанию для программ, входящих в группы **Слабые ограничения** или **Сильные ограничения**) на экран выводится уведомление.

Уведомление выводится, если Kaspersky Internet Security работает в интерактивном режиме (см. раздел «Выбор режима защиты» на стр. 70) и если для программы, сетевая активность которой была обнаружена, не создано пакетное правило (см. стр. 119).

Уведомление содержит следующую информацию:

- название программы и краткую характеристику соединения, которое она инициирует;
- информацию о соединении (тип соединения, локальный и удаленный порты, адрес, с которым выполняется соединение);
- последовательность запуска программы.

Вы можете выбрать одно из следующих действий:

- **Разрешить сейчас**.
- **Запретить сейчас**.
- **Создать правило**. При выборе этого варианта открывается окно **Сетевой экран**, в котором вы можете создать правило, регулирующее сетевую активность программы (см. раздел «Изменение правил программы» на стр. 120).

Вы можете разрешить или запретить сетевую активность программы единожды или на более продолжительный срок, выбрав одно из следующих действий:

- **Разрешить сейчас** или **Запретить сейчас** – единожды разрешить или запретить сетевую активность программы.
- **Разрешить сейчас** или **Запретить сейчас** (при установленном флажке **Запомнить на сессию работы программы**) – запомнить выбранное действие на сессию работы программы, проявившей сетевую активность.

  Если в окне установлен флажок **Запомнить навсегда**, по ссылке **навсегда** можно изменить его название на **Запомнить на сессию работы программы**.
- **Разрешить сейчас** или **Запретить сейчас** (при установленном флажке **Запомнить навсегда**) – запомнить выбранное для программы действие и применять его всегда.

  Если в окне установлен флажок **Запомнить на сессию работы программы**, по ссылке **на сессию работы программы** можно изменить его название на **Запомнить навсегда**.

Обнаружен подозрительный / вредоносный объект

В процессе работы Файлового Антивируса, Почтового Антивируса или проверки на вирусы на экран выводится уведомление в случае обнаружения одного из следующих объектов:

- вредоносного объекта;

- объекта, содержащего код неизвестного вируса;
- объекта, содержащего модифицированный код известного вируса.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Тип угрозы и наименование вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием вредоносного объекта отображается значок. При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе, представляемой объектом.
- Имя файла вредоносного объекта, включая путь к нему.

Вы можете выбрать одно из следующих действий над объектом:

- **Лечить** – пытаться лечить вредоносный объект. Этот вариант предлагается, если угроза известна.

  Перед лечением формируется резервная копия объекта.
- **Карантин** – поместить объект на карантин, где он не будет представлять опасность для вашего компьютера. Этот вариант предлагается, если неизвестны угроза и способы лечения объекта.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  > Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.
- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта.
- **Пропустить / Заблокировать** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем угрозам того же типа, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска Kaspersky Internet Security, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженный объект не является вредоносным, во избежание повторных срабатываний программы при работе с этим объектом рекомендуется добавить его в доверенную зону.

Обнаружена уязвимость

При обнаружении уязвимости на экран выводится уведомление.

Уведомление содержит следующую информацию:

- Описания уязвимости.
- Наименование уязвимости, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

Рядом с наименованием отображается значок  . При нажатии на значок открывается окно с информацией об уязвимости. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об уязвимости.

- Имя файла уязвимого объекта, включая путь к нему.

Вы можете выбрать одно из следующих действий над объектом:

- **Да, исправить** – устранить уязвимость.
- **Пропустить** – не предпринимать никаких действий над уязвимым объектом.

Запрос разрешения на действия программы

При попытке компьютерной программы выполнить какое-либо действие, о безопасности или необходимости которого в Kaspersky Internet Security нет информации, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Наименование программы и значок  . При нажатии на значок открывается окно с информацией о программе.
- Описание действий программы.
- Местонахождение файла программы.
- Последовательность запуска программы.

Вы можете разрешить или запретить выполнение программы, выбрав одно из следующих действий:

- **Сделать доверенной** – поместить программу в группу *Доверенные* (выполнение программы будет всегда разрешено).
- **Разрешить сейчас** – разрешить выполнение программы однократно.
- **Запретить сейчас** – запретить выполнение программы однократно.
- **Завершить программу и сделать недоверенной** – поместить программу в группу *Недоверенные* (выполнение программы будет всегда запрещено).

Обнаружена опасная активность в системе

При обнаружении Проактивной защитой опасной активности какой-либо программы в системе на экран выводится уведомление.

Уведомление содержит следующую информацию:

- Описание угрозы.
- Тип угрозы и наименование вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием вредоносного объекта отображается значок  . При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе, представляемой объектом.
- Идентификатор процесса и имя файла программы, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – разрешить выполнение программы.
- **Карантин** – завершить программу; поместить файл программы на карантин, где он не будет представлять угрозы безопасности вашего компьютера.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.

- **Завершить программу** – прервать выполнение программы.
- **Добавить в исключения** – разрешить программе всегда выполнять подобные действия.

Если вы уверены, что обнаруженная программа не является опасной, во избежание повторных срабатываний Kaspersky Internet Security при ее обнаружении рекомендуется добавить программу в доверенную зону.

Откат изменений, выполненных программой, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя

Изменения в системе, сделанные программой, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя, рекомендуется откатить (отменить). При завершении работы такой программы на экран выводится уведомление с запросом на откат изменений.

В уведомлении содержится следующая информация:

- Запрос на откат изменений, выполненных программой, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.
- Тип программы и ее наименование.

  Рядом с наименованием программы отображается значок . При нажатии на значок открывается окно с информацией о программе.

- Идентификатор процесса и имя файла программы, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Пропустить** – не откатывать изменения.
- **Да, откатить** – откатить изменения, выполненные программой.

Обнаружена вредоносная программа

Когда Мониторинг активности обнаруживает программу, поведение которой соответствует действиям вредоносных программ, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.

- Тип вредоносной программы и ее наименование.

  Рядом с наименованием программы отображается значок. При нажатии на значок открывается окно с информацией о программе.

- Идентификатор процесса и имя файла программы, включая путь к нему.

- Ссылка на окно с историей появления программы.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – разрешить выполнение программы.

- **Карантин** – завершить программу; поместить файл программы на карантин, где он не будет представлять угрозы безопасности вашего компьютера.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.

- **Завершить программу** – прервать выполнение программы.

- **Добавить в исключения** – разрешить программе всегда выполнять подобные действия.

Обнаружена программа, которую могут использовать злоумышленники

Если Файловый Антивирус, Почтовый Антивирус или задача проверки на вирусы обнаруживают программу, которую могут использовать злоумышленники, на экране открывается уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.

- Тип угрозы и наименование объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием объекта отображается значок. При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию.

- Имя файла объекта, включая путь к нему.

Вы можете выбрать одно из следующих действий над объектом:

- **Карантин** – поместить объект на карантин, где он не будет представлять опасность для вашего компьютера. Этот вариант предлагается, если не известны угроза и способы лечения объекта.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.

- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта.
- **Удалить архив** – удалить защищенный паролем архив.
- **Пропустить / Заблокировать** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).
- **Добавить в исключения** – создать правило исключения для данного типа угроз.

Чтобы применить выбранное действие ко всем угрозам того же типа, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска Kaspersky Internet Security, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженный объект не является вредоносным, во избежание повторных срабатываний программы при работе с этим объектом рекомендуется добавить его в доверенную зону.

Обнаружена подозрительная / вредоносная ссылка

Когда Kaspersky Internet Security обнаруживает попытку перейти на веб-сайт с вредоносным или подозрительным содержимым, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- описание угрозы;
- наименование программы (браузера), с помощью которой выполняется загрузка веб-сайта;
- адрес веб-сайта или веб-страницы с подозрительным или вредоносным содержимым.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – продолжить загрузку веб-сайта.
- **Запретить** – заблокировать загрузку веб-сайта.

Чтобы применить выбранное действие ко всем веб-сайтам с угрозой того же типа, обнаруженным в текущем сеансе работы компонента защиты, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента его выключения либо перезапуска Kaspersky Internet Security.

Обнаружен опасный объект в трафике

При обнаружении Веб-Антивирусом опасного объекта в трафике на экран выводится уведомление.

Уведомление содержит следующую информацию:

- Описание угрозы или выполняемых программой действий.
- Наименование программы, выполняющей действие.
- Тип угрозы и наименование вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием вредоносного объекта отображается значок  . При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на

веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе, представляемой объектом.

- Местонахождение объекта (URL-адрес).

Вы можете выбрать одно из следующих действий:

- **Разрешить** – продолжить загрузку объекта.
- **Запретить** – заблокировать загрузку объекта с веб-ресурса.

Чтобы применить выбранное действие ко всем угрозам того же типа, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента его выключения либо перезапуска Kaspersky Internet Security.

Обнаружена попытка обратиться к фишинг-сайту

Когда Kaspersky Internet Security обнаруживает попытку обратиться к веб-сайту, который относится или возможно относится к фишинговым, на экран выводится уведомление об этом.

В уведомлении содержится следующая информация:

- описание угрозы;
- адрес веб-сайта.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – продолжить загрузку веб-сайта.
- **Запретить** – заблокировать загрузку веб-сайта.

Чтобы применить выбранное действие ко всем веб-сайтам с угрозой того же типа, которые обнаружены в текущем сеансе работы Kaspersky Internet Security, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента его выключения либо перезапуска Kaspersky Internet Security.

Обнаружена попытка доступа к системному реестру

При обнаружении Проактивной защитой попытки получения доступа к ключам системного реестра на экран выводится уведомление.

В уведомлении содержится следующая информация:

- ключ реестра, к которому осуществляется попытка получения доступа;
- имя файла процесса, инициирующего попытку получения доступа к ключам реестра, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Разрешить** – однократно разрешить выполнение опасного действия;
- **Запретить** – однократно запретить выполнение опасного действия.

Чтобы выбранное вами действие выполнялось при каждой попытке получения доступа к ключам реестра, установите флажок **Создать правило**.

Если вы считаете, что любая активность программы, которая инициировала обращение к ключам системного реестра, не является опасной, добавьте эту программу в список доверенных.

Лечение объекта невозможно

В некоторых случаях лечение объекта невозможно (например, если файл поврежден настолько, что удалить из него вредоносный код и восстановить целостность не удается). Процедура лечения не применима к некоторым видам вредоносных объектов, например к троянским программам. В случае, если лечение объекта невозможно, на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Тип угрозы и наименование вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием вредоносного объекта отображается значок. При нажатии на значок открывается окно с информацией об объекте. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе, представляемой объектом.
- Имя файла вредоносного объекта, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта.
- **Пропустить / Заблокировать** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).
- **Добавить в исключения** – создать правило исключения для данного типа угроз.

Чтобы применить выбранное действие ко всем угрозам того же типа, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить ко всем объектам**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска Kaspersky Internet Security, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружен скрытый процесс

При обнаружении Проактивной защитой скрытого процесса в системе на экран выводится уведомление.

В уведомлении содержится следующая информация:

- Описание угрозы.
- Тип и наименование угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского».

  Рядом с наименованием отображается значок. При нажатии на значок открывается окно с информацией об угрозе. По ссылке www.securelist.ru в окне вы сможете перейти на веб-сайт Вирусной энциклопедии и получить более подробную информацию об угрозе.
- Имя файла процесса, включая путь к нему.

Вы можете выбрать одно из следующих действий:

- **Карантин** – завершить процесс, файл процесса поместить на карантин, где он не будет представлять угрозу безопасности вашего компьютера.

  При последующих проверках карантина статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  Статус файла, помещенного на карантин, может быть изменен при повторной проверке на *не заражен*, но не ранее, чем через три дня после помещения на карантин.

- **Завершить** – прервать процесс.

- **Разрешить** – разрешить выполнение процесса.

Чтобы применить выбранное действие ко всем угрозам того же типа, обнаруженным в текущем сеансе работы Проактивной защиты, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента его выключения либо перезапуска Kaspersky Internet Security.

Если вы уверены, что обнаруженный процесс не является опасным, во избежание повторных срабатываний Kaspersky Internet Security при его обнаружении рекомендуется добавить его в доверенную зону.

Запрещенный регион домена / Обращение запрещено

Обращение к веб-сайту может быть запрещено Веб-Антивирусом на основе принадлежности веб-сайта к региональному домену. Домен считается запрещенным в следующих случаях:

- обращение к домену запрещено пользователем при настройке Веб-Антивируса;

- предыдущее обращение к веб-сайту из данного региона было запрещено пользователем.

Когда Гео-фильтр (модуль Веб-Антивируса) обнаруживает попытку перейти на веб-сайт, относящийся к запрещенному региону, в окне браузера выводится уведомление.

В уведомлении содержится следующая информация:

- описание причины, по которой заблокировано обращение к веб-сайту;

- название региона, к которому относится веб-сайт;

- домен, характеристика степени зараженности веб-сайтов в домене;

- URL-адрес веб-сайта.

Вы можете выбрать одно из следующих действий:

- **Вернуться к предыдущей странице** – открыть предыдущую страницу.

- **Открыть веб-ресурс** – загрузить веб-сайт, относящийся к запрещенному домену.

- **Открыть настройку Гео-фильтра** – открыть окно настройки Веб-Антивируса на закладке **Гео-фильтр**.

Опасный веб-ресурс

Когда Веб-фильтр (модуль Веб-Антивируса) обнаруживает попытку перейти на опасный веб-сайт, в окне браузера выводится уведомление.

В уведомлении содержится следующая информация:

- описание причины, по которой заблокировано обращение к веб-сайту;
- адрес веб-сайта.

Вы можете выбрать одно из следующих действий:

- **Вернуться к предыдущей странице** – не загружая опасный веб-сайт, открыть предыдущую страницу.
- **Открыть в любом случае** – загрузить опасный веб-сайт.

Нет информации о безопасности веб-ресурса

Когда Веб-фильтр (модуль Веб-Антивируса) обнаруживает попытку перейти на веб-сайт, о безопасности которого нет достоверных сведений, в окне браузера выводится уведомление.

В уведомлении содержится следующая информация:

- описание причины, по которой приостановлено обращение к веб-сайту;
- адрес веб-сайта.

Вы можете выбрать одно из следующих действий:

- **Да, открыть веб-ресурс** – загрузить веб-сайт.
- **Открыть и добавить в доверенные адреса** – загрузить веб-сайт, а его адрес добавить в список доверенных, чтобы в дальнейшем Веб-фильтр не приостанавливал загрузку этого веб-сайта.
- **Открыть в безопасном браузере** – загрузить веб-сайт в безопасном браузере (только для браузеров Microsoft Internet Explorer, Mozilla Firefox и Google Chrome). При загрузке в безопасном браузере вредоносные объекты на загружаемых страницах, не будут представлять угрозу безопасности компьютера.
- **Нет, вернуться к предыдущей странице** – не загружать веб-сайт, а открыть предыдущую страницу.

Рекомендуется перейти в режим безопасного просмотра веб-сайтов

Для работы с интернет-банкингом «Лаборатория Касперского» рекомендует использовать режим безопасного просмотра веб-сайтов, обеспечивающий повышенную защиту ваших персональных данных.

При попытке перейти на веб-сайт интернет-банкинга Веб-Антивирус выводит в окне браузера уведомление.

В уведомлении содержится следующая информация:

- рекомендация перейти в режим безопасного просмотра веб-сайтов;
- адрес ресурса интернет-банкинга.

Вы можете выбрать одно из следующих действий:

- **Открыть в режиме безопасного просмотра веб-сайтов** – открыть веб-сайт, используя безопасный браузер (только для браузеров Microsoft Internet Explorer, Mozilla Firefox и Google Chrome).

- **Открыть веб-ресурс** – открыть веб-сайт в обычном режиме.

- **Вернуться к предыдущей странице** – не открывая веб-сайт, открыть предыдущую страницу в обычном режиме.

Рекомендуется выйти из режима безопасного просмотра веб-сайтов

При работе с веб-сайтами интернет-банкинга используется режим безопасного просмотра веб-сайтов. При переходе на другой веб-сайт, не относящийся к интернет-банкингу, рекомендуется выйти из режима безопасного просмотра веб-сайтов. Если продолжить работу с обычным веб-сайтом в режиме безопасного просмотра веб-сайтов, это может ослабить защиту персональных данных.

При попытке в режиме безопасного просмотра веб-сайтов перейти с веб-сайта интернет-банкинга на другой веб-сайт Веб-Антивирус выводит в окне браузера уведомление.

В уведомлении содержится следующая информация:

- рекомендация выйти из режима безопасного просмотра веб-сайтов;

- адрес веб-сайта, на который вы переходите с веб-сайта интернет-банкинга.

Вы можете выбрать одно из следующих действий:

- **Открыть веб-ресурс в обычном браузере** – выйти из режима безопасного просмотра веб-сайтов и открыть веб-сайт в обычном режиме.

- **Это банковский веб-сайт, продолжить в режиме безопасного просмотра веб-сайтов** – открыть веб-сайт, оставаясь в режиме безопасного просмотра веб-сайтов.

- **Вернуться к предыдущей странице** – открыть предыдущую страницу в режиме безопасного просмотра веб-сайтов.

ГЛОССАРИЙ

B

Boot-вирус (загрузочный)

Вирус, поражающий загрузочные секторы дисков компьютера. Вирус «заставляет» систему при ее перезапуске считывать в память и отдавать управление не оригинальному коду загрузчика, а коду вируса.

K

Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Internet Security на новые виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

Присоединенный или встроенный в другой файл объект. Программа «Лаборатории Касперского» позволяет проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

S

SOCKS

Протокол прокси-сервера, позволяющий реализовать двухточечное соединение между компьютерами внутренней и внешней сетей.

A

Активация программы

Перевод программы в полнофункциональный режим. Для активации программы пользователю необходима лицензия.

Активная лицензия

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

Альтернативные потоки NTFS

Потоки данных файловой системы NTFS (alternate data streams), предназначенные для размещения дополнительных атрибутов или информации к файлу.

Каждый файл в файловой системе NTFS представляет собой набор потоков (streams). В одном из них находится содержимое файла, которое мы сможем увидеть, открыв файл, остальные (альтернативные) предназначены для размещения метаинформации и обеспечивают, например, совместимость системы NTFS с другими системами, такими как старая файловая система Macintosh – Hierarchical File System (HFS). Потоки можно создавать, удалять, сохранять отдельно, переименовывать и даже запускать как процесс.

Альтернативные потоки могут использоваться злоумышленниками для скрытой передачи или получения данных с компьютера.

Аппаратный порт

Разъем на каком-либо элементе аппаратного обеспечения компьютера, в который подключается кабель или вилка (LPT-порт, последовательный порт, USB).

Архив

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

Б

База подозрительных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как потенциально 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

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз.

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

В

Вирусная атака

Ряд целенаправленных попыток заразить компьютер вирусом.

Возможно зараженный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Д

Дамп памяти

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

Двухканальный шлюз

Компьютер, снабженный двумя сетевыми адаптерами, каждый из которых подключен к разным сетям, пересылающий информацию из одной сети в другую.

Доверенный процесс

Программный процесс, файловые операции которого не контролируются программой «Лаборатории Касперского» в режиме постоянной защиты. То есть все объекты, запускаемые, открываемые и сохраняемые доверенным процессом, не проверяются.

Дополнительная лицензия

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

З

Заголовок

Информация, которая содержится в начале файла или сообщения и состоит из низкоуровневых данных о статусе и обработке файла (сообщения). В частности, заголовок сообщения электронной почты содержит такие сведения, как данные об отправителе, получателе и дату.

Загрузочный сектор диска

Загрузочный сектор – это особый сектор на жестком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа «Лаборатории Касперского» позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: **Постоянная защита файлов**, **Полная проверка компьютера**, **Обновление баз**.

Зараженный объект

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

И

Исключение

Исключение – объект, исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

К

Карантин

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

Контролируемый объект

Файл, перемещаемый по протоколам HTTP, FTP или SMTP через межсетевой экран и направляемый на проверку программе «Лаборатории Касперского».

Л

Лечение объектов

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В процессе лечения часть данных может быть потеряна.

Лечение объектов при перезагрузке

Способ обработки зараженных объектов, используемых в момент лечения другими программами. Заключается в создании копии зараженного объекта, лечении созданной копии и замене при следующей перезагрузке исходного зараженного объекта его вылеченной копией.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

М

Маска подсети

Маска подсети (также именуемая сетевой маской) и сетевой адрес определяют адреса входящих в состав сети компьютеров.

Маска файла

Представление имени и расширения файла общими символами. Двумя основными символами, используемыми в масках файлов, являются ***** и **?** (где ***** – любое число любых символов, а **?** – любой один символ). При помощи данных знаков можно представить любой файл. Обратите внимание, что имя и расширение файла всегда пишутся через точку.

Н

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Kaspersky Internet Security.

Нецензурное сообщение

Электронное сообщение, содержащее ненормативную лексику.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Обновление баз

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование баз с серверов обновлений «Лаборатории Касперского» на компьютер и автоматическое подключение их к программе.

Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Опасный объект

Объект, внутри которого содержится вирус. Не рекомендуется работать с такими объектами, поскольку это может привести к заражению компьютера. При обнаружении зараженного объекта рекомендуется лечить его с помощью программ «Лаборатории Касперского» или удалить, если лечение невозможно.

П

Пакет обновлений

Пакет файлов для обновления программного обеспечения, который копируется из интернета и устанавливается на вашем компьютере.

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Перехватчик

Подкомпонент программы, отвечающий за проверку определенных типов почтовых сообщений. Набор подлежащих установке перехватчиков зависит от того, в какой роли или в какой комбинации ролей развернута программа.

Подозрительное сообщение

Сообщение, которое нельзя однозначно классифицировать как спам, но при проверке оно вызвало подозрение (например, некоторые виды рассылок и рекламных сообщений).

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Подозрительные объекты обнаруживаются при помощи эвристического анализатора.

Помещение объектов на карантин

Способ обработки возможно зараженного объекта, при котором доступ к объекту блокируется и он перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Порт ввода-вывода

Используется в микропроцессорах (например, Intel) при обмене данными с аппаратным обеспечением. Порт ввода-вывода сопоставляется с тем или иным устройством и позволяет программам обращаться к нему для обмена данными.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера», для размещения и распространения вредоносного объекта. Как правило, это исполняемые

файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Почтовые базы

Базы, включающие почтовые сообщения, хранящиеся на вашем компьютере и имеющие специальный формат. Каждое входящее / исходящее письмо помещается в почтовую базу после его получения / отправки. Такие базы проверяются во время полной проверки компьютера.

Входящие и исходящие почтовые сообщения в момент их получения и отправки анализируются на присутствие вирусов в реальном времени, если включена постоянная защита.

Проверка трафика

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и пр.).

Программные модули

Файлы, входящие в состав дистрибутива программы «Лаборатории Касперского» и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (Постоянная защита, Проверка по требованию, Обновление), соответствует свой исполняемый модуль. Запуская из главного окна полную проверку вашего компьютера, вы инициируете запуск модуля этой задачи.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Протокол

Четко определенный и стандартизованный набор правил, регулирующих взаимодействие между клиентом и сервером. К ряду хорошо известных протоколов и связанных с ними служб относятся: HTTP (WWW), FTP и NNTP (новости).

Протокол интернета (IP)

Базовый протокол сети интернет, используемый без изменений со времени его разработки в 1974 г. Он осуществляет основные операции передачи данных с одного компьютера на другой и служит в качестве основы для протоколов более высокого уровня, таких как TCP и UDP. Он управляет соединением и обработкой ошибок. Такие технологии, как NAT и маскарад, делают возможным скрытие больших частных сетей за небольшим числом IP-адресов (или даже одним адресом), что позволяет удовлетворить запросы постоянно растущего интернета, используя относительно ограниченное адресное пространство IPv4.

Р

Рейтинг опасности

Показатель опасности компьютерной программы для операционной системы. Рейтинг вычисляется с помощью эвристического анализа на основании критериев двух типов:

- статических (например, информация об исполняемом файле программы: размер файла, дата создания и т. п.);
- динамических, которые применяются во время моделирования работы программы в виртуальном окружении (анализ вызовов программой системных функций).

Рейтинг опасности позволяет выявить поведение, типичное для вредоносных программ. Чем ниже рейтинг опасности, тем больше действий в системе разрешено программе.

Рекомендуемый уровень

Уровень безопасности, базирующийся на параметрах работы программы, рекомендуемых экспертами «Лаборатории Касперского» и обеспечивающих оптимальную защиту вашего компьютера. Данный уровень установлен для использования по умолчанию.

Руткит

Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

В системах Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в системе. Кроме того, как правило, rootkit может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие rootkit устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

С

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей на ваш компьютер.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими компьютерами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится на Сервере администрирования в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Сетевой порт

Параметр протоколов TCP и UDP, определяющий назначение пакетов данных в IP-формате, передаваемых на хост по сети, и позволяющий различным программам, выполняемым на одном хосте, получать данные независимо друг от друга. Каждая программа обрабатывает данные, поступающие на определённый порт (иногда говорят, что программа «слушает» этот номер порта).

Обычно за некоторыми распространенными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу HTTP на TCP-порт 80), хотя в общем случае программа может использовать любой протокол на любом порте. Возможные значения: от 1 до 65535.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения небольшой конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторый веб-сайт.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

Служба имен доменов (DNS)

Распределенная система преобразования имени хоста (компьютера или другого сетевого устройства) в IP-адрес. DNS работает в сетях TCP/IP. Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP (PTR-записи). Разрешение имен DNS обычно осуществляется сетевыми программами, а не самими пользователями.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Спам

Несанкционированная массовая рассылка электронных сообщений, чаще всего рекламного характера.

Список доверенных веб-адресов

Список масок и адресов веб-ресурсов, содержимому которых доверяет пользователь. Программа «Лаборатории Касперского» не проверяет веб-страницы, соответствующие какому-либо элементу списка, на присутствие вредоносных объектов.

Список запрещенных веб-адресов

Список масок и адресов веб-ресурсов, доступ к которым блокируется программой «Лаборатории Касперского». Список адресов формируется пользователем при настройке параметров программы.

Список запрещенных отправителей

(также «Черный» список адресов)

Список электронных адресов, входящие сообщения с которых блокируются программой «Лаборатории Касперского» независимо от их содержания.

Список проверяемых веб-адресов

Список масок и адресов веб-ресурсов, которые проверяются программой «Лаборатории Касперского» на присутствие вредоносных объектов в обязательном порядке.

Список разрешенных веб-адресов

Список масок и адресов веб-ресурсов, доступ к которым не блокируется программой «Лаборатории Касперского». Список адресов формируется пользователем при настройке параметров программы.

Список разрешенных отправителей

(также «Белый» список адресов)

Список электронных адресов, входящие сообщения с которых не проверяются программой «Лаборатории Касперского».

Срок действия лицензии

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». Срок действия лицензии, как правило, составляет календарный год со дня ее установки. После окончания срока действия лицензии функциональность программы сокращается: вы не сможете обновлять базы программы.

Срочное обновление

Критическое обновление модулей программы «Лаборатории Касперского».

Счетчик вирусной эпидемии

Шаблон, на основании которого проводится оповещение об угрозе возникновения вирусной эпидемии. Счетчик вирусной эпидемии содержит набор параметров, определяющих порог вирусной активности, способ распространения и текст рассылаемых сообщений.

Т

Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что параметры проверки (антивирусные базы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой «Лаборатории Касперского» и которому был присвоен статус *незаражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили антивирусные базы, архив будет проверен повторно.

Ограничения технологии **iChecker**:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять, был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов (**exe**, **dll**, **lnk**, **ttf**, **inf**, **sys**, **com**, **chm**, **zip**, **rar**).

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

Удаление объекта

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

Удаление сообщения

Способ обработки электронного сообщения, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам или вредоносный объект. Перед удалением сообщения его копия сохраняется в резервном хранилище (если данная функциональность не отключена).

Упакованный файл

Файл архива, который содержит в себе некоторую программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

Уровень важности события

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

- **Критическое событие**.
- **Отказ функционирования**.
- **Предупреждение**.
- **Информационное сообщение**.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Установка с помощью сценария входа

Метод удаленной установки программ «Лаборатории Касперского», который позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей). При регистрации пользователя в домене предпринимается попытка провести установку программы на клиентском компьютере, с которого пользователь зарегистрировался. Данный метод рекомендуется для установки программ компании на компьютеры, работающие под управлением операционных систем Microsoft Windows 98 / Me.

Ф

Файл ключа

Файл с расширением key, который является вашим личным «ключом», необходимым для работы с программой «Лаборатории Касперского». Файл ключа входит в комплект поставки продукта, если вы приобрели его у

дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера.

Ч

Черный список файлов ключей

База данных, содержащая информацию о заблокированных «Лабораторией Касперского» файлах ключей. Содержимое файла с «черным» списком обновляется вместе с базами.

Ш

Шаблон уведомления

Шаблон, на основании которого проводится оповещение об обнаруженных при проверке зараженных объектах. Шаблон уведомления содержит набор параметров, определяющих порядок уведомления, способ распространения и текст рассылаемых сообщений.

Э

Эвристический анализатор

Технология обнаружения угроз, не определяемых с помощью баз программ «Лаборатории Касперского». Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: 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 для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации 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 новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежечасно*, *база Анти-Спама – каждые 5 минут*.

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 программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки возможно зараженных файлов в архивированном виде)
	http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)
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.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

E

I

A

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Э