Руководство пользователя

KASPERSKY INTERNET SECURITY 2009

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что эта документация поможет вам в работе и ответит на большинство интересующих вопросов, связанных с продуктом.

Изменения в документ могут вноситься без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

+7 (495) 645-7939,
Тел., факс: +7 (495) 797-8700,
+7 (495) 956-7000

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

Дата редакции: 25.07.2008

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В ЭТОМ РАЗДЕЛЕ

Получение информации о приложении

Если у вас возникли вопросы по выбору, приобретению, установке или использованию Kaspersky Internet Security, вы можете быстро получить ответы на них.

«Лаборатория Касперского» предоставляет различные источники информации о приложении, и вы можете выбрать наиболее удобный для вас в зависимости от важности и срочности вопроса.

Обращение в Департамент продаж

Если у вас возникли вопросы по выбору, приобретению Kaspersky Internet Security или продлению срока его использования, вы можете поговорить с сотрудниками Департамента продаж в нашем центральном офисе в Москве по телефонам:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

Обслуживание ведется на русском и английском языках.

Вы можете задать вопрос сотрудникам Департамента продаж по электронной почте, по адресу sales@kaspersky.com.

Обращение в Службу технической поддержки

Если вы уже приобрели Kaspersky Internet Security, вы можете получить информацию о нем от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваши вопросы по установке и использованию приложения, не отраженные в справке, а если ваш компьютер был заражен, то помогут преодолеть последствия работы вредоносных программ.

Прежде чем обращаться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами поддержки (http://support.kaspersky.ru/support/rules).

Электронный запрос в Службу технической поддержки (для зарегистрированных пользователей)

Вы можете задать вопрос специалистам Службы технической поддержки, заполнив веб-форму системы обработки клиентских запросов Helpdesk (http://support.kaspersky.ru/helpdesk.html).

Вы можете отправить свой запрос на русском, английском, немецком, французском или испанском языках.

Чтобы отправить электронный запрос, вам нужно указать в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

Если вы еще не являетесь зарегистрированным пользователем приложений «Лаборатории Касперского», вы можете заполнить регистрационную форму (https://support.kaspersky.com/ru/personalcabinet/registration/form/). При регистрации укажите *код активации* приложения или *имя файла ключа*.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (https://support.kaspersky.com/ru/PersonalCabinet) и по электронному адресу, который вы указали в запросе.

В веб-форме запроса опишите как можно подробнее возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Вопросы, которые пользователи задают наиболее часто, выделены в отдельные темы, например, «Проблема установки/удаления продукта» или «Проблема поиска/удаления вирусов». Если вы не найдете подходящей темы, выберите «Общий вопрос».
- **Название и номер версии приложения**.
- **Текст запроса**. Опишите как можно подробнее возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

Техническая поддержка по телефону

Если проблема срочная, вы всегда можете позвонить в Службу технической поддержки в вашем городе. Обращаясь к русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержке за помощью, пожалуйста, не забудьте представить необходимую информацию (http://support.kaspersky.ru/support/details). Это поможет нашим специалистам максимально быстро вам помочь.

Обсуждение приложений «Лаборатории Касперского» на веб-форуме

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

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Что нового в Kaspersky Internet Security 2009

Kaspersky Internet Security 2009 – это принципиально новый подход к защите информации. Главное в приложении - это ограничение прав доступа программ к ресурсам системы. Это позволяет предотвратить совершение нежелательных действий подозрительными или опасными программами. Значительно расширены возможности приложения по защите конфиденциальных данных пользователя. В состав приложения включены мастеры и инструменты, значительно облегчающие выполнение специфических задач по защите вашего компьютера.

Рассмотрим детально нововведения Kaspersky Internet Security 2009.

Новое в защите:

- В состав Kaspersky Internet Security включен компонент Фильтрация активности (на стр. 77), совместно с Проактивной защитой (см. раздел «Проактивная защита» на стр. 96) и Сетевым экраном (см. раздел «Сетевой экран» на стр. 87) реализующий новый универсальный подход к защите системы от любых угроз – как уже существующих, так и еще неизвестных. Количество обращений Kaspersky Internet Security

к пользователю значительно уменьшено за счет использования списков доверенных приложений (whitelisting).

- Проверка операционной системы и программного обеспечения на наличие уязвимостей с их последующим устранением поддерживает высокий уровень безопасности системы и тем самым предотвращает проникновение на компьютер вредоносных программ.

- Новые мастеры – Анализ безопасности (на стр. 150) и Настройка браузера (на стр. 151) – облегчают поиск и устранение угроз безопасности и уязвимостей в приложениях, установленных на вашем компьютере, параметрах операционной системы и браузера.

- Скорость реагирования «Лаборатории Касперского» на новые угрозы увеличена за счет использования технологии Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 50), которая собирает данные о заражении компьютеров пользователей и передает ее на серверы «Лаборатории Касперского».

- Новые инструменты – Мониторинг сети (на стр. 149) и Анализ сетевых пакетов (на стр. 152) – облегчают сбор и анализ информации о сетевой активности на вашем компьютере.

- Новый мастер Восстановление после заражения (на стр. 155) помогает устранить повреждения системы после атаки вредоносного программного обеспечения.

Новое в защите конфиденциальных данных:

- Новый компонент Фильтрация активности (на стр. 77) эффективно контролирует доступ приложений к конфиденциальным данным, файлам и папкам пользователя.

- Безопасность конфиденциальных данных, вводимых с клавиатуры, обеспечивается новым инструментом Виртуальная клавиатура (на стр. 158).

- В состав Kaspersky Internet Security входит Мастер устранения следов активности (на стр. 157), удаляющий с компьютера пользователя информацию о его действиях, которые могут заинтересовать злоумышленников (список посещаемых веб-сайтов, открываемых файлов, cookies и т.д.).

Новое в защите от получения нежелательных данных:

- Эффективность фильтрации нежелательной почты компонентом Анти-Спам (на стр. 103) повышена за счет использования серверных технологий Recent Terms.

- Использование модулей расширения почтовых клиентов Microsoft Office Outlook, Microsoft Outlook Express, The Bat! и Thunderbird упрощает настройку параметров защиты от спама.

- Усовершенствованный компонент Родительский контроль (на стр. 124) позволяет существенно ограничить доступ детей к нежелательным интернет-ресурсам.

Новое в защите при работе в интернете:

- Улучшена защита от интернет-мошенников за счет расширения баз фишинговых сайтов.

- Добавлена проверка трафика ICQ и MSN, что обеспечивает безопасность работы с интернет-пейджерами.

- Безопасность при работе в беспроводных сетях обеспечивается за счет проверки Wi-Fi-соединений.

Новое в интерфейсе приложения:

- Новый интерфейс Kaspersky Internet Security отражает комплексный подход к защите информации.

- Высокая информативность диалоговых окон помогает пользователю быстро принимать правильные решения.

- Расширена функциональность отчетов и статистической информации о работе приложения. Возможность применения гибко настраиваемых фильтров при работе с отчетами делает продукт незаменимым для профессионалов.

Концепция защиты приложения

Kaspersky Internet Security обеспечивает защиту вашего компьютера от известных и новых угроз, хакерских и мошеннических атак, спама и других нежелательных данных. Каждый тип угроз обрабатывается отдельным компонентом приложения. Такое построение системы защиты позволяет гибко настраивать приложение под нужды конкретного пользователя или предприятия в целом.

Kaspersky Internet Security включает:

- Контроль активности приложений (см. раздел «Контроль приложений» на стр. 77) в системе, предотвращающий выполнение приложениями опасных действий.

- Компоненты защиты от вредоносного ПО (см. раздел «Защита от вредоносного ПО» на стр. 54), обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации в режиме реального времени.

- Компоненты защиты во время работы в интернете (см. раздел «Онлайн-защита» на стр. 99), обеспечивающие защиту вашего компьютера от известных на данный момент сетевых и мошеннических атак.

- Компоненты фильтрации нежелательных данных, (см. раздел «Фильтр содержимого» на стр. 103) помогающие экономить время, веб-трафик и деньги.

- Задачи проверки на вирусы (см. раздел «Проверка на вирусы» на стр. 131), посредством которых выполняется поиск вирусов в отдельных файлах, папках, дисках или областях, либо полная проверка компьютера. Задачи поиска можно настроить для обнаружения уязвимостей в установленных на компьютере приложениях.

- Обновление (на стр. 142), обеспечивающее актуальность внутренних модулей приложения, а также баз, использующихся для поиска вредоносных программ, обнаружения хакерских атак и спам-сообщений.

- Мастеры и инструменты (на стр. 13), облегчающие выполнение задач, возникающих в процессе работы Kaspersky Internet Security.

- Сервисные функции (на стр. 14), обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить его функциональность.

Мастеры и инструменты

Обеспечение безопасности компьютера - непростая задача, требующая знаний об особенностях работы операционной системы и о способах использования ее слабых мест. Кроме этого, большое количество и разнородность информации о безопасности системы затрудняет ее анализ и обработку.

Для облегчения решения специфических задач по обеспечению безопасности компьютера в состав Kaspersky Internet Security включен ряд мастеров и инструментов:

- Мастер Анализа безопасности (см. раздел «Анализ безопасности» на стр. 150), выполняющий диагностику безопасности компьютера и поиск уязвимостей в операционной системе и программах, установленных на компьютере.

- Мастер Настройки браузера (см. раздел «Настройка браузера» на стр. 151), выполняющий анализ параметров браузера Microsoft Internet Explorer, оценивая их в первую очередь с точки зрения безопасности.

- Мастер Восстановления после заражения (см. раздел «Восстановление после заражения» на стр. 155), устраняющий следы пребывания в системе вредоносных объектов.

- Мастер Устранения следов активности (на стр. 157), производящий поиск и устранение следов активности пользователя в системе и параметров операционной системы, способствующих накоплению информации об активности пользователя.

- Мастер создания Диска аварийного восстановления (см. раздел «Диск аварийного восстановления» на стр. 155), предназначенный для восстановления работоспособности системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка.

- Анализ сетевых пакетов (на стр. 152), перехватывающий сетевые пакеты и отображающий подробную информацию о них.

- Мониторинг сети (на стр. 149), предоставляющий подробную информацию о сетевой активности на вашем компьютере.

- Виртуальная клавиатура (на стр. 158), предотвращающая перехват данных, вводимых с клавиатуры.

СЕРВИСНЫЕ ФУНКЦИИ

Kaspersky Internet Security включает ряд сервисных функций. Они предусмотрены для поддержки защиты компьютера в актуальном состоянии, расширения возможностей использования приложения, для оказания помощи в работе.

Kaspersky Security Network

Kaspersky Security Network - система автоматической передачи отчетов об обнаруженных и потенциальных угрозах в централизованную базу данных. Эта база данных позволяет еще быстрее реагировать на наиболее распространенные угрозы и оповещать пользователей об эпидемиях.

Лицензия

При покупке Kaspersky Internet Security между вами и «Лабораторией Касперского» заключается лицензионное соглашение, на основе которого вы можете использовать приложение и получать доступ к обновлению баз приложения и Службе технической поддержки в течение определенного временного периода. Срок использования, а также другая информация, необходимая для полнофункциональной работы приложения, указана в лицензии.

Пользуясь функцией **Лицензия**, вы можете получать подробную информацию об используемой вами лицензии, а также приобретать новую лицензию или продлевать действие текущей.

Поддержка

Все зарегистрированные пользователи Kaspersky Internet Security могут воспользоваться Службой технической поддержки. Для того чтобы узнать о том, где именно вы можете получить техническую поддержку, воспользуйтесь функцией **Поддержка**.

С помощью соответствующих ссылок вы можете перейти на форум пользователей продуктов «Лаборатории Касперского», а также отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе приложения, заполнив специальную форму на сайте.

Также для вас доступна Служба технической поддержи онлайн, сервисы Персонального кабинета пользователя и, конечно, наши сотрудники всегда готовы вам помочь в работе с Kaspersky Internet Security по телефону.

ЭВРИСТИЧЕСКИЙ АНАЛИЗ

Методы эвристического анализа используются в работе некоторых компонентов защиты, например, Файлового Антивируса, Почтового Антивируса и Веб-Антивируса, а также задач проверки на вирусы.

Известно, что проверка на основе сигнатурного метода с использованием сформированных заранее баз, содержащих описание известных угроз и методов их лечения, дает однозначный ответ, является ли

проверяемый объект вредоносным, а также к какому классу опасных программ он относится. Эвристический метод, в отличие от сигнатурного метода, нацелен на обнаружение не сигнатур вредоносного кода, а типичных последовательностей операций, позволяющих сделать вывод о природе файла с достаточной долей вероятности.

Преимуществом эвристического анализа является то, что для его работы не требуется наличие предварительно составленных баз. За счет этого новые угрозы распознаются до того, как их активность становится известна вирусным аналитикам.

Однако, существуют способы обхода эвристических методов. Одним из вариантов такой защиты является заморозка активности вредоносного кода в момент обнаружения применения эвристических методов проверки.

Использование комбинации различных методов проверки обеспечивает большую безопасность работы.

При подозрении на угрозу эвристический анализатор эмулирует выполнение объекта в безопасном виртуальном окружении приложения. В случае если при его выполнении будут обнаружены подозрительные действия, объект будет признан вредоносным и его запуск на компьютере будет заблокирован либо на экран будет выведено уведомление с запросом дальнейших действий у пользователя:

- поместить угрозу на карантин для последующей проверки и обработки с помощью обновленных баз;
- удалить объект;
- пропустить, если вы абсолютно уверены, что данный объект не может являться вредоносным.

Для использования методов эвристики установите флажок **Использовать эвристический анализатор**. Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте бегунок в одну из позиций: поверхностный, средний или глубокий. Уровень детализации проверки представляет собой баланс между тщательностью поиска новых угроз и степенью загрузки ресурсов операционной системы. Чем выше установленный уровень эвристики, тем больше ресурсов системы требует проверка, и тем больше времени она занимает.

Новые угрозы, обнаруживаемые с помощью эвристического анализа, оперативно анализируются специалистами «Лаборатории Касперского» и методы их лечения заносятся в ежечасно обновляемые базы Kaspersky Internet Security.

Если вы регулярно выполняете обновление баз приложения, то вы поддерживаете оптимальный уровень защиты компьютера.

Аппаратные и программные требования к системе

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

Общие требования:

- 75 МБ свободного места на жестком диске.
- CD-ROM (для установки приложения с дистрибутивного CD-диска).
- Устройство ввода, манипулятор типа «мышь».
- Microsoft Internet Explorer 5.5 или выше (для обновления баз и модулей приложения через интернет).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (пакет обновлений 2 или выше), Microsoft Windows XP Professional (пакет обновлений 2 или выше), Microsoft Windows XP Professional x64 Edition (пакет обновлений 2 или выше):

- Процессор Intel Pentium 300 МГц или выше (или совместимый аналог).
- 256 МБ свободной оперативной памяти.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

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

УГРОЗЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Большую часть угроз компьютерной безопасности представляют угрозы-программы. Кроме них опасность может представлять спам, фишинг, хакерские атаки, рекламные баннеры. Эти угрозы связаны с использованием интернета.

В ЭТОМ РАЗДЕЛЕ

Угрозы-программы

Kaspersky Internet Security способно обнаруживать на компьютере сотни тысяч опасных программ. Некоторые из этих программ представляют большую опасность для компьютера пользователя, другие опасны только при выполнении некоторых условий. Обнаружив опасную программу, приложение классифицирует ее и присваивает ей уровень опасности (высокий или средний).

Вирусные аналитики «Лаборатории Касперского» выделяют две основных категории: *вредоносные программы* и *потенциально нежелательные программы*.

Вредоносные программы (на стр. 17) (Malware) созданы специально для того, чтобы наносить вред компьютерам и их пользователям, например, красть, блокировать, изменять или уничтожать информацию, нарушать работу компьютеров или компьютерных сетей.

Потенциально нежелательные программы (на стр. 24) (PUPs (Potentially unwanted programs)) в отличие от вредоносных не предназначены специально для того, чтобы нанести вред, однако с их помощью можно нарушать компьютерную безопасность.

Вирусная энциклопедия (http://www.viruslist.com/ru/viruses/encyclopedia) содержит подробное описание этих программ.

Вредоносные программы

Вредоносные программы созданы специально для того, чтобы наносить вред компьютерам и их пользователям: красть, блокировать, изменять или уничтожать информацию, нарушать работу компьютеров или компьютерных сетей.

Вредоносные программы делят на три подкатегории: *вирусы и черви*, *троянские программы* и *вредоносные утилиты*.

Вирусы и черви (на стр. 18) (Viruses_and_Worms) могут создавать свои копии, обладающие способностью дальнейшего самовоспроизведения. Некоторые из них запускаются без участия пользователя, другие требуют действий пользователя, чтобы запустить их. Эти программы начинают выполнять свое вредоносное действие при запуске.

Троянские программы (на стр. 19) (Trojan_programs) в отличие от червей и вирусов не создают свои копии. Они проникают на компьютер, например, через электронную почту или через веб-браузер, когда пользователь посещает «зараженную» веб-страницу. Для запуска они требуют действий пользователя; они начинают выполнять свое вредоносное действие при запуске.

Вредоносные утилиты (на стр. 22) (Malicious_tools) специально созданы для того, чтобы наносить вред. Но в отличие от других вредоносных программ они не выполняют вредоносных действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Эти программы имеют функции, которые используют для изготовления вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, «взлома» компьютеров или других вредоносных действий.

Вирусы и черви

Подкатегория: вирусы и черви (Viruses_and_Worms)

Уровень опасности: высокий

Классические вирусы и черви выполняют на компьютере действия, не разрешенные пользователем, и могут создавать свои копии, которые обладают способностью дальнейшего самовоспроизведения.

Классический вирус

Попав в систему, классический вирус заражает какой-либо файл, активизируется в нем, выполняет свое вредоносное действие, а затем добавляет свои копии в другие файлы.

Классический вирус размножается только на локальных ресурсах компьютера; он не может самостоятельно проникать на другие компьютеры. Он может попасть на другой компьютер только в случае, если добавит свою копию в файл, который хранится в папке общего доступа или на установленном компакт-диске, или если пользователь сам перешлет электронное письмо с вложенным в него зараженным файлом.

Код классического вируса может внедряться в различные области компьютера, операционной системы или приложения. По среде обитания вирусы различают на *файловые*, *загрузочные*, *скриптовые* и *макро-вирусы*.

Вирусы могут заражать файлы различными способами. *Перезаписывающие* (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожив его содержимое. Зараженный файл перестает работать и не лечится. *Паразитические* (Parasitic) вирусы изменяют файлы, оставляя их полностью или частично работоспособными. *Вирусы-компаньоны* (Companion) не изменяют файлы, но создают их двойники. При открытии зараженного файла запускается его двойник, то есть вирус. Есть *вирусы-ссылки* (Link), вирусы, *заражающие объектные модули* (OBJ), вирусы, *заражающие библиотеки компиляторов* (LIB), вирусы, *заражающие исходные тексты программ* и другие.

Червь

Код червя, как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Но свое название червь получил благодаря способности «переползать» с компьютера на компьютер – без разрешения пользователя распространять свои копии через различные информационные каналы.

Основным признаком, по которому черви различаются между собой, является способ распространения. Описание типов червей по способу распространения приводится в следующей таблице.

Таблица 1. Черви по способу распространения

Тип	Название	Описание
Email-Worm	Почтовые черви	Распространяются через электронную почту. Зараженное письмо содержит прикрепленный файл с копией червя или ссылку на такой файл на веб-сайте, например, взломанном или хакерском. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие электронные адреса и отправляя по ним зараженные сообщения.

Тип	Название	Описание
IM-Worm	Черви интернет-пейджеров	Распространяются через интернет-пейджеры (системы мгновенного обмена сообщениями), такие как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager или Skype. Обычно такой червь рассылает по контакт-листам сообщения, в которых есть ссылка на файл с его копией на веб-сайте. Когда пользователь загружает файл и открывает его, червь активизируется.
IRC-Worm	Черви интернет-чатов	Распространяются через ретранслируемые интернет-чаты (Internet Relay Chats) – сервисные системы, с помощью которых можно общаться через интернет с другими людьми в реальном времени. Такой червь публикует в интернет-чате файл со своей копией или ссылку на файл. Когда пользователь загружает файл и открывает его, червь активизируется.
Net-Worm	Сетевые черви (черви компьютерных сетей)	Распространяются через компьютерные сети. В отличие от червей других типов, сетевой червь распространяется без участия пользователя. Он ищет в локальной сети компьютеры, на которых используются программы, содержащие уязвимости. Для этого он посылает специально сформированный сетевой пакет (эксплойт), который содержит код червя или его часть. Если в сети находится «уязвимый» компьютер, то этот компьютер принимает сетевой пакет. Полностью проникнув на компьютер, червь активизируется.
P2P-Worm	Черви файлообменных сетей	Распространяются через файлообменные пиринговые сети, такие как Kazaa, Grokster, EDonkey, FastTrack или Gnutella. Чтобы внедриться в файлообменную сеть, червь копирует себя в каталог обмена файлами, обычно расположенный на компьютере пользователя. Файлообменная сеть отображает информацию об этом файле, и пользователь может «найти» зараженный файл в сети, как и любой другой, загрузить его и открыть. Более сложные черви имитируют сетевой протокол конкретной файлообменной сети: они отвечают положительно на поисковые запросы и предлагают для загрузки свои копии.
Worm	Прочие черви	К прочим сетевым червям относятся: • Черви, которые распространяют свои копии через сетевые ресурсы. Используя функции операционной системы, они перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный доступ. В отличие от червей компьютерных сетей, пользователю нужно открыть файл с копией червя, чтобы активизировать его. • Черви, которые не обладают ни одним из описанных в этой таблице способов распространения (например, распространяются через мобильные телефоны).

Троянские программы

Подкатегория: троянские программы (Trojan_programs)

Уровень опасности: высокий

В отличие от червей и вирусов, троянские программы не создают свои копии. Они проникают на компьютер, например, через электронную почту или через веб-браузер, когда пользователь посещает «зараженную» веб-страницу. Троянские программы запускаются при участии пользователя; они начинают выполнять свое вредоносное действие при запуске.

Разные троянские программы ведут себя на зараженном компьютере по-разному. Основными функциями «троянцев» является блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Кроме этого, троянские программы могут принимать или отправлять файлы, выполнять

их, выводить на экран сообщения, обращаться к веб-страницам, загружать и устанавливать программы, перезагружать компьютер.

Злоумышленники часто используют «наборы» из разных троянских программ.

Типы троянских программ по их поведению описаны в следующей таблице.

Таблица 2. Типы троянских программ по поведению на зараженном компьютере

Тип	Название	Описание
Trojan-ArcBomb	Троянские программы - «архивные бомбы»	Архивы; при распаковке увеличиваются до таких размеров, что нарушают работу компьютера. Как только вы попытаетесь распаковать такой архив, компьютер может начать работать медленно или «зависнуть», диск может заполниться «пустыми» данными. «Архивные бомбы» особенно опасны для файловых и почтовых серверов. Если на сервере используется система автоматической обработки входящей информации, такая «архивная бомба» может остановить сервер.
Backdoor	Троянские программы удаленного администрирования	Считаются наиболее опасными среди троянских программ; по функциям напоминают программы удаленного администрирования, которые есть в свободной продаже. Эти программы устанавливают себя в компьютере незаметно для пользователя и позволяют злоумышленнику удаленно управлять компьютером.
Trojan	Троянские программы	Включают следующие вредоносные программы: • **классические троянские программы**; они выполняют только основные функции троянских программ: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей; они не имеют дополнительных функций, свойственных другим типам троянских программ, описанным в этой таблице; • **«многоцелевые» троянские программы**; они имеют дополнительные функции, присущие сразу нескольким типам троянских программ.
Trojan-Ransom	Троянские программы, требующие выкупа	«Берут в заложники» информацию на компьютере пользователя, изменяя или блокируя ее, или нарушают работу компьютера таким образом, чтобы пользователь не мог воспользоваться информацией. Злоумышленник требует от пользователя выкуп за обещание выслать программу, которая восстановит работоспособность компьютера и данные на нем.
Trojan-Clicker	Троянские программы-кликеры	С компьютера пользователя обращаются к веб-страницам: они или сами посылают команды веб-браузеру, или заменяют хранящиеся в системных файлах веб-адреса. С помощью этих программ злоумышленники организовывают сетевые атаки, повышают посещаемость сайтов, чтобы увеличить количество показов рекламных баннеров.
Trojan-Downloader	Троянские программы-загрузчики	Обращаются к веб-странице злоумышленника, загружают с нее другие вредоносные программы и устанавливают их на компьютере пользователя; могут хранить имя файла загружаемой вредоносной программы в себе или получать его с веб-страницы, к которой обращаются.

Тип	Название	Описание
Trojan-Dropper	Троянские программы-установщики	Сохраняют на диске компьютера, а затем устанавливают другие троянские программы, которые хранятся в теле этих программ. Злоумышленники могут использовать троянские программы-установщики, чтобы: • установить вредоносную программу незаметно для пользователя: троянские программы-установщики не отображает никаких сообщений или отображает ложные сообщения, например, об ошибке в архиве или неверной версии операционной системы; • защитить от обнаружения другую известную вредоносную программу: не все антивирусы могут распознать вредоносную программу внутри троянской программы-установщика.
Trojan-Notifier	Троянские программы-уведомители	Сообщают злоумышленнику о том, что зараженный компьютер находится «на связи»; передают ему информацию о компьютере: IP-адрес, номер открытого порта или адрес электронной почты. Они связываются со злоумышленником по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. Троянские программы-уведомители часто используются в наборах из разных троянских программ. Они извещают злоумышленника о том, что другие троянские программы успешно установлены на компьютере пользователя.
Trojan-Proxy	Троянские программы-прокси	Позволяют злоумышленнику анонимно обращаться через компьютер пользователя к веб-страницам; часто используются для рассылки спама.
Trojan-PSW	Троянские программы, крадущие пароли	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей, например, регистрационную информацию к программному обеспечению. Они отыскивают конфиденциальную информацию в системных файлах и реестре и пересылают ее «хозяину» по электронной почте, через FTP, обращаясь к веб-странице злоумышленника или другим способом. Некоторые из этих троянских программ выделены в отдельные типы, описанные в этой таблице. Это троянские программы, крадущие банковские счета (Trojan-Banker), троянские программы, крадущие данные пользователей интернет-пейджеров (Trojan-IM) и троянские программы, крадущие данные пользователей сетевых игр (Trojan-GameThief).
Trojan-Spy	Троянские программы-шпионы	Ведут электронный шпионаж за пользователем: собирают информацию о его действиях на компьютере, например, перехватывают данные, которые пользователь вводит с клавиатуры, делают снимки экрана или собирают списки активных приложений. Получив эту информацию, они передают ее злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-DDoS	Троянские программы-сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании). Такими программами часто заражают многие компьютеры, чтобы с них одновременно атаковать один сервер.

Тип	Название	Описание
Trojan-IM	Троянские программы, крадущие данные пользователей интернет-пейджеров	Крадут номера и пароли пользователей интернет-пейджеров (систем мгновенного обмена сообщениями), таких как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager или Skype. Передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Rootkit	Руткиты	Скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в системе; могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра, которые запускают вредоносные программы; скрывать обмен данными между приложениями на компьютере пользователя и других компьютерах в сети.
Trojan-SMS	Троянские программы-SMS-сообщения	Заражают мобильные телефоны и с них отправляют SMS-сообщения на платные номера.
Trojan-GameThief	Троянские программы, крадущие данные пользователей сетевых игр	Крадут данные учетных записей пользователей сетевых компьютерных игр; передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Banker	Троянские программы, крадущие банковские счета	Крадут данные банковских счетов или счетов в системах электронных денег; передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Mailfinder	Троянские программы-сборщики электронных адресов	Собирают адреса электронной почты на компьютере и передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. По собранным адресам злоумышленники могут рассылать спам.

Вредоносные утилиты

Подкатегория: вредоносные утилиты (Malicious_tools)

Уровень опасности: средний

Вредоносные утилиты созданы специально для того, чтобы наносить вред. Но в отличие от других вредоносных программ они не выполняют вредоносных действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Эти программы имеют функции, которые используют для изготовления вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, «взлома» компьютеров или других вредоносных действий.

Вредоносные утилиты разнообразны по своим функциям. Их типы описаны в следующей таблице.

Таблица 3. Вредоносные утилиты по функциям

Тип	Название	Описание
Constructor	Конструкторы	Позволяют создавать новые вирусы, черви и троянские программы. Некоторые конструкторы имеют стандартный оконный интерфейс, в котором с помощью меню можно выбирать тип создаваемой вредоносной программы, способ ее противодействия отладчику и другие свойства.

Тип	Название	Описание
Dos	Сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании).
Exploit	Эксплойты	Эксплойт – это набор данных или программный код, использующий уязвимости приложения, в котором он обрабатывается, чтобы выполнить на компьютере вредоносное действие. Например, эксплойт может записывать или считывать файлы или обращаться к «зараженным» веб-страницам. Разные эксплойты используют уязвимости разных приложений или сетевых служб. Эксплойт в виде сетевого пакета передается по сети на многие компьютеры, выискивая компьютеры с уязвимыми сетевыми службами. Эксплойт в файле DOC использует уязвимости текстового редактора. Он может начать выполнять заложенные злоумышленником функции, когда пользователь откроет зараженный файл. Эксплойт, внедренный в сообщение электронной почты, ищет уязвимости в какой-либо почтовой программе; он может начать выполнять вредоносное действие, как только пользователь откроет зараженное сообщение в этой программе. С помощью эксплойтов распространяются сетевые черви (Net-Worm). Эксплойты *ньюкеры* (Nuker) представляют собой сетевые пакеты, которые выводят компьютеры из строя.
FileCryptor	Шифровальщики	Шифруют другие вредоносные программы, чтобы скрыть их от антивирусного приложения.
Flooder	Программы для «замусоривания» сетей	Рассылают многочисленные сообщения по сетевым каналам. К ним относятся, например, программы для замусоривания ретранслируемых интернет-чатов (Internet Relay Chats). К ним не относятся программы, «забивающие мусором» каналы электронной почты, интернет-пейджеров и мобильных систем. Эти программы выделяют в отдельные типы, описанные в этой таблице (Email-Flooder, IM-Flooder и SMS-Flooder).
HackTool	Инструменты хакера	Позволяют взламывать компьютер, на котором установлены или атаковать другой компьютер (например, без разрешения пользователя добавлять других пользователей системы; очищать системные журналы, чтобы скрыть следы присутствия в системе). К ним относят некоторые снифферы, которые обладают вредоносными функциями, например перехватывают пароли. Снифферы (Sniffers) – это программы, которые позволяют просматривать сетевой трафик.
not-virus:Hoax	Злые шутки	Пугают пользователя вирусоподобными сообщениями: могут обнаружить вирус в незараженном файле или объявлять о форматировании диска, которого на самом деле не происходит.
Spoofer	Утилиты-имитаторы	Отправляют сообщения и сетевые запросы с поддельным адресом отправителя. Злоумышленники используют утилиты-имитаторы, чтобы, например, выдать себя за отправителя.
VirTool	Инструменты для модификации вредоносных программ	Позволяют модифицировать другие вредоносные программы так, чтобы скрыть их от антивирусных приложений.
Email-Flooder	Программы для «замусоривания» адресов электронной почты	Отправляют многочисленные сообщения по адресам электронной почты («забивают их мусором»). Большой поток сообщений не дает пользователям просматривать полезную входящую почту.

Тип	Название	Описание
IM-Flooder	Программы для «замусоривания» интернет-пейджеров	Отправляют многочисленные сообщения пользователям интернет-пейджеров (систем мгновенного обмена сообщениями), таких как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager или Skype. Большой поток сообщений не дает пользователям просматривать полезные входящие сообщения.
SMS-Flooder	Программы для «замусоривания» смс-сообщениями	Отправляют многочисленные смс-сообщения на мобильные телефоны.

ПОТЕНЦИАЛЬНО НЕЖЕЛАТЕЛЬНЫЕ ПРОГРАММЫ

Потенциально нежелательные программы, в отличие от вредоносных, не предназначены специально для того, чтобы нанести вред. Однако с их помощью можно нарушать компьютерную безопасность.

К потенциально нежелательным относятся *программы рекламного характера*, *программы порнографического характера* и *другие потенциально нежелательные программы*.

Программы рекламного характера (на стр. 24) (Adware) связаны с показом пользователю рекламной информации.

Программы порнографического характера (на стр. 24) (Pornware) связаны с показом пользователю информации порнографического характера.

Другие потенциально нежелательные программы (на стр. 25) (Riskware) – это чаще всего полезные программы, которыми многие пользуются. Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать их функции, чтобы нарушать безопасность.

Потенциально нежелательные программы устанавливаются одним из следующих способов:

- Их устанавливает сам пользователь, отдельно или в составе другой программы (например, производители включают программы рекламного характера в бесплатное или условно-бесплатное программное обеспечение).
- Их устанавливают злоумышленники, например, включают их в пакеты с другими вредоносными программами, используют «уязвимости» веб-браузера или троянские программы-загрузчики и установщики.

ПРОГРАММЫ РЕКЛАМНОГО ХАРАКТЕРА

Подкатегория: программы рекламного характера (Adware)

Уровень опасности: средний

Программы рекламного характера связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них также собирают и переправляют своему разработчику маркетинговую информацию о пользователе, например, какие тематические сайты он посещает, какие поисковые запросы делает (в отличие от троянских программ-шпионов, они передают эту информацию с разрешения пользователя).

ПРОГРАММЫ ПОРНОГРАФИЧЕСКОГО ХАРАКТЕРА

Подкатегория: программы порнографического характера (Pornware)

Уровень опасности: средний

Обычно пользователи сами устанавливают такие программы, чтобы искать и загружать порнографическую информацию.

Злоумышленники также могут устанавливать такие программы на компьютере пользователя, чтобы без его разрешения показывать рекламу платных порнографических сайтов и сервисов. Для установки они используют уязвимости операционной системы или веб-браузера, троянские программы-загрузчики и программы-установщики.

Выделяют три типа программ порнографического характера по их функциям. Эти типы описаны в таблице.

Таблица 4. Типы программ порнографического характера по функциям

Тип	Название	Описание
Porn-Dialer	Программы автодозвона	Дозваниваются до порнографических телефонных служб (хранят в себе их телефонные номера); в отличие от троянских программ автодозвона уведомляют пользователя о своих действиях.
Porn-Downloader	Программы для загрузки файлов из интернета	Загружают на компьютер данные порнографического характера; в отличие от троянских программ автодозвона уведомляют пользователя о своих действиях.
Porn-Tool	Инструменты	Позволяют искать и отображать порнографические материалы; к ним относят специальные панели инструментов для браузеров или особые видеоплееры.

Другие потенциально нежелательные программы

Подкатегория: другие потенциально нежелательные программы (Riskware)

Уровень опасности: средний

Большинство этих программ являются полезными, ими многие пользуются. Среди них программы-клиенты IRC, программы автодозвона (Dialers), программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Однако, если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции, чтобы нарушать безопасность.

Другие потенциально нежелательные программы различают по функциям. Их типы описаны в таблице.

Таблица 5. Типы других потенциально нежелательных программ по функциям

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона, «звонилки»	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (смотреть, какие приложения работают, как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.

Тип	Название	Описание
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники для наблюдения за удаленными компьютерами и управления ими. Потенциально нежелательные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; потенциально нежелательные программы этими функциями не обладают.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют электронные сообщения в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы; они выводят сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

КАК KASPERSKY INTERNET SECURITY ОБНАРУЖИВАЕТ ЗАРАЖЕННЫЕ, ПОДОЗРИТЕЛЬНЫЕ И ПОТЕНЦИАЛЬНО ОПАСНЫЕ ОБЪЕКТЫ

Kaspersky Internet Security обнаруживает вредоносные программы в объектах двумя методами: *реактивным* (с использованием баз) и *проактивным* (с использованием эвристического анализа).

Базы представляют собой файлы с записями, которые позволяют идентифицировать наличие в проверяемых объектах сотен тысяч известных вредоносных программ. Эти записи содержат информацию о контрольных

участках кода вредоносных программ и алгоритмы лечения объектов, в которых эти программы содержатся. Вирусные аналитики «Лаборатории Касперского» ежедневно обнаруживают сотни новых вредоносных программ, создают идентифицирующие их записи и включают их в обновления баз.

Если Kaspersky Internet Security обнаруживает в проверяемом объекте участки кода, которые полностью совпадают с контрольными участками кода какой-либо вредоносной программы в соответствии с информацией о них в базе, оно признает такой объект *зараженным*, а если совпадает частично (в соответствии с определенными условиями) - *подозрительным*.

С помощью проактивного метода удается обнаружить самые новые вредоносные программы, информации о которых еще нет в базах.

Kaspersky Internet Security распознает объекты, содержащие новые вредоносные программы по их поведению. Нельзя сказать, что код такого объекта частично или полностью совпадает с кодом известной вредоносной программы, но он содержит свойственные вредоносным программам последовательности команд, такие как открытие файла или запись в файл или перехват векторов прерываний. Приложение определяет, например, что файл выглядит как зараженный неизвестным вирусом.

Объекты, обнаруженные проактивным методом, называются *потенциально опасными*.

Интернет-угрозы

Приложение «Лаборатории Касперского» использует специальные технологии, чтобы предупредить следующие угрозы компьютерной безопасности:

- спам, или нежелательная входящая почта;
- фишинг (на стр. 27);
- сетевые атаки (на стр. 28);
- показ баннеров (на стр. 28).

Спам или нежелательная входящая почта

Приложение «Лаборатории Касперского» защищает пользователей от спама. Спамом называется нежелательная входящая почта, часто рекламного характера. Спам нагружает каналы и почтовые серверы провайдера. Получатель оплачивает созданный спамом трафик, а обычная почта проходит медленнее. В результате во многих странах рассылка спама является противозаконной.

Приложение «Лаборатории Касперского» проверяет входящие сообщения Microsoft Office Outlook, Microsoft Outlook Express, The Bat! и Thunderbird, и если оно распознает какое-либо сообщение как спам, то выполняет выбранные вами действия, например, переносит в отдельную папку или удаляет. Также возможна проверка сообщений на трафике по протоколам POP3 и IMAP с добавлением соответствующих тегов в тему письма.

Приложение «Лаборатории Касперского» распознает спам с высокой точностью. Он применяет сразу несколько технологий фильтрации спама: определяет спам по адресу отправителя, словам и выражениям в заголовке и тексте сообщения; распознает спам в виде изображений и использует самообучающийся алгоритм для распознавания спама по тексту сообщения.

Базы Анти-Спама содержат «черный» и «белый» списки адресов отправителей, списки слов и выражений, которые относятся к различным спам-категориям, таким как реклама, медицина и здоровье, азартные игры и другие.

Фишинг

Фишинг (phishing) - это вид интернет-мошенничества, который заключается в «выуживании» у пользователей номеров их кредитных карт, пин-кодов и других личных данных с целью кражи у них денежных средств.

Фишинг часто связан с интернет-банкинком. Злоумышленники создают точную копию сайта выбранного банка, затем рассылают от имени этого банка письма его клиентам. Они сообщают о том, что из-за выхода из строя или смены программного обеспечения в системе интернет-банкинка утеряны учетные данные пользователя, и он должен подтвердить или изменить их на сайте банка. Пользователь щелкает по ссылке, ведущей на созданный злоумышленниками веб-сайт, и вводит там свои данные.

Базы Анти-Фишинга содержат список URL-адресов сайтов, которые известны как используемые для фишинг-атак.

Приложение «Лаборатории Касперского» просматривает входящие сообщения Microsoft Office Outlook и Microsoft Outlook Express и если обнаруживает в каком-либо из них ссылку на URL-адрес, который есть в базах, то помечает такое письмо как спам. А если пользователь открывает сообщение и пытается перейти по ссылке, приложение блокирует страницу.

СЕТЕВЫЕ АТАКИ

Сетевая атака - это вторжение в систему на удаленном компьютере, чтобы захватить управление на ней, привести ее к отказу в обслуживании, или получить доступ к защищенной информации.

Сетевыми атаками называют как действия злоумышленников (например, сканирование портов, подбор паролей), так и вредоносные программы, которые исполняют команды от имени пользователя, передают информацию своему «хозяину» или выполняют другие функции сетевых атак. К ним относят некоторые троянские программы, DoS-атаки, вредоносные скрипты, разновидности сетевых червей.

Сетевые атаки распространяются в локальных или глобальных сетях через уязвимости в операционных системах и приложениях. Они передаются как отдельные IP-пакеты данных во время сетевых соединений.

Kaspersky Internet Security останавливает сетевые атаки, не нарушая сетевых соединений. Он использует специальные базы Сетевого экрана. Эти базы содержат записи, которые идентифицируют IP-пакеты данных, характерные для разных хакерских программ. Приложение анализирует сетевые соединения и блокирует в них IP-пакеты, которые признает опасными.

ПОКАЗ БАННЕРОВ

Баннеры, или рекламные объявления, которые являются ссылкой на веб-сайт рекламодателя, бывают чаще всего в виде изображений. Их показ на веб-странице не является угрозой компьютерной безопасности, но считается помехой нормальной работе на компьютере. Мелькание баннеров на экране ухудшает условия работы, снижая производительность. Пользователя отвлекает информация, не относящаяся к делу. Переходы по баннерам повышают интернет-трафик.

Многие организации применяют исключение баннеров из интерфейса как часть политики безопасности.

Kaspersky Internet Security блокирует баннеры по URL-адресу страницы, на которую указывает баннер. Он использует обновляемые базы Анти-Баннера, содержащие список URL-адресов российских и зарубежных баннерных сетей. Приложение просматривает ссылки на загружаемой веб-странице, сравнивает их адреса с адресами в базах и, если находит какой-либо из них, то удаляет ссылку на этот адрес со страницы и продолжает загружать страницу.

УСТАНОВКА KASPERSKY INTERNET SECURITY НА КОМПЬЮТЕР

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

Перед началом установки рекомендуется закрыть все работающие приложения.

Чтобы установить Kaspersky Internet Security на ваш компьютер, на CD-диске с продуктом запустите файл дистрибутива (файл с расширением *.exe).

Установка приложения с дистрибутива, полученного через интернет, полностью совпадает с установкой приложения с дистрибутивного CD-диска.

После этого будет произведен поиск установочного пакета приложения (файл с расширением *.msi) и, если он присутствует, будет произведен поиск более новой версии на серверах «Лаборатории Касперского» в интернете. Если файл установочного пакета не найден, вам будет предложено загрузить его. По окончании загрузки будет запущена установка Kaspersky Internet Security. В случае отказа от загрузки установка приложения будет продолжена в обычном режиме.

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Кратко поясним их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.
- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки продукта.
- **Готово** – завершить процедуру установки приложения на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

В ЭТОМ РАЗДЕЛЕ

ШАГ 1. ПОИСК БОЛЕЕ НОВОЙ ВЕРСИИ ПРИЛОЖЕНИЯ

Прежде чем устанавливать Kaspersky Internet Security на ваш компьютер, выполняется обращение к серверам обновлений «Лаборатории Касперского» и проверка наличия более новой версии устанавливаемого приложения.

Если более новой версии приложения 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 скачать и установить ее на 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 приложения.

ШАГ 2. ПРОВЕРКА СООТВЕТСТВИЯ СИСТЕМЫ НЕОБХОДИМЫМ УСЛОВИЯМ УСТАНОВКИ

Перед установкой Kaspersky Internet Security на вашем компьютере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки (см. раздел «Аппаратные и программные требования к системе» на стр. 15). Также проверяется наличие на вашем компьютере требуемых программ и ваши права на установку программного обеспечения.

В случае если какое-либо из требований не выполнено, на экран будет выведено соответствующее уведомление. Рекомендуется установить требуемые пакеты обновлений посредством сервиса **Windows Update** и необходимые программы перед установкой приложения «Лаборатории Касперского».

ШАГ 3. ПРИВЕТСТВИЕ МАСТЕРА УСТАНОВКИ

Если ваша система полностью соответствует предъявляемым требованиям (см. раздел «Аппаратные и программные требования к системе» на стр. 15), более новой версии приложения на серверах обновлений «Лаборатории Касперского» не обнаружено или вы отказались от установки более новой версии, на вашем

компьютере запускается мастер установки текущей версии Kaspersky Internet Security. На экране будет открыто стартовое окно мастера установки, содержащее информацию о начале установки приложения на ваш компьютер.

Для продолжения установки нажмите на кнопку **Далее**. Отказ от установки выполняется по кнопке **Отмена**.

Шаг 4. Просмотр лицензионного соглашения

Следующее окно мастера установки содержит лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Внимательно прочтите его, и, при условии, что вы согласны со всеми пунктами соглашения, выберите вариант **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**. Установка будет продолжена.

Для отказа от установки нажмите на кнопку **Отмена**.

Шаг 5. Выбор типа установки

На данном этапе вам предлагается выбрать наиболее подходящий вам тип установки Kaspersky Internet Security:

- **Быстрая установка**. При выборе данного варианта приложение будет полностью установлено на ваш компьютер с параметрами защиты, рекомендуемыми специалистами «Лаборатории Касперского». По окончании установки будет запущен мастер настройки приложения (на стр. 41).

- **Выборочная установка**. В данном случае вам будет предложено выбрать, какие компоненты приложения вы хотите установить на ваш компьютер, указать папку, куда будет установлено приложение (см. раздел «Шаг 6. Выбор папки назначения» на стр. 31), а также провести активацию приложения и его настройку с помощью специального мастера.

При выборе первого варианта мастер установки приложения сразу переходит к шагу 8 (см. раздел «Шаг 8. Поиск других антивирусных программ» на стр. 32). Во втором случае на каждом этапе установки от вас потребуется ввод либо подтверждение некоторых данных.

Шаг 6. Выбор папки назначения

Данный шаг мастера установки выполняется только в том случае, если вы выбрали выборочную установку приложения (см. раздел «Шаг 5. Выбор типа установки» на стр. 31).

На этом этапе установки вам предлагается определить папку на вашем компьютере, в которую будет установлено Kaspersky Internet Security. По умолчанию задан путь:

- **<Диск> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009** – для 32-разрядных систем.

- **<Диск> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009** – для 64-разрядных систем.

Вы можете указать другую папку, нажав на кнопку **Обзор** и выбрав ее в стандартном окне выбора папки или введя путь к ней в соответствующем поле ввода.

Помните, если вы указываете полный путь к папке установки вручную, его длина не должна превышать 200 символов и содержать спецсимволы.

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

ШАГ 7. ВЫБОР КОМПОНЕНТОВ ПРИЛОЖЕНИЯ ДЛЯ УСТАНОВКИ

Данный шаг мастера установки выполняется только в том случае, если вы выбрали выборочную установку приложения (см. раздел «Шаг 5. Выбор типа установки» на стр. 31).

При выборочной установке вам нужно определить компоненты Kaspersky Internet Security, которые вы хотите установить на ваш компьютер. По умолчанию для установки выбраны все компоненты приложения: компоненты защиты, задачи проверки и обновления.

Для принятия решения о том, какие компоненты вы не хотите устанавливать, воспользуйтесь краткой информацией о компоненте. Для этого выберите компонент в списке в прочтите информацию о нем в поле ниже. Информация включает краткое описание назначения компонента и место на диске, требующееся для его установки.

Для того чтобы отказаться от установки какого-либо компонента, откройте контекстное меню на значке рядом с именем компонента и выберите пункт **Компонент будет недоступен**. Помните, что отменяя установку какого-либо компонента, вы лишаетесь защиты от целого ряда опасных программ.

Для того чтобы выбрать компонент для установки, откройте контекстное меню на значке рядом с именем компонента и выберите пункт **Компонент будет установлен на локальный жесткий диск**.

После того, как выбор устанавливаемых компонентов будет завершен, нажмите на кнопку **Далее**. Чтобы вернуться к списку устанавливаемых компонентов по умолчанию, нажмите на кнопку **Сброс**.

ШАГ 8. ПОИСК ДРУГИХ АНТИВИРУСНЫХ ПРОГРАММ

На этом этапе осуществляется поиск других установленных на вашем компьютере антивирусных продуктов, в том числе и продуктов «Лаборатории Касперского», совместное использование с которыми Kaspersky Internet Security может привести к возникновению конфликтов.

При обнаружении таких программ на вашем компьютере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Под списком обнаруженных антивирусных приложений вы можете выбрать, автоматически удалить их или вручную.

Если в числе обнаруженных антивирусных программ есть приложение «Лаборатории Касперского» версии 7.0, при его удалении вручную рекомендуем вам сохранить используемый в работе этого приложения файл ключа. Вы сможете использовать его в качестве ключа для приложения новой версии. Также рекомендуем сохранить объекты карантина и резервного хранилища, эти объекты будут автоматически помещены в карантин Kaspersky Internet Security новой версии, и вы сможете продолжить работу с ними.

При автоматическом удалении приложения версии 7.0 информация об активации будет сохранена программой и подхватится при установке версии 2009.

Приложение поддерживает файлы ключей для версии 6.0 и 7.0. Ключи, использующиеся для приложений версии 5.0, не поддерживаются.

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

Шаг 9. Завершающая подготовка к установке приложения

На данном этапе вам будет предложено произвести завершающую подготовку к установке Kaspersky Internet Security на ваш компьютер.

При первоначальной и выборочной установке (см. раздел «Шаг 5. Выбор типа установки» на стр. 31) приложения не рекомендуется снимать флажок **Включить защиту модулей до начала установки**. Это позволит защитить модули Kaspersky Internet Security, начиная с его установки на ваш компьютер, от несанкционированного изменения. При повторной установке или восстановлении приложения рекомендуется снять данный флажок.

При удаленной установке приложения на компьютер через **Удаленный Рабочий стол** рекомендуется снимать флажок **Включить защиту модулей до начала установки**. Если такой флажок установлен, процедура установки может быть не проведена или проведена некорректно.

Для продолжения установки нажмите на кнопку **Далее**. В результате запустится процесс копирования файлов дистрибутива приложения на ваш компьютер.

В процессе установки происходит разрыв текущих сетевых соединений, если в составе Kaspersky Internet Security присутствуют компоненты, перехватывающие сетевой трафик. Большинство прерванных соединений восстанавливается через некоторое время.

Шаг 10. Завершение процедуры установки

Окно **Завершение установки** содержит информацию об окончании процесса установки Kaspersky Internet Security на ваш компьютер.

Следующий шаг - это настройка приложения для обеспечения максимальной защиты вашей информации на компьютере. Настроить Kaspersky Internet Security быстро и правильно поможет мастер настройки (см. раздел «Мастер настройки приложения» на стр. 41). Нажмите на кнопку **Далее**, чтобы перейти к настройке приложения.

ИНТЕРФЕЙС ПРИЛОЖЕНИЯ

Kaspersky Internet Security обладает достаточно простым и удобным в работе интерфейсом. В данной главе будут подробно рассмотрены основные его элементы.

Кроме основного интерфейса приложение имеет компоненты расширения (плагины), встраиваемые в Microsoft Office Outlook (проверка на вирусы и проверка на спам), Microsoft Outlook Express (проверка на спам), The Bat! (проверка на вирусы и проверка на спам), Thunderbird (проверка на спам), Microsoft Internet Explorer, Microsoft Windows Explorer. Плагины расширяют возможности перечисленных программ, позволяя из их интерфейса осуществлять управление и настраивать параметры компонентов **Почтовый Антивирус** и **Анти-Спам**.

В ЭТОМ РАЗДЕЛЕ

Значок в области уведомлений

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

Значок является индикатором работы приложения. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых приложением.

Если значок активный  (цветной), это означает, что защита включена полностью либо работают какие-либо ее компоненты. Если значок неактивный  (черно-белый), значит все компоненты защиты выключены.

В зависимости от выполняемой операции значок Kaspersky Internet Security меняется:

 - выполняется проверка почтового сообщения.

 - выполняется обновление баз и модулей приложения.

 - требуется перезагрузка компьютера для применения обновлений.

 - произошел сбой в работе какого-либо компонента приложения.

Также значок обеспечивает доступ к основным элементам интерфейса приложения: контекстному меню (см. раздел «Контекстное меню» на стр. 35) и главному окну (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36).

Чтобы открыть контекстное меню, щелкните правой клавишей мыши по значку приложения.

Чтобы открыть главное окно приложения, дважды щелкните левой клавишей мыши по значку приложения. Главное окно всегда открывается на разделе **Защита**.

В результате появления новостей от «Лаборатории Касперского» в области уведомлений панели задач Microsoft Windows появляется значок  . Щелкните по нему дважды левой клавишей мыши и в открывшемся окне ознакомьтесь с текстом новости.

Контекстное меню

Контекстное меню позволяет перейти к выполнению основных задач защиты.

Меню Kaspersky Internet Security содержит следующие пункты:

- **Обновление** - запуск обновления баз и модулей приложения, и их установка на вашем компьютере.
- **Полная проверка компьютера** - запуск полной проверки компьютера на присутствие вредоносных объектов. В результате будут проверены объекты на всех дисках, в том числе и на съемных носителях.
- **Проверка на вирусы** - переход к выбору объектов и запуску проверки на вирусы. По умолчанию список содержит ряд объектов, таких как папка **Мои Документы** и почтовые ящики. Вы можете пополнить список, выбрать объекты для проверки и запустить поиск вирусов.
- **Мониторинг сети** - просмотр списка установленных сетевых соединений, открытых портов и трафика.
- **Виртуальная клавиатура** - переход к виртуальной клавиатуре (см. раздел «Виртуальная клавиатура» на стр. 158).
- **Kaspersky Internet Security** - открытие главного окна приложения (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36).
- **Настройка** - переход к просмотру и настройке параметров работы приложения.
- **Активация** - переход к активации Kaspersky Internet Security. Для получения статуса зарегистрированного пользователя, необходимо активировать вашу версию приложения. Данный пункт меню присутствует только в том случае, если приложение не активировано.
- **О программе** - вызов информационного окна о приложении.
- **Приостановка защиты / Возобновление защиты** - выключение на время / включение работы компонентов постоянной защиты. Данный пункт меню не влияет на обновление приложения и на выполнение задач поиска вирусов.
- **Блокирование сетевого трафика / Разблокирование сетевого трафика** - временное блокирование всех сетевых соединений компьютера. Для того чтобы разрешить взаимодействие компьютера с сетью повторно, выберите пункт **Разблокирование сетевого трафика** в контекстном меню.

- **Выход** - завершение работы Kaspersky Internet Security (при выборе данного пункта меню приложение будет выгружено из оперативной памяти компьютера).

Рисунок 1: Контекстное меню

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

ГЛАВНОЕ ОКНО KASPERSKY INTERNET SECURITY

Главное окно приложения условно можно разделить на три части:

- Верхняя часть окна сигнализирует о текущем состоянии защиты вашего компьютера.

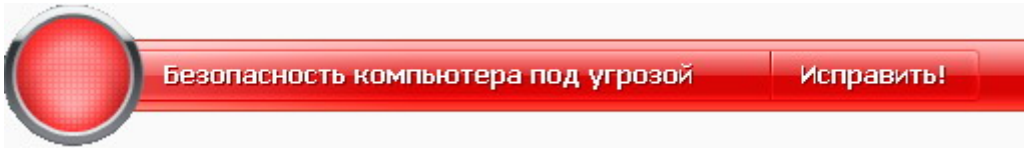

Рисунок 2: Текущее состояние защиты компьютера

Существует три возможных состояния защиты, каждое из которых выражено определенным цветом, аналогично сигналам светофора. Зеленый цвет говорит о том, что защита вашего компьютера осуществляется на должном уровне, желтый и красный цвета сигнализируют о наличии разного рода угроз безопасности в настройке параметров или работе Kaspersky Internet Security. К угрозам относятся не только вредоносные программы, но и устаревшие базы приложения, некоторые выключенные компоненты защиты, минимальные параметры работы приложения и др.

По мере возникновения угроз безопасности их необходимо устранять. Для получения подробной информации о них и быстрого их устранения воспользуйтесь ссылкой **Исправить** (см. рис. выше).

- Левая часть окна позволяет быстро перейти к работе с любой функцией приложения, к выполнению задач проверки на вирусы или обновления и др.

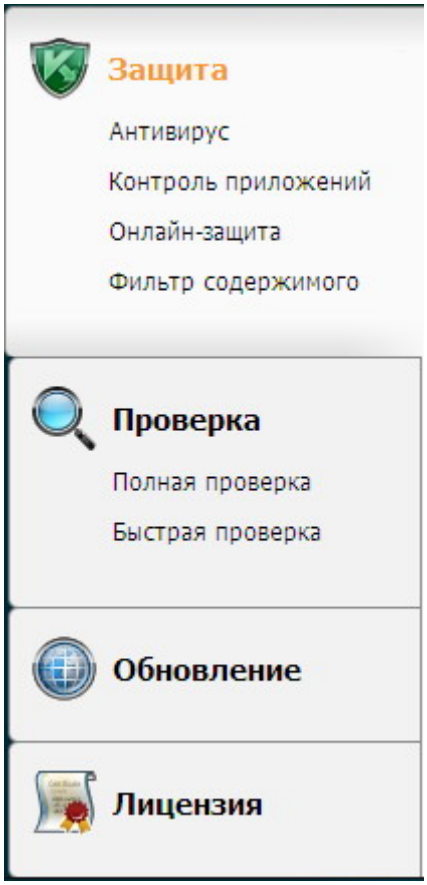

Рисунок 3: Левая часть главного окна

- Правая часть окна содержит информацию по выбранной в левой части функции приложения, позволяет настроить параметры каждой из них, предоставляет инструменты для выполнения задач проверки на вирусы, получения обновлений и др.

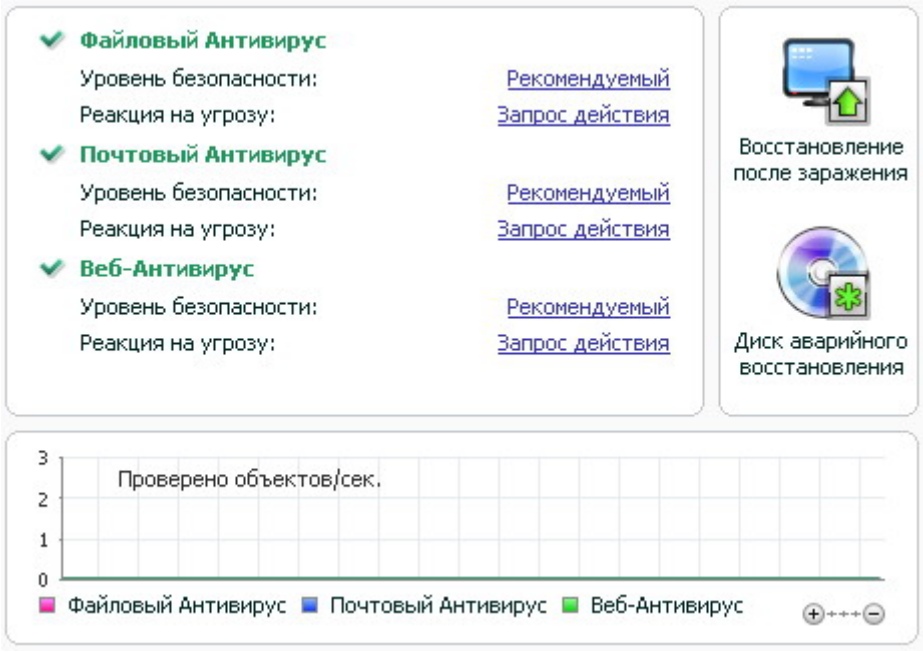

Рисунок 4: Информационная часть главного окна

Также вы можете воспользоваться кнопками:

- **Настройка** - переход к окну настройки параметров приложения (см. раздел «Настройка параметров приложения» на стр. 159).
- **Справка** - переход к справочной системе Kaspersky Internet Security.
- **Обнаружено** - переход к списку опасных объектов, обнаруженных в результате работы какого-либо компонента или выполненной задачи проверки на вирусы, а также к просмотру подробной статистики по результатам работы приложения.
- **Отчеты** - переход к списку событий, произошедших в работе приложения.
- **Поддержка** - открытие окна с информацией о системе и ссылками на информационные ресурсы «Лаборатории Касперского» (сайт Службы технической поддержки, форум).

Вы можете менять внешний вид Kaspersky Internet Security, создавая и используя свои графические элементы и цветовую палитру.

Уведомления

При возникновении событий в процессе работы Kaspersky Internet Security на экран выводятся специальные уведомления - всплывающие сообщения над значком приложения в панели задач Microsoft Windows.

В зависимости от степени важности события, с точки зрения безопасности компьютера, уведомления могут быть следующих типов:

- **Тревога**. Произошло событие критической важности, например, обнаружен вирус или опасная активность в системе. Необходимо немедленно принять решение о дальнейших действиях. Данный тип уведомления имеет красный цвет.

- **Внимание**. Произошло потенциально опасное событие, например, обнаружен возможно зараженный объект или подозрительная активность в системе. Необходимо принять решение, насколько данное событие опасно на ваш взгляд. Данный тип уведомления имеет желтый цвет.

- **Информация**. Уведомление информирует о событии, не имеющем первостепенной важности. К данному типу относятся, например, уведомления, появляющиеся в процессе работы компонента **Фильтр содержимого**. Информационные уведомления имеют зеленый цвет.

См. также

Уведомления.....193

Окно настройки параметров приложения

Окно настройки параметров Kaspersky Internet Security можно открыть из главного окна (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36) или контекстного меню (см. раздел «Контекстное меню» на стр. 35). Для этого нажмите на кнопку **Настройка** в верхней части главного окна либо выберите одноименный пункт в контекстном меню приложения.

Окно настройки состоит из двух частей:

- левая часть окна обеспечивает доступ к компонентам Kaspersky Internet Security, задачам проверки на вирусы, обновления и др;

- правая часть окна содержит перечень параметров выбранного в левой части компонента, задачи и т. п.

См. также

Настройка параметров приложения.....159

НАЧАЛО РАБОТЫ

Одной из главных задач специалистов «Лаборатории Касперского» при создании Kaspersky Internet Security являлась оптимальная настройка всех параметров приложения. Это дает возможность пользователю с любым уровнем компьютерной грамотности, не углубляясь в параметры, обеспечить безопасность компьютера сразу же после установки приложения.

Для удобства пользователей мы постарались объединить этапы предварительной настройки в едином интерфейсе мастера настройки приложения (см. раздел «Мастер настройки приложения» на стр. 41), который запускается в конце процедуры установки. Следуя указаниям мастера, вы сможете провести активацию приложения, настроить параметры обновления, ограничить доступ к приложению с помощью пароля и произвести другие настройки.

Ваш компьютер может быть заражен вредоносными программами до установки Kaspersky Internet Security. Чтобы обнаружить имеющиеся вредоносные программы, запустите проверку компьютера (см. раздел «Проверка компьютера на вирусы» на стр. 48).

В результате работы вредоносных программ и сбоев системы настройки параметров вашего компьютера могут быть повреждены. Запустите мастер Анализа безопасности (см. раздел «Анализ безопасности» на стр. 47), чтобы найти уязвимости установленного программного обеспечения и аномалии настроек системы.

На момент установки приложения входящие в поставку базы могут устареть. Запустите обновление приложения (на стр. 47) (если это не было сделано с помощью мастера настройки либо автоматически сразу после установки приложения).

Входящий в состав Kaspersky Internet Security компонент Анти-Спам использует самообучающийся алгоритм для распознавания нежелательных сообщений. Запустите мастер обучения Анти-Спама (см. раздел «Обучение с помощью Мастера обучения» на стр. 107), чтобы настроить компонент для работы с вашей корреспонденцией.

После выполнения вышеописанных действий приложение готово к работе. Чтобы оценить уровень защиты вашего компьютера, воспользуйтесь мастером управления безопасностью (см. раздел «Управление безопасностью» на стр. 51).

В ЭТОМ РАЗДЕЛЕ

Мастер настройки приложения

Мастер настройки приложения запускается в конце процедуры установки. Его задача – помочь вам провести первичную настройку параметров Kaspersky Internet Security, исходя из особенностей и задач вашего компьютера.

Интерфейс мастера настройки выполнен в виде последовательности окон (шагов), переход между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера – при помощи кнопки **Отмена**.

Рассмотрим подробнее шаги мастера

Шаг 1. Активация приложения

Перед активацией Kaspersky Internet Security убедитесь, что системное время и дата компьютера соответствуют реальной дате и времени.

Процедура активации приложения заключается в установке ключа, на основании которого приложение будет определять наличие прав и срок на его использование.

Ключ содержит служебную информацию, необходимую для полнофункциональной работы Kaspersky Internet Security, а также дополнительные сведения:

- информация о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также дату его окончания.

В зависимости от того, имеется ли у вас ключ или вам необходимо получить его с сервера ЗАО «Лаборатория Каперского», вам предлагаются следующие варианты активации Kaspersky Internet Security:

- онлайн-активация (на стр. 42);
- активация пробной версии (на стр. 43);
- активация с помощью ранее полученного файла ключа (см. раздел «Активация с помощью ключа» на стр. 43);

- активировать приложение позже. При выборе этого варианта этап активации Kaspersky Internet Security будет пропущен. Приложение будет установлено на ваш компьютер, вам будут доступны все функции приложения, за исключением обновления (обновить приложение вы сможете только один раз после установки).

Для активации Kaspersky Internet Security требуется подключение к интернету. Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже из интерфейса приложения либо, выйдя в интернет с другого компьютера, получить ключ по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

ОНЛАЙН-АКТИВАЦИЯ

Онлайн-активация основана на вводе кода активации, который вы получаете по электронной почте при покупке Kaspersky Internet Security через интернет. В случае приобретения приложения в коробке код активации будет указан на конверте с установочным диском.

Код активации представляет собой последовательность цифр, разделенных дефисами на четыре блока по пять символов, без пробелов. Например, 11111-11111-11111-11111. Обратите внимание, что код должен вводиться латинскими символами.

Если вы уже проходили процедуру регистрации клиентов ЗАО «Лаборатории Касперского» и у вас есть номер клиента и пароль, то установите флажок **У меня есть номер клиента**. При нажатии на ссылки рядом с флажком открывается Персональный кабинет на сайте Службы технической поддержки, где вы можете получить интересующую вас информацию.

В нижней части окна укажите ваши номер клиента и пароль, если вы уже проходили процедуру регистрации клиентов «Лаборатории Касперского», и у вас есть эти данные. Если вы еще не регистрировались, оставьте поля пустыми. В этом случае на следующем этапе мастер активации запросит вашу контактную информацию и выполнит регистрацию (в случае активации подписки регистрация не требуется и, следовательно, следующий шаг мастера будет пропущен). По окончании регистрации вам будут присвоены номер клиента и пароль, которые являются обязательным условием для получения технической поддержки.

РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ

На данном этапе активации требуется указать вашу контактную информацию: адрес электронной почты, страну и город проживания. Данная информация требуется Службе технической поддержки «Лаборатории Касперского» для идентификации вас как зарегистрированного пользователя.

После ввода информации ваши данные будут отправлены на сервер активации, после чего вам будет присвоен номер клиента и пароль к Персональному кабинету на веб-сайте Службы технической поддержки.

ПОЛУЧЕНИЕ ФАЙЛА КЛЮЧА

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете, отправляет ваши регистрационные данные (код активации, контактную информацию). Код активации и полнота заполнения контактной информации будут проверены на сервере.

В случае успешной проверки кода активации мастер получает файл ключа.

Полученный файл будет автоматически установлен для работы Kaspersky Internet Security, и вы увидите окно завершения активации с подробной информацией об используемом ключе.

В случае активации подписки, кроме перечисленной выше информации, также доступна информация о статусе подписки (см. раздел «Подписка на автоматическое продление лицензии» на стр. 49).

Если код активации не пройдет проверку, на экране появится соответствующее уведомление. В данном случае обратитесь за информацией в компанию, где вы приобрели Kaspersky Internet Security.

Если в случае активации, число активаций с помощью кода активации, по которому приложение пытается получить ключ, превышено, код активации будет заблокирован и приложение предложит вам обратиться в Службу поддержки «Лаборатории Касперского».

Активация пробной версии

Данный вариант активации следует использовать, если вы хотите установить пробную версию Kaspersky Internet Security перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный ключ со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения. По истечении срока действия ключа возможность активации пробной версии вторично будет недоступна.

Активация с помощью ключа

Если у вас есть файл ключа, вы можете активировать Kaspersky Internet Security с его помощью. Для этого воспользуйтесь кнопкой **Обзор** и выберите файл с расширением *.key*.

После успешной установки ключа в нижней части окна будет представлена информации об используемом ключе: имя владельца, номер ключа, его тип (коммерческий, для бета-тестирования, пробный и т.д.), а также дата окончания срока действия ключа.

Завершение активации

Мастер настройки информирует вас об успешном завершении активации Kaspersky Internet Security. Кроме того, приводится информация об установленном ключе: имя владельца, номер ключа, его тип (коммерческий, коммерческий с подпиской, для бета-тестирования, пробный и т.д.), а также дата окончания срока действия ключа.

В случае активации подписки вместо даты окончания срока действия ключа приводится информация о статусе подписки (см. раздел «Подписка на автоматическое продление лицензии» на стр. 49).

Шаг 2. Выбор режима защиты

Выберите режим защиты, предоставляемой Kaspersky Internet Security.

Для выбора доступны два режима:

- **Автоматический**. При возникновении важных событий Kaspersky Internet Security автоматически выполняет действие, рекомендуемое специалистами «Лаборатории Касперского». При обнаружении угрозы приложение пытается вылечить объект, а, если это невозможно - удаляет объект. Подозрительные объекты пропускаются без обработки. О возникающих событиях информируют всплывающие сообщения.

- **Интерактивный**. В этом режиме приложение реагирует на возникновение событий заданным вами образом. При возникновении событий, требующих вашего вмешательства, приложение выводит уведомления (на стр. 193) с возможностью выбора действия.

Уведомление об обнаружении активного заражения выводится независимо от выбранного режима защиты.

Шаг 3. Настройка обновления приложения

Данный шаг мастера настройки приложения пропускается, если был выбран режим быстрой установки. Параметрам приложения, настраиваемым на данном шаге, задаются значения по умолчанию.

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей приложения. В данном окне мастера настройки вам предлагается выбрать режим обновления Kaspersky Internet Security и сформировать параметры расписания:

- **Автоматически**. Kaspersky Internet Security проверяет наличие пакета обновлений в источнике обновления с заданной периодичностью. Частота проверки может увеличиваться во время вирусных

эпидемий и сокращаться вне их. При обнаружении свежих обновлений приложение скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.

- **По расписанию** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открывающемся по кнопке **Настройка**.

- **Вручную**. В этом случае вы будете самостоятельно запускать обновление приложения.

Обратите внимание, что базы и модули приложения, входящие в дистрибутив, могут устареть на момент установки Kaspersky Internet Security. Поэтому мы рекомендуем получить самые последние обновления приложения. Для этого нажмите на кнопку **Обновить сейчас**. В данном случае приложение получит необходимый набор обновлений с сайтов обновления в интернете и установит их на ваш компьютер.

Если вы хотите перейти к настройке параметров обновления (см. раздел «Обновление» на стр. 142) (выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления с правами определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на ссылку **Настройка**.

Шаг 4. Ограничение доступа к приложению

Данный шаг мастера настройки Kaspersky Internet Security пропускается, если был выбран режим быстрой установки. Параметрам приложения, настраиваемым на данном шаге, задаются значения по умолчанию.

В связи с тем, что персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности, а также в связи с возможностями отключения защиты со стороны вредоносных программ, вам предлагается ограничить доступ к Kaspersky Internet Security с помощью пароля. Пароль позволяет защитить приложение от попыток несанкционированного отключения защиты или изменения его параметров.

Для включения защиты установите флажок **Включить защиту паролем** и заполните поля **Пароль** и **Подтверждение** пароля.

Ниже укажите область, на которую будет распространяться ограничение доступа:

- **Все операции (кроме уведомлений об опасности)**. Запрашивать пароль при инициировании любого действия пользователя с приложением, за исключением работы с уведомлениями об обнаружении опасных объектов.

- **Отдельные операции:**

  - **Настройка параметров приложения** - запрос пароля при попытке пользователя сохранить изменения параметров Kaspersky Internet Security.

  - **Завершение работы приложения** - запрос пароля при попытке пользователя завершить работу приложения.

  - **Отключение компонентов защиты, запуск и остановка задач** - запрос пароля при попытке пользователя приостановить или выключить полностью работу какого-либо компонента защиты либо задачи проверки на вирусы.

Шаг 5. Выбор обнаруживаемых угроз

Данный шаг мастера настройки приложения пропускается, если был выбран режим быстрой установки. Параметрам приложения, настраиваемым на данном шаге, задаются значения по умолчанию.

На данном этапе вы можете выбрать категории угроз, обнаруживаемые Kaspersky Internet Security. Программы, способные нанести вред вашему компьютеру, Kaspersky Internet Security обнаруживает всегда. К таким типам

программ относятся вирусы и черви (на стр. 18), троянские программы (на стр. 19) и вредоносные инструменты (см. раздел «Угрозы-программы» на стр. 17).

Вы можете выбрать для обнаружения следующие категории нежелательного программного обеспечения:

- программы-рекламы (см. раздел «Программы рекламного характера» на стр. 24) (Adware);
- программы, связанные с распространением порнографии (см. раздел «Программы порнографического характера» на стр. 24) (Pornware);
- потенциально опасные программы (см. раздел «Другие потенциально нежелательные программы» на стр. 25), в том числе некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, IRC-клиенты, FTP-серверы, всевозможные утилиты для остановки процессов или скрытия их работы;
- программы-упаковщики. Такие программы не представляют непосредственной угрозы для компьютера, но часто применяются при изготовлении вредоносных программ.

Шаг 6. Отключение кеширования доменных имен (DNS)

Данный шаг мастера настройки приложения пропускается, если был выбран режим быстрой установки. Параметрам приложения, настраиваемым на данном шаге, задаются значения по умолчанию.

Сервис кеширования доменных имен значительно сокращает время соединения вашего компьютера с нужным интернет-ресурсом, однако в то же время является опасной уязвимостью, используя которую злоумышленники могут получить доступ к вашим данным.

Установите флажок **Отключить кеширование DNS**, чтобы повысить уровень безопасности вашего компьютера.

При отключении кеширования DNS возможны проблемы в работе приложений, использующих множественные соединения (например, клиентов файлообменных сетей).

На данном шаге вы также можете указать нужно ли выводить в отчет защиты записи о некритических событиях. Для этого установите флажок **Записывать некритические события**.

Шаг 7. Анализ системы

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

Шаг 8. Анализ почты

На данном этапе происходит обучение Анти-Спама на исходящих сообщениях электронной почты. Для обучения алгоритма iBayes необходимо 50 полезных и 50 спам-сообщений. На момент установки Kaspersky Internet Security обучение на спам-сообщениях уже выполнено.

Исходящие сообщения анализируются в папках исходящих сообщений учетных записей Microsoft Outlook Express и Microsoft Office Outlook. Для успешного завершения обучения достаточно 50 уникальных писем. Если писем недостаточно, то алгоритм Анти-Спама считается необученным и вам будет предложено обучить Анти-Спам в процессе работы с приложением.

Данный шаг мастера настройки приложения пропускается, если компонент Анти-Спам не был выбран для установки.

ШАГ 9. ОБРАТНАЯ СВЯЗЬ

Данный шаг мастера настройки приложения пропускается, если был выбран режим быстрой установки. Параметрам приложения, настраиваемым на данном шаге, задаются значения по умолчанию.

На данном этапе вам предлагается принять участие в программе Kaspersky Security Network. Участие в данной программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, отправку уникального идентификатора, присвоенного вашему компьютеру приложением, и информации о системе. При этом гарантируется, что никакие персональные данные отправлены не будут.

Установите флажок **Я согласен участвовать в Kaspersky Security Network**, чтобы включить отправку «Лаборатории Касперского» информации.

Кроме перечисленных выше данных, Kaspersky Internet Security собирает расширенную статистику: информацию о скачанных вами исполняемых файлах и подписанных приложений, а также о приложениях, запускаемых на вашем компьютере. Чтобы разрешить отправку расширенной статистики, установите флажок **Я согласен отправлять расширенную статистику в рамках Kaspersky Security Network**.

ШАГ 10. ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА

В последнем окне мастера вам предлагается перезагрузить компьютер для завершения установки приложения. Перезагрузка необходима для регистрации драйверов Kaspersky Internet Security.

Вы можете отложить перезагрузку компьютера, но в этом случае некоторые компоненты защиты приложения не будут работать.

ВЫБОР ТИПА СЕТИ

После установки Kaspersky Internet Security компонент Сетевой экран исследует активные сетевые соединения на вашем компьютере. Каждому сетевому соединению назначается статус, определяющий разрешенную сетевую активность.

Если вы выбрали интерактивный режим работы (см. раздел «Шаг 2. Выбор режима защиты» на стр. 43) Kaspersky Internet Security, при обнаружении сетевого соединения открывается уведомление. В окне уведомления вы можете выбрать статус новой сети:

- **Публичная сеть** - для сетевых соединений с таким статусом запрещается доступ к вашему компьютеру извне. В такой сети также запрещен доступ в общим папкам и принтерам. Такой статус рекомендуется назначать сети Интернет.

- **Локальная сеть** - для сетевых соединений с таким статусом разрешается доступ к общим папкам и сетевым принтерам. Такой статус рекомендуется назначать защищенной локальной сети, например, корпоративной.

- **Доверенная сеть** - для сетевых соединений с таким статусом разрешается любая активность. Такой статус рекомендуется назначать только для абсолютно безопасной зоны.

Для каждого статуса сети в поставку Kaspersky Internet Security включен набор правил (см. раздел «Правила Сетевого экрана» на стр. 91), управляющих сетевой активностью. Статус сети, заданный при ее первом обнаружении, впоследствии можно сменить (см. раздел «Изменение статуса сети» на стр. 89).

Обновление приложения

Для обновления Kaspersky Internet Security требуется наличие соединения с интернетом.

В поставку Kaspersky Internet Security включены базы, содержащие сигнатуры угроз, образцы фраз, характерных для спама и описания сетевых атак. Однако на момент установки приложения базы могут устареть, так как «Лаборатория Касперского» регулярно обновляет базы и модули приложения.

Во время работы мастера настройки приложения вы можете выбрать режим запуска обновления (см. раздел «Шаг 3. Настройка обновления приложения» на стр. 43). По умолчанию Kaspersky Internet Security автоматически проверяет наличие обновлений на серверах «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Kaspersky Internet Security в фоновом режиме скачивает и устанавливает их.

Для поддержания защиты вашего компьютера в актуальном состоянии рекомендуется обновить Kaspersky Internet Security непосредственно после установки.

Чтобы самостоятельно обновить Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Запустить обновление**.

См. также

Обновление.....142

Мастер настройки приложения.....41

Анализ безопасности

В результате нежелательной активности на вашем компьютере, которая может быть результатом сбоев системы или активности вредоносных программ, повреждаются настройки параметров операционной системы. Кроме этого, приложения, установленные на вашем компьютере, могут иметь уязвимости, используемые злоумышленниками для причинения вреда вашему компьютеру.

Для обнаружения и устранения таких проблем безопасности специалисты «Лаборатории Касперского» рекомендуют запустить *мастер Анализа безопасности* после установки приложения. Мастер Анализа безопасности (см. раздел «Анализ безопасности» на стр. 150) осуществляет поиск уязвимостей в установленных приложениях, а также поиск повреждений и аномалий в настройках параметров операционной системы и браузера.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Запустите задачу **Анализ безопасности**.

ПРОВЕРКА КОМПЬЮТЕРА НА ВИРУСЫ

Разработчики вредоносного программного обеспечения предпринимают массу усилий для сокрытия деятельности своих программ, поэтому вы можете не заметить присутствия на вашем компьютере вредоносных программ.

На момент установки Kaspersky Internet Security автоматически выполняется задача **Быстрой проверки** компьютера. Эта задача направлена на поиск и нейтрализацию вредоносных программ в объектах, загружаемых при старте операционной системы.

Специалисты «Лаборатории Касперского» также рекомендуют выполнить задачу **Полной проверки** компьютера.

Чтобы запустить / остановить задачу проверки на вирусы, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Нажмите на кнопку **Запустить проверку**, чтобы начать проверку. Нажмите на кнопку **Остановить проверку** во время работы задачи, если возникла необходимость остановить ее выполнение.

См. также

Проверка на вирусы 131

УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ

Возможность использования Kaspersky Internet Security определяется наличием файла ключа. Ключ предоставляется вам на основании покупки продукта и дает право использовать приложение со дня установки ключа.

Без ключа в случае, если не было активации пробной версии Kaspersky Internet Security, приложение будет работать в режиме – одно обновление. В дальнейшем новые обновления производиться не будут.

Если была активирована пробная версия приложения, то после завершения срока ее использования, Kaspersky Internet Security работать не будет.

По окончании срока действия коммерческого ключа функциональность приложения сохраняется за исключением возможности обновления баз приложения. Вы по-прежнему можете проверять ваш компьютер посредством задач поиска вирусов и использовать компоненты защиты, но только на основе баз, актуальных на дату окончания срока действия ключа. Следовательно, мы не гарантируем вам стопроцентную защиту от новых вирусов, которые появятся после окончания действия ключа.

Чтобы избежать заражения вашего компьютера новыми вирусами, мы рекомендуем вам продлить ключ на использование Kaspersky Internet Security. За две недели до истечения срока действия ключа приложение уведомляет вас об этом. В течение некоторого периода времени при каждом запуске приложения на экран выводится соответствующее сообщение.

Информация об используемом ключе представлена в разделе **Лицензия** главного окна Kaspersky Internet Security: номер ключа, его тип (коммерческий, коммерческий с подпиской, пробный, для бета-тестирования), ограничение количества компьютеров, на которых можно использовать данный ключ, дата окончания срока действия ключа и количество дней до этой даты. Информация об окончании срока действия ключа не отображается, если установлена коммерческая лицензия с подпиской (см. раздел «Подписка на автоматическое продление лицензии» на стр. 49).

Чтобы ознакомиться с условиями лицензионного соглашения на использование приложения воспользуйтесь кнопкой **Прочесть лицензионное соглашение**. Для удаления ключа из списка нажмите на кнопку **Удалить**.

Для приобретения ключа или продления срока его действия выполните следующее:

1. Приобретите новый ключ. Для этого воспользуйтесь кнопкой **Купить лицензию** (в случае если приложение не было активировано) или **Продлить лицензию**. На открывшейся веб-странице вам будет предоставлена полная информация об условиях покупки ключа через интернет-магазин «Лаборатории Касперского» либо у партнеров компании. При покупке через интернет-магазин по факту оплаты на электронный адрес, указанный в форме заказа, вам будет отправлен файл ключа либо код активации приложения.

2. Установите ключ. Для этого воспользуйтесь кнопкой **Установить ключ** в разделе **Лицензия** главного окна приложения либо командой **Активация** контекстного меню приложения. В результате будет запущен мастер активации.

Регулярно «Лаборатория Касперского» проводит акции, позволяющие продлить лицензию на использование наших продуктов со значительными скидками. Следите за акциями на веб-сайте «Лаборатории Касперского» в разделе **Продукты → Акции и спецпредложения**.

См. также

Подписка на автоматическое продление лицензии 49

Подписка на автоматическое продление лицензии

При лицензировании с помощью подписки Kaspersky Internet Security автоматически через определенные промежутки времени обращается к серверу активации для поддержания вашей лицензии в актуальном состоянии на весь срок подписки.

Если срок действия текущего ключа истек, Kaspersky Internet Security самостоятельно в фоновом режиме проверяет наличие обновленного ключа на сервере и в случае его наличия, скачивает и устанавливает его в режиме замены предыдущего ключа. Тем самым лицензия продлевается без вашего участия. Если период, в течение которого, приложение самостоятельно продлевает лицензию также истек, появляется возможность ее продления вручную. В течение периода, когда вы можете продлить лицензию вручную, функциональность приложения сохраняется. После окончания периода, если лицензия так и не была продлена, приложение перестает скачивать обновления баз. Чтобы отказаться от подписки на автоматическое продление лицензии, необходимо связаться с онлайн-магазином, где вы приобрели Kaspersky Internet Security.

Если на момент активации подписки, Kaspersky Internet Security уже был активирован ранее с помощью коммерческого ключа, то он будет заменен ключом с подпиской. Для того чтобы снова использовать коммерческий ключ, необходимо удалить ключ с подпиской и заново активировать приложение кодом активации, с помощью которого ранее был получен коммерческий ключ.

Состояние подписки характеризуется следующими статусами:

- *Определяется*. Запрос на активацию подписки еще не обработан (для обработки запроса на сервере требуется некоторое время). Kaspersky Internet Security работает в полнофункциональном режиме. Если по окончании определенного периода запрос на подписку не будет обработан, вы получите уведомление о том, что подписка не выполнена. При этом перестанут обновляться базы приложения.

- *Активирована*. Подписка на автоматическое продление лицензии была активирована на неограниченный срок (дата не ограничена), или на определенный промежуток времени (дата окончания подписки определена).

- *Продлена*. Подписка была продлена автоматически или вручную на неограниченный срок (дата не ограничена), или на определенный промежуток времени (дата окончания подписки определена).

- *Ошибка*. Продление подписки завершилось с ошибкой.

- *Истекла*. Срок подписки истек. Вы можете воспользоваться другим кодом активации или продлить подписку, связавшись с онлайн-магазином, где вы приобрели Kaspersky Internet Security.

- *Отказ от подписки*. Вы отказались от использования подписки на автоматическое продление лицензии.

- *Требуется обновление*. Ключ на продление подписки не был получен вовремя по каким-либо причинам. Воспользуйтесь кнопкой **Обновить статус подписки**, чтобы продлить действие подписки.

Если срок действия подписки истек и истек дополнительный период, в течение которого доступно продление лицензии (статус подписки – *Истекла*), Kaspersky Internet Security уведомляет вас об этом и прекращает попытки получения обновленного ключа с сервера. Функциональность приложения сохраняется за исключением обновления баз приложения.

Если по каким-либо причинам лицензия не была продлена (статус подписки – *Требуется обновление*) вовремя (например, компьютер был выключен весь период, когда было доступно продление лицензии), вы можете выполнить обновление ее статуса вручную. Для этого воспользуйтесь кнопкой **Обновить статус подписки**. До момента продления подписки Kaspersky Internet Security прекращает обновление баз приложения.

При использовании подписки вы не сможете установить ключи другого типа или воспользоваться другим кодом активации с целью продлить срок действия лицензии. Воспользоваться другим кодом активации вы можете только после окончания срока подписки (статус подписки - *Истекла*).

Помните, что при использовании подписки на автоматическое продление лицензии, в случае переустановки приложения на вашем компьютере, вам необходимо повторно вручную активировать продукт с помощью кода активации, полученного при покупке приложения.

См. также

Управление лицензией.....48

Участие в Kaspersky Security Network

Каждый день в мире появляются множество новых угроз. Для ускорения сбора статистики о типе новых угроз, их источнике и разработки способа нейтрализации «Лаборатория Касперского» предоставляет вам право воспользоваться услугой Kaspersky Security Network.

Использование Kaspersky Security Network подразумевает отправку «Лаборатории Касперского» следующей информации:

- Уникального идентификатора, присваиваемого вашему компьютеру Kaspersky Internet Security. Этот идентификатор характеризует аппаратные параметры вашего компьютера и не содержит никакой личной информации.

- Информации об угрозах, обнаруженных компонентами приложения. Состав информации зависит от типа обнаруженной угрозы.

- Информации о системе: версии операционной системы, установленные пакеты обновлений, загружаемые сервисы и драйверы, версии браузеров и почтовых клиентов, расширения браузеров, номер версии установленного приложения «Лаборатории Касперского».

В рамках Kaspersky Security Network также производится сбор расширенной статистики, в которую входит информация о:

- загружаемых на ваш компьютер исполняемых файлах и подписанных приложениях,

- запускаемых на вашем компьютере приложениях.

Отправка статистической информации происходит в конце обновления приложения.

«Лаборатория Касперского» гарантирует, что в рамках Kaspersky Security Network не происходит накопление и отправка персональных данных пользователя.

Чтобы настроить параметры отправки статистики, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Обратная связь**.
3. Установите флажок **Я согласен участвовать в Kaspersky Security Network**, чтобы подтвердить участие в Kaspersky Security Network. Установите флажок **Я согласен отправлять расширенную статистику в рамках Kaspersky Security Network**, чтобы подтвердить согласие на отправку расширенной статистики.

Управление безопасностью

О появлении проблем в защите компьютера сигнализирует статус защиты компьютера (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36) посредством изменения цвета значка статуса защиты и панели, на которой он расположен. При возникновении проблем в защите рекомендуется немедленно устранить их.

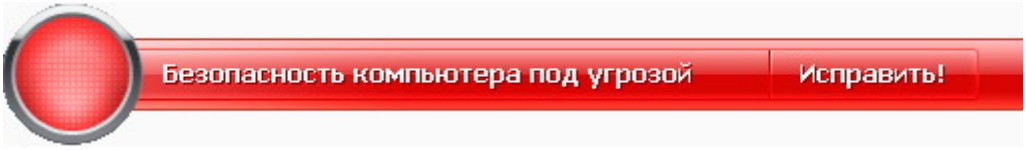

Рисунок 5: Текущее состояние защиты компьютера

Просмотреть список возникших проблем, их описание и возможные пути решения вы можете на закладке **Статус** (см. рис. ниже), переход к которой осуществляется по ссылке **Исправить** (см. рис. выше).

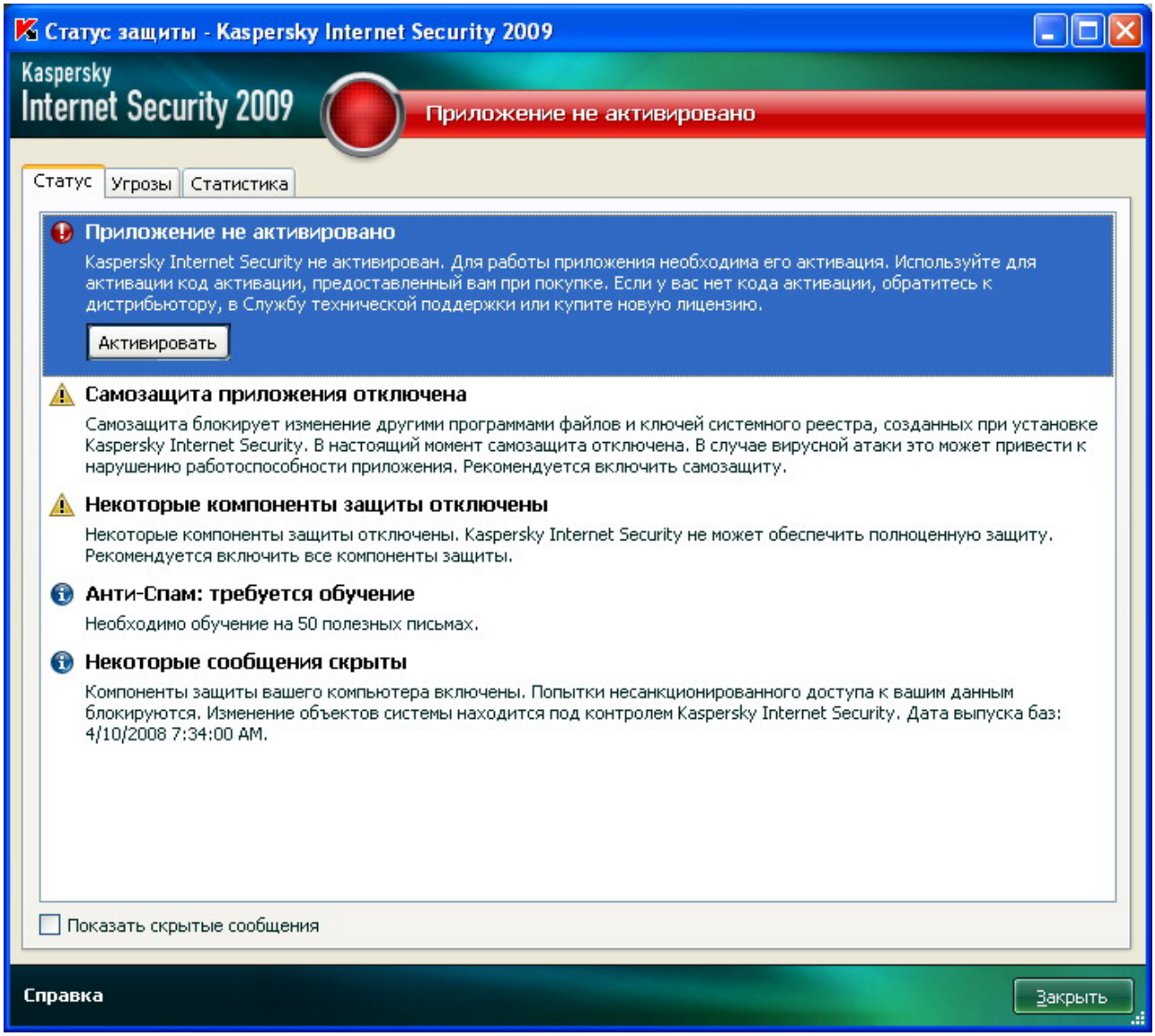

Рисунок 6: Решение проблем безопасности

Вы можете просмотреть список имеющихся проблем. Проблемы расположены исходя из важности их решения: сначала наиболее важные, то есть те, значок статуса которых красный; затем менее важные - значок статуса желтый, и последними - информационные сообщения. Для каждой проблемы дается ее подробное описание и предлагаются следующие варианты действий:

- *Немедленно устранить*. Используя соответствующие кнопки, вы можете перейти к непосредственному устранению проблемы, что является рекомендуемым действием.

- *Отложить устранение*. Если по какой-либо причине сиюминутное устранение проблемы невозможно, вы можете отложить данное действие и вернуться к нему позже. Для этого используйте кнопку **Скрыть сообщение**.

  Обратите внимание, что для серьезных проблем данная возможность не предусмотрена. К ним относится, например, наличие необезвреженных вредоносных объектов, сбой в работе одного или нескольких компонентов, повреждение файлов приложения.

Чтобы ранее скрытые сообщения были вновь отображены в общем списке, установите флажок **Показать скрытые сообщения**.

Приостановка защиты

Приостановка защиты означает отключение на некоторый промежуток времени всех компонентов защиты.

Чтобы приостановить защиту компьютера:

1. В контекстном меню (см. раздел «Контекстное меню» на стр. 35) приложения выберите пункт **Приостановка защиты**.

2. В открывшемся окне выберите период времени, спустя который защита будет включена:

   - **Через <временной интервал>** - защита будет включена через указанное время. Для выбора значения временного интервала воспользуйтесь раскрывающимся списком.

   - **После перезагрузки** - защита будет включена после перезагрузки системы (при условии, что включен режим запуска Kaspersky Internet Security при включении компьютера).

   - **Вручную** - защита будет включена только тогда, когда вы сами ее запустите. Для включения защиты выберите пункт **Возобновление защиты** в контекстном меню приложения.

В результате временного отключения работа всех компонентов защиты приостанавливается. Об этом свидетельствуют:

- Неактивные (серого цвета) названия выключенных компонентов в разделе **Защита** главного окна.

- Неактивный (серый) значок приложения (см. раздел «Значок в области уведомлений» на стр. 34) в системной панели.

- Красный цвет значка статуса и панели главного окна Kaspersky Internet Security.

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

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

В состав Kaspersky Internet Security входят компоненты, предназначенные для защиты вашего компьютера от заражения. Эти компоненты постоянно находятся в оперативной памяти компьютера и проверяют все открываемые, сохраняемые и запускаемые файлы, и объекты, поступающие из интернета и электронной почты.

Файловый Антивирус (см. раздел «Защита файлов и памяти» на стр. 55) перехватывает обращение пользователя или некоторой программы к каждому файлу при открытии, сохранении и запуске и проверяет этот файл.

Почтовый Антивирус (см. раздел «Защита почты» на стр. 65) проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP, MAPI и NNTP. Индикатором работы компонента является значок в области уведомлений панели задач, который принимает вид  каждый раз при проверке письма.

Веб-Антивирус (см. раздел «Защита веб-трафика» на стр. 71) защищает информацию, поступающую на ваш компьютер по HTTP-протоколу, а также предотвращает запуск на компьютере опасных скриптов.

По умолчанию компоненты защиты запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить работу какого-либо компонента.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют **не отключать** компоненты защиты, поскольку это может привести к заражению вашего компьютера и потере данных.

Также вы можете перейти к отчету о работе компонентов защиты, где будет представлена полная информация о событиях, произошедших в ходе их работы.

- *Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Антивирус**.
  3. В правой части окна нажмите левой клавишей мыши на галочку рядом с названием нужного компонента.
  4. В открывшемся меню выберите пункт **Выключить**.

- *Чтобы перейти к отчету о работе компонентов защиты, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Антивирус**.
  3. В правой части окна нажмите левой клавишей мыши на галочку рядом с названием нужного компонента.
  4. В открывшемся меню выберите пункт **Отчеты и статистика**.

В ЭТОМ РАЗДЕЛЕ

Защита файлов и памяти

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.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы. Проверка файлов происходит с определенным набором параметров, который называется уровнем безопасности. При обнаружении угроз Файловый Антивирус выполняет заданное действие.

Уровень защиты файлов и памяти на вашем компьютере определяется наборами параметров:

- параметры, формирующие защищаемую область;
- параметры, определяющие используемый метод проверки;
- параметры, определяющие проверку составных файлов (в том числе составных файлов больших размеров);
- параметры, задающие режим проверки;
- параметры, позволяющие приостановить работу компонента (по расписанию; во время работы выбранных приложений).

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

Вы можете восстановить параметры работы Файлового Антивируса по умолчанию, выберите один из уровней безопасности.

Чтобы изменить параметры работы Файлового Антивируса, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. Внесите необходимые изменения в настройки параметров компонента.

См. также

АЛГОРИТМ РАБОТЫ КОМПОНЕНТА

Файловый Антивирус запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы, то есть файлы, которые добавились или изменились со времени последнего обращения к ним. Процесс проверки файла выполняется по следующему алгоритму:

1. Компонент перехватывает обращение пользователя или некоторой программы к каждому файлу.

2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базах iChecker и iSwift и на основании полученной информации принимает решение о необходимости проверки файла.

Проверка включает следующие действия:

1. Файл анализируется на присутствие вирусов. Распознавание вредоносных объектов происходит на основании баз приложения. Базы содержат описание всех известных на настоящий момент вредоносных программ, угроз, сетевых атак и способов их обезвреживания.

2. В результате анализа возможны следующие варианты поведения Kaspersky Internet Security:

   a. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл, создает его резервную копию и пытается провести лечение. В результате успешного лечения файл становится доступным для работы, если же лечение произвести не удалось, файл удаляется.

   b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл подвергается лечению и помещается в специальное хранилище - карантин.

   c. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

При обнаружении зараженного или возможно зараженного объекта приложение уведомит вас об этом. Вам следует отреагировать на уведомление выбором действия:

- поместить угрозу на карантин для последующей проверки и обработки с помощью обновленных баз;

- удалить объект;
- пропустить, если вы абсолютно уверены, что данный объект не может являться вредоносным.

См. также

Защита файлов и памяти.....55

Изменение уровня безопасности файлов и памяти

Под уровнем безопасности понимается предустановленный набор параметров Файлового Антивируса. Специалистами «Лаборатории Касперского» были сформированы три уровня безопасности. Решение о том, какой уровень выбрать, принимается вами на основе условий работы и сложившейся ситуации.

- Если вы подозреваете, что вероятность заражения вашего компьютера очень высока, выберите высокий уровень безопасности.
- Рекомендуемый уровень обеспечивает баланс между производительностью и безопасностью и подходит для большинства случаев.
- Если вы работаете в защищенной среде (например, корпоративная сеть с централизованным обеспечением безопасности), вам подходит низкий уровень безопасности. Также вы можете установить низкий уровень в случае работы с ресурсоемкими приложениями.

Рисунок 7: Изменение уровня безопасности

Перед включением низкого уровня безопасности рекомендуется провести полную проверку компьютера (см. раздел «Проверка на вирусы» на стр. 131) с высоким уровнем.

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы (см. раздел «Защита файлов и памяти» на стр. 55) Файлового Антивируса. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы компонента по умолчанию, выберите один из предустановленных уровней.

Чтобы изменить установленный уровень безопасности файлов и памяти, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с названием уровня безопасности.
4. В раскрывшемся меню выберите нужный уровень безопасности.

Изменение действия над обнаруженными объектами

Файловый Антивирус в результате проверки присваивает найденным объектам один из следующих статусов:

- статус одной из вредоносных программ (например, **вирус**, **троянская программа**).

- **возможно зараженный**, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Это означает, что в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

Если в результате проверки на вирусы Kaspersky Internet Security находит зараженные или возможно зараженные объекты, то вы получаете уведомление об этом. Вам следует отреагировать на возникшую угрозу выбором действия над объектом. Такое поведение приложения, когда в качестве действия над обнаруженным объектом выбран **Запрос действий**, задано по умолчанию. Вы можете изменить действие. Например, вы уверены, что каждый найденный объект следует пытаться вылечить, и не хотите каждый раз выбирать действие **Лечить** при получении уведомления об обнаружении зараженного или подозрительного объекта. В этом случае вам следует выбрать действие **Без запроса. Лечить**.

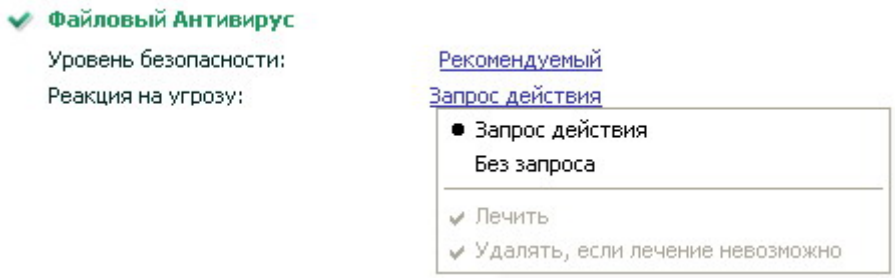

Рисунок 8: Изменение действия над объектом

Перед лечением или удалением зараженного объекта Kaspersky Internet Security формирует его резервную копию на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

Если вы работаете в автоматическом режиме (см. раздел «Шаг 2. Выбор режима защиты» на стр. 43), то приложение будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов. Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных - **Пропускать**.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным действием.
4. В раскрывшемся меню выберите нужное действие.

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Под областью защиты понимается не только местоположение проверяемых объектов, но и тип файлов, которые следует проверять. По умолчанию Kaspersky Internet Security проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков.

Вы можете расширить или сузить область защиты, путем добавления / удаления объектов проверки или изменения типа проверяемых файлов. Например, вы хотите проверять только exe-файлы, запускаемые с сетевых дисков. Однако вы должны быть уверены, что при сужении области защиты, вы не подвергаете безопасность своего компьютера риску быть зараженным.

При выборе типа файлов следует помнить следующее:

- Существует ряд форматов файлов, вероятность внедрения в которые вредоносного кода и его последующая активация достаточно низка (например, *txt*). И наоборот, есть форматы, которые содержат

или могут содержать исполняемый код (*exe*, *dll*, *doc*). Риск внедрения в такие файлы вредоносного кода и его последующей активации достаточно высок.

- Злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, хотя на самом деле такой файл может быть исполняемым, переименованным в *txt*-файл. Если выбран параметр **Файлы, проверяемые по расширению**, то такой файл будет пропущен в процессе проверки. Если выбран параметр **Файлы, проверяемые по формату**, невзирая на расширение, Файловый Антивирус проанализирует заголовок файла, в результате чего выяснится, что файл имеет *exe*-формат. Такой файл будет подвергнут проверке на вирусы.

Чтобы изменить список проверяемых объектов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Общие** в разделе **Область защиты** нажмите на ссылку **Добавить**.
6. В окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**.
7. После добавления всех нужных объектов нажмите на кнопку **ОК** в окне **Выбор объекта для проверки**.
8. Чтобы исключить какие-либо объекты из списка проверки, снимите флажок рядом с ними.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности .
4. Выберите пункт **Настройка** в раскрывшемся меню.
5. В открывшемся окне на закладке **Общие** в блоке **Типы файлов** выберите нужный параметр.

Использование эвристического анализа

По умолчанию проверка ведется на основе баз, содержащих описание известных угроз и методов лечения. Kaspersky Internet Security сравнивает найденный объект с записями в базах, в результате чего вы получаете однозначный ответ, является ли проверяемый объект вредоносным и к какому классу опасных программ он относится. Такой подход называется *сигнатурным анализом* и по умолчанию используется всегда.

В то же время каждый день появляются новые вредоносные объекты, записи о которых еще не попали в базы. Обнаружить такие объекты поможет эвристический анализ. Суть метода в анализе активности, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны до того, как их активность станет известна вирусным аналитикам.

Приложение уведомит вас об обнаружении вредоносного объекта. Следует отреагировать на уведомление выбором действия.

Дополнительно вы можете задать уровень детализации проверки. Уровень обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и временем проверки. Чем выше установлен уровень детализации проверки, тем больше ресурсов она потребует и больше времени займет.

- *Чтобы начать использовать эвристический анализ и задать уровень детализации проверки, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите флажок **Эвристический анализ** и ниже задайте уровень детализации проверки.

ОПТИМИЗАЦИЯ ПРОВЕРКИ

Чтобы сократить время проверки и увеличить скорость работы Kaspersky Internet Security, вы можете проверять только новые файлы и те, что изменились с момента предыдущего их анализа. Этот режим работы распространяется как на простые, так и на составные файлы.

- *Чтобы проверять только новые файлы и те, что изменились с момента предыдущего анализа, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ

Распространенной практикой сокрытия вирусов является их внедрение в составные файлы: архивы, базы данных, и т.д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Установочные пакеты и файлы, содержащие OLE-объекты, исполняются при открытии, что делает их более опасными, чем архивы. Обезопасить свой компьютер от исполнения вредоносного кода и, одновременно, снизить скорость проверки, вы можете отключив проверку архивов и включив проверку файлов данных типов.

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

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** установите флажки рядом с теми типами составных файлов, которые будет проверять приложение.

См. также

Проверка составных файлов большого размера 61

Проверка составных файлов большого размера

При проверке составных файлов большого размера их предварительная распаковка может занять много времени. Сократить время можно, если проводить проверку файлов в фоновом режиме. Если во время работы с таким файлом будет обнаружен вредоносный объект, Kaspersky Internet Security уведомит вас об этом.

Снизить время задержки доступа к составным файлам вы можете отключив распаковку файлов с размером, больше заданного. Проверка файлов при извлечении из архивов будет производится всегда.

- *Чтобы приложение распаковывало файлы больших размеров в фоновом режиме, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Антивирус**.
  3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
  6. В окне **Составные файлы** установите флажок **Распаковывать составные файлы в фоновом режиме** и задайте значение минимального размера файла в поле ниже.

- *Чтобы приложение не распаковывало составные файлы большого размера, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Антивирус**.
  3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
  6. В окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и задайте значение максимального размера файла в поле ниже.

См. также

Проверка составных файлов 60

Изменение режима проверки

Под режимом проверки понимается условие срабатывания Файлового Антивируса. По умолчанию приложение использует интеллектуальный режим, когда решение о проверке объекта принимается на основе операций, выполняемых с ним. Например, при работе с документом Microsoft Office приложение проверяет файл при

первом открытии и последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Вы можете изменить режим проверки объектов. Выбор режима зависит от того, с какими файлами вы работаете большую часть времени.

Чтобы изменить режим проверки объектов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим.

ТЕХНОЛОГИЯ ПРОВЕРКИ

Дополнительно вы можете задать технологию, которая будет использоваться Файловым Антивирусом:

- **iChecker**. Технология позволяет увеличить скорость проверки за счет исключения некоторых объектов. Исключение объекта из проверки осуществляется по специальному алгоритму, учитывающему дату выпуска баз приложения, дату предыдущей проверки объекта, а также изменение параметров проверки.

  Например, у вас есть файл архива, который был проверен приложением и ему 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 базы приложения, архив будет проверен повторно.

  Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а также применима только к объектам с известной приложению структурой (например, файлы exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Технология является развитием технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе, а также применима только к объектам, расположенным в файловой системе NTFS.

Чтобы изменить технологию проверки объектов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужное значение параметра.

Приостановка работы компонента: формирование расписания

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу Файлового Антивируса. Для того чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить отключение компонента в определенное время.

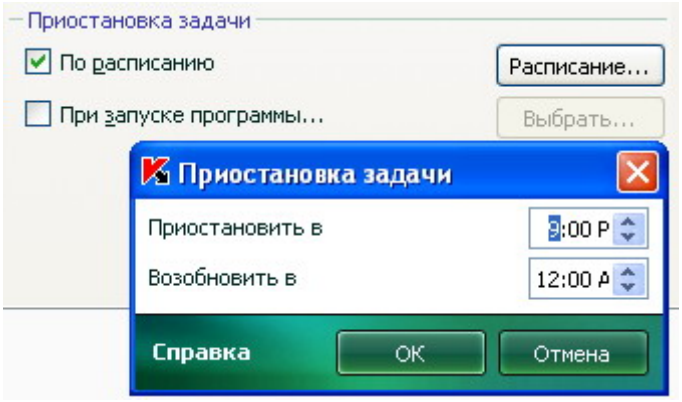

Рисунок 9: Формирование расписания

Чтобы настроить расписание приостановки работы компонента, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **По расписанию** и нажмите на кнопку **Расписание**.
6. В окне **Приостановка задачи** укажите время (в формате ЧЧ:ММ), в течение которого защита будет приостановлена (поля **Приостановить в** и **Возобновить в**).

См. также

Приостановка работы компонента: формирование списка приложений.....64

ПРИОСТАНОВКА РАБОТЫ КОМПОНЕНТА: ФОРМИРОВАНИЕ СПИСКА ПРИЛОЖЕНИЙ

При выполнении работ, требующих значительных ресурсов операционной системы, вы можете временно останавливать работу Файлового Антивируса. Для того чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить отключение компонента при работе с определенными программами.

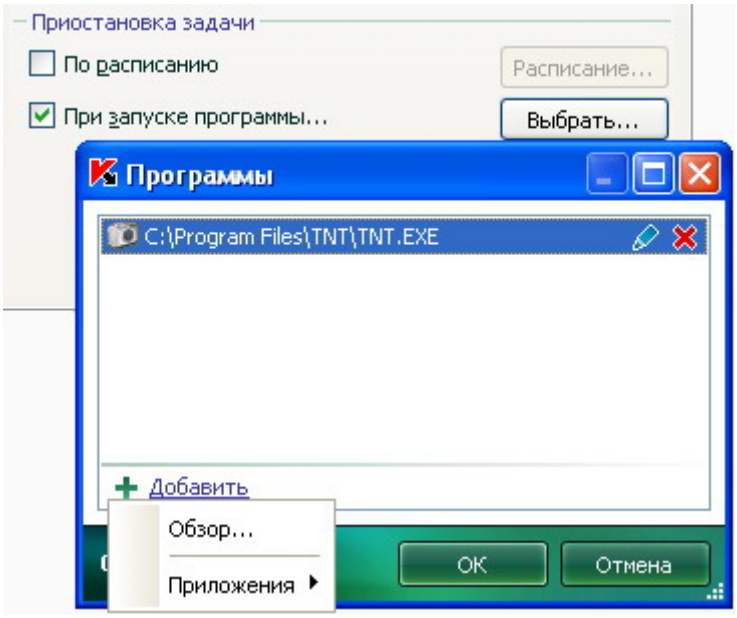

Рисунок 10: Формирование списка приложений

Настройка отключения Файлового Антивируса при конфликте с определенными приложениями - экстренная мера! В случае возникновения конфликтов при работе компонента обратитесь в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru). Специалисты поддержки помогут вам наладить совместную работу приложения с приложениями на вашем компьютере.

Чтобы настроить приостановку компонента на время работы указанных приложений, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Файловый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **При запуске программы** и нажмите на кнопку **Выбрать**.
6. В окне **Программы** сформируйте список приложений, при работе которых работа компонента будет приостановлена.

См. также

Приостановка работы компонента: формирование расписания.....63

ЗАЩИТА ПОЧТЫ

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 по протоколам POP3, SMTP, IMAP, MAPI и NNTP.

Проверка почты происходит с определенным набором параметров, который называется уровнем безопасности. При обнаружении угроз Почтовый Антивирус выполняет заданное действие. Правила, по которым осуществляется проверка вашей почты, определяются набором параметров. Их можно разбить на следующие группы:

- параметры, определяющие защищаемый поток сообщений;
- параметры, определяющие использование методов эвристического анализа;
- параметры, определяющие проверку составных файлов;
- параметры фильтрации вложенных файлов.

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

Вы можете восстановить параметры работы Почтового Антивируса по умолчанию, выберите один из уровней безопасности.

Чтобы изменить параметры работы Почтового Антивируса, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. Внесите необходимые изменения в настройки параметров компонента.

См. также

АЛГОРИТМ РАБОТЫ КОМПОНЕНТА

В состав Kaspersky Internet Security включен компонент, обеспечивающий защиту входящей и исходящей почты на наличие опасных объектов, - **Почтовый Антивирус**. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP, MAPI и NNTP, а также через защищенные соединения (SSL) по протоколам POP3 и IMAP.

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

По умолчанию защита почты осуществляется по следующему алгоритму:

1. Каждое письмо, принимаемое или отправляемое пользователем, перехватывается компонентом.

2. Почтовое сообщение разбирается на составляющие его части: заголовок письма, тело, вложения.

3. Тело и вложения почтового сообщения (в том числе вложенные OLE-объекты) проверяются на присутствие в нем опасных объектов. Распознавание вредоносных объектов происходит на основании баз, используемых в работе приложения, и с помощью эвристического алгоритма. Базы содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в базах.

4. В результате проверки на вирусы возможны следующие варианты поведения:

   - Если тело или вложение письма содержит вредоносный код, Почтовый Антивирус блокирует письмо, создает его резервную копию и пытается обезвредить объект. В результате успешного лечения письмо становится доступным для пользователя, если же лечение произвести не удалось, зараженный объект из письма удаляется. В результате антивирусной обработки в тему письма помещается специальный текст, уведомляющий о том, что письмо обработано приложением.

   - Если тело или вложение письма содержит код, похожий на вредоносный, но стопроцентной гарантии этого нет, подозрительная часть письма помещается в специальное хранилище - карантин.

   - Если в письме не обнаружено вредоносного кода, оно сразу же становится доступным для пользователя.

Для почтовой программы Microsoft Office Outlook предусмотрен встраиваемый модуль расширения (см. раздел «Проверка почты в Microsoft Office Outlook» на стр. 69), позволяющий производить более тонкую настройку проверки почты.

Если вы используете почтовую программу The Bat!, приложение может использоваться наряду с другими антивирусными приложениями. При этом правила обработки почтового трафика (см. раздел «Проверка почты плагином в The Bat!» на стр. 69) настраиваются непосредственно в программе The Bat! и превалируют над параметрами защиты почты приложения.

При работе с остальными почтовыми программами (в том числе 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 по протоколу IMAP, если используются фильтры, перемещающие сообщения из папки **Входящие**.

См. также

Защита почты.....65

ИЗМЕНЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ЗАЩИТЫ ПОЧТЫ

Под уровнем безопасности понимается предустановленный набор параметров Почтового Антивируса. Специалистами «Лаборатории Касперского» были сформированы три уровня безопасности. Решение о том, какой уровень выбрать, принимается вами на основе условий работы и сложившейся ситуации.

- Если вы работаете в опасной среде, то вам подходит высокий уровень безопасности почты. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты.

- Рекомендуемый уровень обеспечивает баланс между производительностью и безопасностью и подходит для большинства случаев. Рекомендуемый уровень установлен по умолчанию.

- Если вы работаете в хорошо защищенной среде, вам подходит низкий уровень безопасности. Примером такой среды может служить корпоративная сеть с централизованным обеспечением безопасности почты.

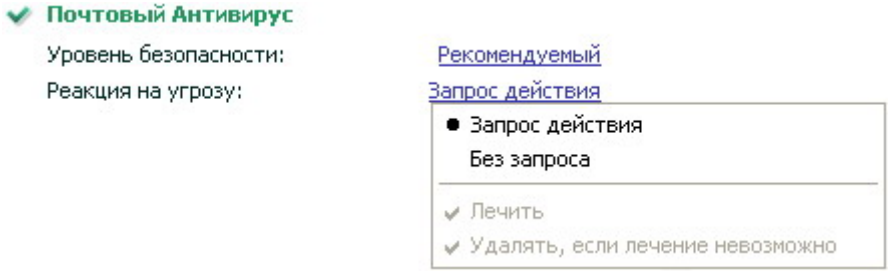

Рисунок 11: Изменение уровня безопасности

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы (см. раздел «Защита почты» на стр. 65) Почтового Антивируса. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы компонента по умолчанию, выберите один из предустановленных уровней.

Чтобы изменить установленный уровень безопасности почты, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Антивирус**.

3. Для компонента **Почтовый Антивирус** нажмите на ссылку с названием уровня безопасности.

4. В раскрывшемся меню выберите нужный уровень безопасности.

ИЗМЕНЕНИЕ ДЕЙСТВИЯ НАД ОБНАРУЖЕННЫМИ ОБЪЕКТАМИ

Почтовый Антивирус проверяет почтовое сообщение. Если в результате проверки выясняется, что письмо или какой либо его объект (тело, вложение) заражен или подозревается на заражение, дальнейшие операции компонента зависят от статуса объекта и выбранного действия.

Почтовый Антивирус в результате проверки присваивает найденным объектам один из следующих статусов:

- статус одной из вредоносных программ (см. раздел «Вредоносные программы» на стр. 17) (например, **вирус**, **троянская программа**).

- **возможно зараженный**, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Это означает, что в письме или его объекте обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

Если в результате проверки почты Kaspersky Internet Security находит зараженные или возможно зараженные объекты, то вы получаете уведомление об этом. Вам следует отреагировать на возникшую угрозу выбором

действия над объектом. Такое поведение приложения, когда в качестве действия над обнаруженным объектом выбран **Запрос действий**, задано по умолчанию. Вы можете изменить действие. Например, вы уверены, что каждый найденный объект следует пытаться вылечить, и не хотите каждый раз выбирать действие **Лечить** при получении уведомления об обнаружении зараженного или подозрительного объекта в письме. В этом случае вам следует выбрать действие **Без запроса. Лечить**.

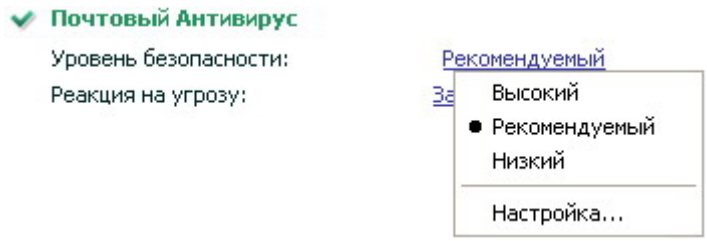

Рисунок 12: Изменение действия над объектом

Перед лечением или удалением зараженного объекта приложение формирует его резервную копию на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

Если вы работаете в автоматическом режиме (см. раздел «Шаг 2. Выбор режима защиты» на стр. 43), то приложение будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов. Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных - **Пропускать**.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с действием.
4. В раскрывшемся меню выберите нужное действие.

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Под областью защиты понимается тип сообщений, которые следует проверять. По умолчанию Kaspersky Internet Security проверяет как входящие, так и исходящие сообщения. При выборе проверки только входящих сообщений, следует помнить следующее: в самом начале работы с приложением рекомендуется проверять исходящую почту, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала собственного распространения. Это позволит избежать неприятностей, связанных с неконтролируемой рассылкой зараженных электронных сообщений с вашего компьютера.

К области защиты относятся также параметры интеграции Почтового Антивируса в систему и проверяемые протоколы. По умолчанию Почтовый Антивирус интегрируется в почтовые клиенты Microsoft Office Outlook и The Bat!.

Чтобы отключить проверку исходящей почты, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** задайте нужные значения параметров.

Проверка почты в Microsoft Office Outlook

Если в качестве почтового клиента вы используете Microsoft Office Outlook, вы можете дополнительно настроить проверку вашей почты на вирусы.

При установке приложения в Microsoft Office Outlook встраивается специальный модуль расширения. Он позволяет быстро перейти к настройке параметров Почтового Антивируса, а также определить, в какой момент времени почтовое сообщение будет проверено на присутствие опасных объектов.

Модуль расширения реализован в качестве специальной закладки **Защита почты**, расположенной в меню **Сервис → Параметры**. На закладке вы можете задать режимы проверки почты.

Чтобы задать режимы проверки почты, выполните следующие действия:

1. Откройте главное окно Microsoft Office Outlook.
2. В меню программы выберите пункт **Сервис → Параметры**.
3. На закладке **Защита почты** задайте нужный режим проверки почты.

Проверка почты плагином в The Bat!

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

Параметры Почтового Антивируса, определяющие проверять или нет входящую и исходящую почту, 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 модули, поддерживающие работу с The Bat!

Следует помнить, что при получении почтовые сообщения сначала проверяются Почтовым Антивирусом, и только потом плагином почтового клиента The Bat! При обнаружении вредоносного объекта приложение обязательно уведомит вас об этом. Если при этом выбрать действие **Лечить** (**Удалить**) в окне уведомления Почтового Антивируса, 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.

Вам нужно определить:

- какой поток почтовых сообщений подвергать проверке (входящий, исходящий);
- в какой момент времени будет производиться проверка объектов письма (при открытии письма, перед сохранением на диск);
- действия, предпринимаемые почтовым клиентом при обнаружении опасных объектов в почтовых сообщениях. Например, вы можете выбрать:
  - **Попробовать излечить зараженные части** - пытаться вылечить зараженный объект письма; если его вылечить невозможно, объект остается в письме.
  - **Удалить зараженные части** - удалить опасный объект письма, 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 в программе The Bat!

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

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

Использование эвристического анализа

Суть эвристического метода состоит в том, что анализу подвергается активность, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны до того, как их активность станет известна вирусным аналитикам. По умолчанию эвристический анализ включен.

Приложение уведомит вас об обнаружении вредоносного объекта в сообщении. Следует отреагировать на уведомление выбором действия.

Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте ползунок в одну из позиций: поверхностный, средний или глубокий.

Чтобы использовать / отключить эвристический анализ и задать уровень детализации проверки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите / снимите флажок **Эвристический анализ** и ниже задайте уровень детализации проверки.

Проверка составных файлов

Выбор режима проверки составных файлов влияет на производительность Kaspersky Internet Security. Вы можете включать или отключать проверку вложенных архивов, а также ограничивать максимальный размер проверяемых архивов.

Чтобы настроить параметры проверки составных файлов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** выберите режим проверки составных файлов.

Фильтрация вложений

Вы можете настроить условия фильтрации присоединенных к почтовому сообщению объектов. Использование фильтра обеспечит дополнительную безопасность вашему компьютеру, поскольку вредоносные программы распространяются через почту чаще всего в виде вложенных файлов. Переименование или удаление вложений определенного типа позволит защитить ваш компьютер от, например, автоматического запуска вложенного файла при получении сообщения.

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

Чтобы настроить параметры фильтрации вложений, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Почтовый Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Фильтр вложений** задайте условия фильтрации присоединенных к почтовому сообщению объектов. При выборе последних двух режимов становится активным список типов файлов, в котором вы можете отметить нужные типы или добавить маску нового типа.

   Если необходимо добавить маску нового типа, нажмите на ссылку **Добавить** и в открывшемся окне **Маска имени файла** введите необходимые данные.

Защита веб-трафика

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на вашем компьютере, риску заражения опасными программами. Они могут проникнуть на ваш компьютер, пока вы скачиваете бесплатные программы, просматриваете информацию на заведомо безопасных сайтах (которые до вашего посещения подверглись атаке хакеров). Более того, сетевые черви могут проникать на ваш компьютер до открытия веб-страницы или скачивания файла - непосредственно при установлении соединения с интернетом.

Для обеспечения безопасности вашей работы в интернете предназначен компонент *Веб-Антивирус*. Он защищает информацию, поступающую на ваш компьютер по HTTP-протоколу, а также предотвращает запуск на компьютере опасных скриптов.

Веб-защита предусматривает контроль HTTP-трафика, проходящего только через порты, указанные в списке контролируемых портов. Список портов, которые чаще всего используются для передачи почты и HTTP-трафика, включен в поставку приложения. Если вы используете порты, отсутствующие в данном списке, для обеспечения защиты проходящего через них трафика добавьте их в список.

Если вы работаете в незащищенном пространстве, рекомендуется использовать Веб-Антивирус для защиты вашей работы в интернете. Если же ваш компьютер работает в сети, защищенной сетевым экраном или фильтрами HTTP-трафика, Веб-Антивирус обеспечит дополнительную защиту работы в интернете.

Проверка трафика происходит с определенным набором параметров, который называется уровнем безопасности. При обнаружении угроз Веб-Антивирус выполняет заданное действие.

Уровень защиты веб-трафика на вашем компьютере определяется набором параметров. Их можно разбить на следующие группы:

- параметры, формирующие защищаемую область;
- параметры, определяющие производительность защиты трафика (использование эвристического анализа, оптимизация проверки).

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

Чтобы изменить параметры работы Веб-Антивируса, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. Внесите необходимые изменения в настройки параметров компонента.

См. также

АЛГОРИТМ РАБОТЫ КОМПОНЕНТА

Веб-Антивирус защищает информацию, поступающую на компьютер по HTTP-протоколу и предотвращает запуск на компьютере опасных скриптов.

Рассмотрим подробнее схему работы компонента. Защита HTTP-трафика обеспечивается по следующему алгоритму:

1. Каждая веб-страница или файл, к которому происходит обращение пользователя или некоторой программы по протоколу HTTP, перехватывается и анализируется Веб-Антивирусом на присутствие вредоносного кода. Распознавание вредоносных объектов происходит на основании баз, используемых в работе приложения, и с помощью эвристического алгоритма. Базы содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в базах.
2. В результате анализа возможны следующие варианты поведения:
   - Если веб-страница или объект, к которому обращается пользователь, содержат вредоносный код, доступ к нему блокируется. При этом на экран выводится уведомление о том, что запрашиваемый объект или страница заражена.
   - Если файл или веб-страница не содержат вредоносного кода, они сразу же становятся доступны для пользователя.

Проверка скриптов выполняется по следующему алгоритму:

1. Каждый запускаемый на веб-странице скрипт перехватывается Веб-Антивирусом и анализируется на присутствие вредоносного кода.

2. Если скрипт содержит вредоносный код, Веб-Антивирус блокирует его, уведомляя пользователя специальным всплывающим сообщением.

3. Если в скрипте не обнаружено вредоносного кода, он выполняется.

Для программы Microsoft Internet Explorer предусмотрен специальный модуль расширения, который встраивается в программу при установке приложения. О его наличии свидетельствует кнопка  в панели инструментов браузера. При нажатии на нее открывается информационная панель со статистикой Веб-Антивируса по количеству проверенных и заблокированных скриптов.

См. также

Защита веб-трафика 71

Изменение уровня безопасности HTTP-трафика

Под уровнем безопасности понимается предустановленный набор параметров Веб-Антивируса. Специалистами «Лаборатории Касперского» были сформированы три уровня безопасности. Решение о том, какой уровень выбрать, принимается вами на основе условий работы и сложившейся ситуации:

- Высокий уровень безопасности рекомендуется использовать в агрессивном окружении, когда не используются другие средства защиты HTTP-трафика.
- Рекомендуемый уровень безопасности является оптимальным для использования в большинстве случаев.
- Низкий уровень безопасности рекомендуется использовать, если на вашем компьютере установлены дополнительные средства защиты HTTP-трафика.

Рисунок 13: Изменение уровня безопасности

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы (см. раздел «Защита веб-трафика» на стр. 71) Веб-Антивируса. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы компонента по умолчанию, выберите один из предустановленных уровней.

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с названием уровня безопасности.
4. В раскрывшемся меню выберите нужный уровень безопасности.

ИЗМЕНЕНИЕ ДЕЙСТВИЯ НАД ОБНАРУЖЕННЫМИ ОБЪЕКТАМИ

Если в результате анализа объекта HTTP-трафика выясняется, что он содержит вредоносный код, дальнейшие операции Веб-Антивируса зависят от указанного вами действия.

Что касается действий над опасными скриптами, то Веб-Антивирус всегда блокирует их исполнение и выводит на экран всплывающее сообщение, уведомляющее пользователя о выполненном действии. Вы не можете изменить действие над опасным скриптом, кроме как отключить работу модуля проверки скриптов (см. раздел «Формирование области защиты» на стр. 74).

Рисунок 14: Изменение действия

Если вы работаете в автоматическом режиме (см. раздел «Шаг 2. Выбор режима защиты» на стр. 43), то приложение будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с действием.
4. В раскрывшемся меню выберите нужное действие.

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Под областью защиты понимается тип проверки объектов Веб-Антивирусом и список доверенных адресов, информация с которых не будет анализироваться компонентом на присутствие опасных объектов. По умолчанию Веб-Антивирус выполняет проверку HTTP-трафика и скриптов одновременно. Вы можете отключить любой из этих типов проверки.

Одновременное отключение проверки HTTP-трафика и скриптов останавливает работу Веб-Антивируса.

Вы можете сформировать список доверенных адресов, содержанию которых вы безоговорочно доверяете. Веб-Антивирус не будет анализировать информацию с данных адресов на присутствие опасных объектов. Такая возможность может быть использована в том случае, если Веб-Антивирус препятствует загрузке некоторого файла, блокируя попытки его скачать.

Чтобы изменить тип проверки объектов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **Общие** установите / снимите соответствующий нужному типу проверки флажок.

Чтобы сформировать список доверенных адресов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Доверенные адреса** нажмите на ссылку **Добавить**.
6. В открывшемся окне **Маска адреса (URL)** введите доверенный адрес (или его маску).

Использование эвристического анализа

Суть эвристического метода состоит в том, что анализу подвергается активность, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны до того, как их активность станет известна вирусным аналитикам. По умолчанию эвристический анализ включен.

Приложение уведомит вас об обнаружении вредоносного объекта в сообщении. Следует отреагировать на уведомление выбором действия.

Дополнительно вы можете выбрать уровень детализации проверки, для этого передвиньте ползунок в одну из позиций: поверхностный, средний или глубокий.

Чтобы использовать / отключить эвристический анализ и задать уровень детализации проверки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите / снимите флажок **Эвристический анализ** и ниже задайте уровень детализации проверки.

Оптимизация проверки

Для повышения уровня обнаружения вредоносного кода Веб-Антивирусом используется кеширование фрагментов объектов, поступающих из интернета. При использовании этого способа проверка объекта осуществляется только после его полного получения Веб-Антивирусом. Далее объект подвергается анализу на вирусы и по результатам анализа передается пользователю для работы либо блокируется.

Однако использование кеширования увеличивает время обработки объекта и передачи его пользователю для работы, а также может вызывать проблемы при копировании и обработке больших объектов, связанные с истечением тайм-аута на соединение HTTP-клиента.

Для решения этой проблемы мы предлагаем ввести ограничение на время кеширования фрагментов веб-объекта. При истечении этого ограничения каждая полученная часть файла будет передаваться пользователю непроверенной, а по завершении копирования объекта он будет проверен целиком. Это позволит уменьшить время передачи объекта пользователю, решить проблему разрыва соединения, не сокращая уровень безопасности работы в интернете.

По умолчанию настроено ограничение на время кеширования фрагментов файла в 1 секунду. Увеличение этого значения либо снятие ограничения времени кеширования приводит к повышению уровня антивирусной проверки, но и предполагает некоторое замедление предоставления доступа к объекту.

Чтобы задать ограничение на время кеширования фрагментов или снять это ограничение, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Для компонента **Веб-Антивирус** нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Производительность** установите / снимите флажок **Ограничить время кеширования фрагментов** и задайте время (в секундах) в поле справа.

КОНТРОЛЬ ПРИЛОЖЕНИЙ

В состав Kaspersky Internet Security входят компоненты, предназначенные для предотвращения выполнения приложениями опасных для системы действий. Эти компоненты постоянно находятся в оперативной памяти компьютера и проверяют используемые приложениями файлы, ключи реестра, устройства и сетевые соединения.

Фильтрация активности (на стр. 77) управляет доступом приложений к системным ресурсам. Правила, регулирующие доступ приложения к ресурсам, создаются при первом запуске приложения.

Сетевой экран (на стр. 87) защищает ваш компьютер от сетевых атак. Безопасность работы в сети обеспечивается за счет использования правил для сетевых пакетов, где на основании анализа параметров пакетов разрешается или блокируется сетевая активность.

Проактивная защита (на стр. 96) анализирует последовательность действий, выполняемых приложением. Это позволяет распознать новую угрозу, информация о которой отсутствует в базах Kaspersky Internet Security.

По умолчанию компоненты **Контроля приложений** запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить работу какого-либо компонента.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют **не отключать** компоненты **Контроля приложений**, поскольку это может привести к заражению вашего компьютера и потере данных.

Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. В правой части окна нажмите на галочку рядом с названием нужного компонента.
4. В открывшемся меню выберите пункт **Выключить**.

В ЭТОМ РАЗДЕЛЕ

ФИЛЬТРАЦИЯ АКТИВНОСТИ

Все приложения с точки зрения безопасности для системы можно разделить на три группы:

- **Заведомо безопасные**. В эту группу попадают приложения, разработанные известными производителями и снабженные цифровыми подписями. Таким приложениям можно позволить производить любые действия в системе.
- **Заведомо опасные**. В эту группу попадают известные на данный момент угрозы. Деятельность приложений этой группы необходимо блокировать.
- **Неизвестные**. В эту группу можно отнести приложения собственной разработки, без цифровой подписи. Такие приложения необязательно наносят вред системе. Принять однозначное решение о безопасности использования приложений этой группы можно только после запуска и анализа их поведения. До

принятия решения о безопасности неизвестного приложения разумным решением будет ограничение доступ к ресурсам системы.

Компонент Фильтрация активности регистрирует действия, совершаемые приложениями в системе, и регулирует деятельность приложений, исходя из того, к какой группе (см. раздел «Группы приложений» на стр. 81) он относит приложение. Для каждой группы приложений задан набор правил (см. раздел «Правила Фильтрации активности» на стр. 84). Эти правила регламентируют доступ приложений к различным ресурсам:

- файлам и папкам;
- ключам реестра;
- сетевым адресам;
- сетевым пакетам;
- устройствам;
- среде исполнения.

При обращении приложения к ресурсу Фильтрация активности проверяет наличие у приложения нужных прав доступа и выполняет действие, заданное правилом.

Чтобы изменить параметры работы Фильтрации активности, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.
4. В открывшемся окне внесите нужные изменения.

См. также

Алгоритм работы компонента

Для корректной работы компонента **Фильтрация активности** должно быть установлено соединение с интернетом. В противном случае на активность заведомо безопасных приложений могут быть наложены ограничения.

При первом запуске приложения **Фильтрация активности** исследует его по следующему алгоритму:

1. Отправляет контрольную сумму исполняемого файла в базу известных приложений, находящуюся на сервере «Лаборатории Касперского». Если в базе есть запись, соответствующая контрольной сумме, то приложение попадает в группу **Доверенные**.
2. Вычисляет рейтинг опасности приложения (см. раздел «Рейтинг опасности» на стр. 81). Рейтинг опасности позволяет классифицировать приложения, не имеющие цифровую подпись. Приложения с

низким рейтингом опасности попадают в группу **Слабые ограничения**. Если рейтинг приложения высок, Kaspersky Internet Security уведомит вас об этом и предложит выбрать группу, в которую следует поместить приложение.

Если у приложения отсутствует цифровая подпись и рейтинг опасности очень высок, то такие приложения считаются подозрительными. Если сигнатурный или эвристический анализ при этом признает приложение зараженным, то оно автоматически помещается в группу **Недоверенные**. Иначе Kaspersky Internet Security уведомляет вас о подозрительном приложении и позволяет выбрать группу, в которую следует поместить приложение. Фильтрация активности полностью блокирует деятельность таких приложений.

После выполнения всех проверок на экран выводится уведомление о решении, принятом относительно приложения. Для приложений, попавших в группу **Доверенные**, уведомление по умолчанию отключено.

При повторном запуске Kaspersky Internet Security **Фильтрация активности** выполняет следующие действия:

1. Проверяет наличие пути к исполняемому файлу запущенного приложения в списке известных приложений.

   - Если путь отсутствует в списке, приложение считается неизвестным. Фильтрация активности исследует его по приведенному выше алгоритму.

   - Если путь существует, Фильтрация активности переходит к следующему действию.

2. Проверка наличия контрольной суммы запущенного приложения в списке известных приложений.

   - Если контрольная сумма отсутствует в списке, Фильтрация активности проверяет цифровую подпись приложения.

     a. Если цифровая подпись отсутствует, приложение считается неизвестным. Фильтрация активности исследует его по приведенному выше алгоритму.

     b. Если цифровая подпись приложения присутствует, является корректной, и известна Фильтрация активности, то запущенное приложение считается обновлением известного приложения. Фильтрация активности обновляет информацию о приложении и применяет к нему существующее правило.

   - Если контрольная сумма совпадает с контрольной суммой из списка, Фильтрация активности применяет к приложению существующее правило.

Приложения могут быть перемещены или удалены, некоторые приложения, например инсталляционные пакеты, могут запускаться всего один раз. Правила для таких приложений могут засорять список. Фильтрации активности проверяет актуальность списка правил для приложений с определенной периодичностью. Во время этой проверки Фильтрация активности пересчитывает рейтинг опасности для приложения. В результате перерасчета рейтинга опасности возможны следующие ситуации:

1. Исполняемый файл приложения недоступен по пути, сохраненному в списке. В этом случае проверяется число запусков и время, прошедшее со времени последнего запуска приложения:

   - Если приложение запускалось один раз, правило для приложения удаляется из списка.

   - Если со времени последнего запуска прошло больше 30 дней, правило для приложения удаляется из списка.

2. Рейтинг опасности приложения не совпадает с ранее подсчитанным. В этом случае приложение перемещается в группу в соответствии с новым рейтингом опасности.

3. Рейтинг опасности приложения совпадает с ранее подсчитанным. В этом случае правило для приложения остается без изменений.

См. также

Наследование прав

В текущей версии продукта механизм наследования прав не применяется для сетевой активности приложений.

Важной частью компонента Фильтрация активности является механизм *наследования прав*. Этот механизм предотвращает использование доверенных приложений недоверенным или ограниченным в правах приложением для того, чтобы выполнить привилегированные действия.

Когда приложение пытается получить доступ к контролируемому ресурсу, Фильтрация активности анализирует права всех родительских процессов приложения на доступ к ресурсу. При этом выполняется *правило минимального приоритета*: при сравнении прав доступа приложения и родительского процесса к активности приложения будут применены права доступа с минимальным приоритетом.

Приоритет прав доступа:

1. **Разрешить**. Данные права доступа имеют высший приоритет.
2. **Запросить пользователя**.
3. **Блокировать**. Данные права доступа имеют низший приоритет.

Пример: троянская программа пытается использовать *regedit.exe* для изменения реестра Microsoft Windows. В правиле для троянской программы в качестве реакции на доступ к реестру установлено действие **Блокировать**, в правиле для *regedit.exe* – действие **Разрешить**.

В результате активность *regedit.exe*, запущенного троянской программой, будет заблокирована, так как права *regedit.exe* будут унаследованы от родительского процесса. При этом срабатывает правило минимального приоритета – действие будет заблокировано, несмотря на наличие разрешающих права у программы *regedit.exe*.

Если активность программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права (см. раздел «Быстрая настройка параметров правила» на стр. 86).

Вносить изменения в права родительского процесса программы следует только в том случае, если вы абсолютно уверены в том, что активность процесса не угрожает безопасности системы!

См. также

Рейтинг опасности

Для каждого приложения, запускаемого на вашем компьютере, Фильтрация активности вычисляет рейтинг опасности. *Рейтинг опасности* – показатель опасности приложения для системы, вычисленный на основе критериев двух типов:

- Статических. К таким критериям относятся информация об исполняемом файле приложения: наличие цифровой подписи, размер файла и другие критерии.

- Динамических. Эти критерии применяются во время моделирования работы приложения в виртуальном окружении (анализ вызовов приложением системных функций).

В соответствии со значениями рейтинга Фильтрация активности распределяет приложения по группам (см. раздел «Группы приложений» на стр. 81). Чем ниже рейтинг опасности, тем больше действий в системе разрешено приложению.

См. также

Алгоритм работы компонента 78

Наследование прав 80

Группы приложений 81

Группы приложений

Все запускаемые на компьютере приложения распределяются Фильтрацией активности по *группам*, исходя из уровня опасности для системы, и, следовательно, прав доступа приложений к ресурсам системы.

Есть четыре предустановленные группы приложений.

- **Доверенные**. Приложения, обладающие цифровой подписью доверенных производителей, или запись о которых присутствует в базе доверенных приложений. Для таких приложений не отграничений на действия, совершаемые в системе. Активность этих приложений контролируется **Проактивной защитой** и **Файловым Антивирусом**.

- **Слабые ограничения**. Приложения, не имеющие цифровой подписи доверенных производителей или соответствующих записей в базе доверенных приложений. Однако эти приложения имеют низкое значение рейтинга опасности (см. раздел «Рейтинг опасности» на стр. 81). Им разрешены некоторые операции, например: доступ к другим процессам, управление системой, скрытый доступ к сети. Для большинства операций необходимо разрешение пользователя.

- **Сильные ограничения**. Приложения, не имеющие цифровой подписи или записей в базе доверенных приложений. Эти приложения имеют высокое значение рейтинга опасности. Для большинства действий в системе приложениям этой группы требуется разрешение пользователя, некоторые действия таким приложениям запрещены.

- **Недоверенные**. Приложения, не имеющие цифровой подписи или записей в базе доверенных приложений. Эти приложения имеют очень высокое значение рейтинга опасности. Фильтрация активности блокирует любые действия таких приложений.

Приложения, отнесенные Фильтрацией активности к определенной группе, наследуют права доступа к ресурсам из правила (см. раздел «Правила Фильтрации активности» на стр. 84) группы.

Специалисты «Лаборатории Касперского» не рекомендуют перемещать приложения по группам. Вместо этого при необходимости измените права доступа приложения к конкретным ресурсам системы.

См. также

ВЫБОР РЕЖИМА РАБОТЫ КОМПОНЕНТА

Фильтрация активности управляет доступом приложений к ресурсам системы в одном из двух режимов:

- **Согласно правилам**. Контроль над действиями приложений осуществляется на основе правил Фильтрации активности. Этот режим используется по умолчанию.
- **Разрешать**. Разрешаются любые действия приложений над категорией ресурсов, для которой установлен такой режим работы. Правила для этой категории ресурсов не применяются.

Специалисты «Лаборатории Касперского» не рекомендуют устанавливать режим работы компонента в **Разрешать**. При этом вредоносное приложение может получить доступ к критически важным ресурсам системы.

Чтобы выбрать режим работы Фильтрации активности, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для одной из категорий ресурсов системы нажмите на ссылку с названием установленного режима работы **Фильтрации активности**.
4. В раскрывшемся меню выберите нужный режим.

См. также

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Категории ресурсов, контролируемые Фильтрацией активности, зависят от версии операционной системы.

Фильтрация активности управляет правами приложений на совершение действий над следующими категориями ресурсов:

Операционная система. В эту категорию входят:

- ключи реестра, содержащие параметры автозапуска;
- ключи реестра, содержащие параметры работы в интернете;

- ключи реестра, влияющие на безопасность системы;
- ключи реестра, содержащие параметры системных служб;
- системные файлы и папки;
- папки автозапуска.

Конфиденциальные данные. В эту категорию входят:

- файлы пользователя (папка My Documents, файлы cookies, данные об активности пользователя);
- файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ: интернет-браузеров, файловых менеджеров, почтовых клиентов, интернет-пейджеров и электронных кошельков.

Устройства. В эту категорию входят:

- USB-устройства: устройства хранения данных, игровые устройства, принтеры, клавиатуры, мыши и другие;
- Bluetooth-устройства: устройства Jabra, устройства Blusoleil и другие.

Системные привилегии. В эту категорию входят права:

- на доступ к другим процессам: управление процессами, внедрение в процесс и другие;
- на изменение системы: низкоуровневый доступ к дискам и файловой системе, снятие копий экрана, работа с реестром, доступ к хранилищу паролей, завершение работы Microsoft Windows, скрытый доступ к сети и другие.

Сети. В эту категорию входят сетевые соединения, обнаруженные в системе. Фильтрация активности контролирует сетевую активность приложений на самом низком уровне - путем разрешения или запрещения доступа к сетям с определенным статусом. Комплексное управление сетевой активностью приложений осуществляет компонент Сетевой экран.

По умолчанию Фильтрация активности управляет доступом приложений к важным ресурсам вашего компьютера. Вы можете расширить область защиты Фильтрации активности.

Внести изменения в список контролируемых устройств невозможно.

Чтобы расширить область защиты Фильтрации активности, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Фильтрация активности** нажмите на ссылку **Согласно правилам** для ресурсов компьютера.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Ресурсы** выберите группу ресурсов.
6. В нижней части дерева ресурсов добавьте группу защищаемых ресурсов по ссылке **Добавить**. Обратите внимание, что созданная группа будет входить в группу, которая была выделена в дереве ресурсов.
7. В дереве ресурсов выделите созданную группу.
8. В правой части окна нажмите на ссылку **Добавить** и выберите нужный тип ресурса в раскрывшемся меню:

- **Файл или папка**. В открывшемся окне **Выбор файла или папки** укажите файл или папку.
- **Ключ реестра**. В открывшемся окне **Выбор объекта в реестре** задайте защищаемый ключ реестра.
- **Сетевой сервис**. В открывшемся окне **Сетевой сервис** задайте параметры контролируемого сетевого соединения (см. раздел «Настройка параметров сетевого сервиса» на стр. 94).
- **IP-адрес(а)**. В открывшемся окне **Сетевые адреса** укажите защищаемый диапазон адресов.

После того, как ресурс добавлен в область защиты, вы можете изменить или удалить ресурс с помощью одноименных ссылок в нижней части закладок. Если вы хотите исключить ресурс из области защиты, снимите флажок слева от ресурса в правой части окна.

ИЗМЕНЕНИЕ ПРАВ ДОСТУПА К УСТРОЙСТВАМ

По умолчанию Фильтрация активности разрешает доступ по всем устройствам.

Чтобы изменить права доступа приложений к устройствам, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Устройства** в графе **Активность** вызовите контекстное меню.
5. В раскрывшемся меню выберите нужные права доступа.

См. также

Формирование области защиты 82

Наследование прав 80

ПРАВИЛА ФИЛЬТРАЦИИ АКТИВНОСТИ

Правило – набор реакций Фильтрации активности на действия приложением или группой приложений над контролируемыми ресурсами (см. раздел «Формирование области защиты» на стр. 82).

Возможные реакции компонента:

- **Унаследовать**. Фильтрация активности будет применять к активности приложения (группы) правило, заданное для группы, к которой отнесено приложение (группа). Данная реакция применяется по умолчанию.
- **Разрешить**. Фильтрация активности позволяет приложению (группе) совершать действие.
- **Блокировать**. Фильтрация активности не позволяет приложению (группе) совершать действие.
- **Запросить пользователя**. Фильтрация активности информирует пользователя о том, что приложение (группа) пытается выполнить действие, и запрашивает пользователя о дальнейших действиях.
- **Записать в отчет**. Информация об активности приложения и реакции Фильтрации активности будет записана в отчет. Добавление информации в отчет может быть использовано в комбинации с любым другим действием компонента.

По умолчанию приложение наследует права доступа из группы, в которую оно входит. Вы можете изменить правило для приложения. В этом случае параметры правила для приложения будут иметь более высокий приоритет, чем параметры правила для группы, в которую входит приложение.

См. также

Создание правила для приложения

Вы можете ограничить права приложения на совершение действий в системе до запуска этого приложения. Для этого нужно создать для него правило.

Чтобы добавить правило для приложения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Приложения** в графе **Программа** выберите группу, в которую вы хотите поместить приложение и нажмите на ссылку **Добавить**.
5. В открывшемся окне выберите исполняемый файл приложения. Приложение будет добавлено в группу. По умолчанию правило для приложения наследует параметры группового правила. Вы можете внести изменения в права доступа для приложения (см. раздел «Подробная настройка параметров правила» на стр. 86).

См. также

Создание сетевого правила для приложения

По умолчанию после первого запуска приложения Фильтрация активности относит приложение к одной из предустановленных групп (см. раздел «Группы приложений» на стр. 81). Групповое правило регламентирует доступ приложения к сетям с определенным статусом. Если вам необходимо особым образом обрабатывать доступ приложения к определенным сетевым сервисам, вы можете создать сетевое правило.

Чтобы создать правило, регулирующее сетевую активность приложения:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Приложения** в графе **Программа** выберите приложение.

5. В нижней части закладки нажмите на ссылку **Изменить**.

6. В открывшемся окне на закладке **Правила** в раскрывающемся списке выберите категорию **Сетевое правило** и нажмите на ссылку **Добавить**.

7. В открывшемся окне **Сетевое правило** задайте параметры пакетного правила.

8. Для созданного правила назначьте приоритет (см. раздел «Изменение приоритета правила» на стр. 96).

См. также

Правила Фильтрации активности 84

Быстрая настройка параметров правила

Правила Фильтрации активности применяются к действиям, совершаемым приложениями над ресурсами из области защиты (см. раздел «Формирование области защиты» на стр. 82). В каждую контролируемую категорию входит множество ресурсов. Для упрощения настройки прав доступа приложений к ресурсам системы вы можете изменить права доступа к отдельным категориям ресурсов.

Чтобы изменить права доступа к категориям ресурсов, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Контроль приложений**.

3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.

4. В открывшемся окне на закладке **Приложения** в графе **Программа** выберите приложение.

5. В графе, соответствующей нужной категории ресурсов, вызовите контекстное меню.

6. В раскрывшемся меню установите нужные права доступа.

См. также

Правила Фильтрации активности 84

Подробная настройка параметров правила

Правило Фильтрации активности применяется к большому количеству ресурсов системы и действиями над ними.

Чтобы конкретизировать права приложения на совершение действий с ресурсами системы, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Контроль приложений**.

3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.

4. В открывшемся окне на закладке **Приложения** в графе **Приложения** выберите приложение.

5. В нижней части окна нажмите на ссылку **Изменить**.

6. В открывшемся окне на закладке **Правила** выберите категорию ресурсов, для которой требуется подробная настройка прав доступа, с помощью раскрывающегося списка.

7. В графе, содержащей действия с защищаемыми ресурсами, вызовите контекстное меню.

8. В раскрывшемся меню выберите нужные права доступа.

См. также

Правила Фильтрации активности 84

Настройка исключений

При создании правила для приложения по умолчанию Фильтрация активности контролирует любые действия приложения: доступ к файлам и папкам, доступ к среде исполнения и доступ к сети. Вы можете исключить из проверки определенные действия приложений.

Чтобы исключить действия приложения из проверки, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Контроль приложений**.

3. Для компонента **Фильтрация активности** нажмите на ссылку **Настройка**.

4. В открывшемся окне на закладке **Приложения** в графе **Программа** выберите приложение.

5. В нижней части закладки нажмите на ссылку **Изменить**.

6. В открывшемся окне на закладке **Исключения** установите флажки, соответствующие исключаемым действиям. При исключении проверки сетевого трафика приложения настройте дополнительные параметры исключения.

Все исключения, созданные в правилах для приложений, доступны в окне настройки параметров приложения в разделе **Угрозы и исключения** (на стр. 172).

Если вы работаете с приложением, которое в процессе работы постоянно создает новые файлы (например, Microsoft Visual Studio), добавьте это приложение в исключения. Тогда Фильтрация активности не будет каждый раз при изменении файлов выводить на экран всплывающие сообщения. Для этого следует при задании исключения в окне **Тип угроз** указать имя угрозы (в данном случае - HIPS.Skip.Start), установить флажок **Дополнительные параметры** и задать дополнительный критерий исключения в поле ниже (C:\wincmd\WINCMD32.EXE).

См. также

Правила Фильтрации активности 84

Сетевой экран

Для обеспечения безопасности вашей работы в локальных сетях и интернете предназначен специальный компонент Kaspersky Internet Security - *Сетевой экран*. Он производит фильтрацию всей сетевой активности согласно правилам двух типов: *правилам для приложений* и *пакетным правилам*.

Сетевой экран анализирует параметры сетей, к которым вы подключаете компьютер. Если приложение работает в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 162), Сетевой экран при первом подключении запрашивает у вас статус подключенной сети. Если интерактивный режим

выключен, Сетевой экран определяет статус в зависимости от типа сети, диапазонов адресов и других характеристик. В зависимости от статуса сети Сетевой экран применяет различные правила для фильтрации сетевой активности.

Чтобы изменить параметры работы Сетевого экрана, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладках **Сетевые пакеты** и **Сети** измените параметры работы **Сетевого экрана**.

См. также

ВЫБОР РЕЖИМА РАБОТЫ КОМПОНЕНТА

Сетевой экран может работать в одном из следующих режимов:

- **Разрешить** - в этом режиме разрешается любая сетевая активность на вашем компьютере. Правила для пакетов данных и приложений не действуют. Рекомендуется устанавливать такой уровень в крайне редких случаях, когда не наблюдается активных сетевых атак, и вы абсолютно доверяете любой сетевой активности.
- **Согласно правилам** - в этом режиме сетевая активность на вашем компьютере регулируется правилами Сетевого экрана. Данный режим работы используется по умолчанию.
- **Заблокировать** - в этом режиме запрещена любая сетевая активность на вашем компьютере. Если установлен такой уровень, вы не сможете использовать ни один сетевой ресурс; программы, для работы которых требуется сетевое соединение, также не будут работать. Рекомендуется устанавливать такой уровень только в случае сетевых атак или при работе компьютера в незащищенной сети.

Чтобы изменить режим работы Сетевого экрана, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку с названием установленного режима работы.
4. В раскрывшемся меню выберите режим работы.

Изменение статуса сети

Все сетевые соединения на вашем компьютере контролируются Сетевым экраном. Каждому соединению Сетевой экран назначает определенный статус. В зависимости от статуса сети Сетевой экран применяет различные правила фильтрации сетевой активности.

При подключении новой сети Сетевой экран выводит на экран уведомление. Вам предлагается назначить *статус* обнаруженной сети, в зависимости от которого будет производиться фильтрация сетевой активности:

- **Публичная сеть (Интернет)**. Этот статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными приложениями, сетевыми экранами, фильтрами (например, для сети интернет-кафе). Пользователям таких сетей закрыт доступ к файлам и принтерам находящимся на вашем компьютере. Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям сети с таким статусом. Если вы разрешили удаленный доступ к рабочему столу, пользователи этой сети так же не смогут его получить. Фильтрация сетевой активности каждого приложения производится в соответствии с правилами для этого приложения. По умолчанию этот статус присвоен сети Интернет.

- **Локальная сеть**. Этот статус рекомендуется применять для сетей, пользователям которых вы доверяете доступ к файлам и принтерам на вашем компьютере (например, для внутренней корпоративной сети или домашней сети).

- **Доверенная сеть**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, сети, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность в рамках этой сети.

Виды сетевой активности, разрешенные для сетей с определенным статусом, зависят от параметров пакетных правил, установленных по умолчанию. Вы можете изменять эти правила.

Статус сети определяет набор правил, которые используются для фильтрации сетевой активности, относящейся к этой сети.

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и нажмите на ссылку **Изменить**.
5. В открывшемся окне на закладке **Свойства** выберите нужный статус из раскрывающегося списка.

См. также

Расширение диапазона адресов сети.....89

Выбор режима оповещения об изменениях сети.....90

Расширение диапазона адресов сети

Каждой сети соответствует один или несколько диапазонов IP-адресов. Если вы подключаетесь к сети, доступ к подсетям которой осуществляется через маршрутизатор, вы можете вручную добавить доступные через него подсети.

Пример: если вы подключаетесь к сети одного из офисов вашей компании, и хотите, чтобы правила фильтрации были одинаковы для офиса, к которому вы подключены напрямую, и для офисов, доступных через сеть.

Узнайте у администратора сети диапазоны адресов сетей этих офисов и добавьте их.

Чтобы расширить диапазон адресов сети, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и нажмите на ссылку **Изменить**.
5. В открывшемся окне на закладке **Свойства** в блоке **Дополнительные подсети** нажмите на ссылку **Добавить**.
6. В открывшемся окне **IP-адрес** задайте IP-адрес или маску адресов.

См. также

Изменение статуса сети 89

Выбор режима оповещения об изменениях сети 90

ВЫБОР РЕЖИМА ОПОВЕЩЕНИЯ ОБ ИЗМЕНЕНИЯХ СЕТИ

Параметры сетевых соединений могут меняться в ходе работы. Вы можете получать уведомления о следующих изменениях:

- При подключении к сети.
- При изменении соответствия MAC-адреса IP-адресу. Это уведомление открывается при изменении IP-адреса одного из компьютеров сети.
- При появлении MAC-адреса. Это уведомление открывается при добавлении нового компьютера в сеть.

Чтобы включить оповещение об изменениях параметров сетевого соединения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и нажмите на ссылку **Изменить**.
5. В открывшемся окне на закладке **Дополнительно** установите флажки для тех событий, о которых вы хотите получать уведомления.

Правила Сетевого экрана

Правило Сетевого экрана представляет собой действие, совершаемое Сетевым экраном при обнаружении попытки соединения с заданными параметрами: направлением и протоколом передачи данных, диапазоном адресов и портов, с которыми происходит соединение.

Сетевой экран работает на основе правил двух видов:

- *Пакетные правила* используются для ввода ограничений на пакеты и потоки данных независимо от приложений.
- *Правила для приложений* используются для ввода ограничений сетевой активности конкретного приложения. Такие правила позволяют тонко настраивать фильтрацию, когда, например, определенный тип потоков данных запрещен для одних приложений, но разрешен для других.

Пакетные правила имеют более высокий приоритет, чем правила для приложений. Если для одного и того же вида сетевой активности заданы и пакетные правила и правила для приложений, эта сетевая активность будет обрабатываться по правилам для пакетов.

См. также

Создание пакетного правила

Как правило, пакетные правила ограничивают входящую сетевую активность по определенным портам протоколов TCP и UDP, подвергают фильтрации ICMP-сообщения.

Пакетное правило состоит из набора условий и действий над пакетами и потоками данных, которые выполняются при соблюдении условий.

При создании пакетных правил помните, что они имеют приоритет над правилами для приложений (см. раздел «Правила Фильтрации активности» на стр. 84).

При формировании условий правила вы можете указывать сетевой сервис и сетевой адрес. В качестве сетевого адреса может использоваться IP-адрес или указываться статус сети. В последнем случае адреса берутся из всех сетей, подключенных в данный момент и имеющих указанный статус.

Чтобы создать пакетное правило, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.

4. В открывшемся окне на закладке **Сетевые пакеты** нажмите на ссылку **Добавить**.

5. В открывшемся окне **Сетевое правило** настройте параметры правила.

6. Для созданного правила назначьте приоритет (см. раздел «Изменение приоритета правила» на стр. 96).

После создания правила вы можете внести изменения в его параметры или удалить его с помощью ссылок в нижней части закладки. Чтобы отключить правило, снимите флажок рядом с его названием.

См. также

Создание правила для приложения

Сетевой экран анализирует активность каждого запускаемого на вашем компьютере приложения. В зависимости от рейтинга опасности, при первом запуске каждое приложение заносится о определенную группу:

- **Доверенным** приложениям разрешается любая сетевая активность независимо от статуса сети.
- Если приложение находится в группе **Слабые ограничения**, в неинтерактивном режиме ему разрешена любая сетевая активность. В интерактивном режиме на экран выводится уведомление, с помощью которого вы можете разрешить или запретить соединение или создать правило для приложения с помощью Мастера (см. раздел «Мастер создания правила» на стр. 93).
- Если приложение находится в группе **Сильные ограничения**, в неинтерактивном режиме ему запрещена любая сетевая активность. В интерактивном режиме на экран выводится уведомление, с помощью которого вы можете разрешить или запретить соединение или создать правило для приложения с помощью Мастера (см. раздел «Мастер создания правила» на стр. 93).
- **Недоверенным** приложениям запрещена любая сетевая активность.

Вы можете изменять правила как для целой группы, так и для конкретного приложения в группе, создавать дополнительные правила для более тонкой фильтрации сетевой активности.

Пользовательские правила для конкретных приложений имеют больший приоритет, чем правила, наследуемые от группы.

После анализа активности приложения Сетевой экран создает правила, регулирующие доступ приложения к сетям с определенным статусом. Вы можете создать дополнительные правила, управляющие сетевой активностью приложения более гибко.

Чтобы создать правило для приложения, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Контроль приложений**.

3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.

4. В открывшемся окне на закладке **Сетевые пакеты** выберите группу правил для приложения и нажмите на ссылку **Добавить**.

5. В открывшемся окне **Сетевое правило** настройте параметры правила.

6. Для созданного правила назначьте приоритет (см. раздел «Изменение приоритета правила» на стр. 96).

После создания правила вы можете внести изменения в его параметры или удалить его с помощью ссылок в нижней части закладки. Чтобы отключить правило, снимите флажок рядом с его названием.

См. также

Выбор действия, совершаемого правилом....93

Настройка параметров сетевого сервиса....94

Выбор диапазона адресов....95

Изменение приоритета правила....96

Создание пакетного правила....91

Мастер создания правила

В случае срабатывания правила, в котором в качестве действия выбрано **Запрос действия** (по умолчанию такое действие устанавливается для приложений, входящих группы (см. раздел «Группы приложений» на стр. 81) **Слабые** или **Сильные ограничения**), на экран выводится уведомление. В окне уведомления вы можете выбрать один из вариантов дальнейших действий:

- **Разрешить**.
- **Запретить**.
- **Создать правило**. При выборе этого варианта запускается *Мастер создания правила*, который поможет вам создать правило, регулирующее сетевую активность приложения.

Действие в сработавшем правиле можно изменить на **Разрешить** или **Запретить**, установив флажок **Запомнить для этого приложения**.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Выбор действия, совершаемого правилом

При применении правила Сетевой экран применяет к пакету или потоку данных одно из следующих действий:

- **Разрешить**.
- **Блокировать**.
- **Обработать по правилам приложения**. В этом случае обработка пакета или потока данных пакетным правилом прекращается. К соединению применяются правила для приложений.

Дополнительно вы можете включить режим **Записывать в журнал событий**, если вы хотите фиксировать информацию о попытке соединения и действиях Сетевого экрана в отчете.

Чтобы изменить действие, совершаемое Сетевым экраном, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сетевые пакеты** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Сетевое правило** в блоке **Действие** выберите действие.

См. также

Настройка параметров сетевого сервиса 94

Выбор диапазона адресов 95

Изменение приоритета правила 96

Создание пакетного правила 91

Создание правила для приложения 92

НАСТРОЙКА ПАРАМЕТРОВ СЕТЕВОГО СЕРВИСА

Параметры, характеризующие сетевую активность, для которой создается правило, описываются *сетевым сервисом*. Сетевой сервис имеет следующие параметры:

Название. Этот текст отображается в списке доступных для выбора сетевых сервисов.

Направление. Сетевой экран контролирует соединения по следующим направлениям:

- **Входящее**. Правило применяется для пакетов данных, принимаемых вашим компьютером. Не применяется в правилах для приложений.
- **Входящее (поток)**. Правило применяется для сетевого соединения, открытого удаленным компьютером.
- **Входящее / исходящее**. Правило применяется как ко входящему, так и к исходящему пакету или потоку данных, независимо от того, каким компьютером (вашим или удаленным) было инициировано сетевое соединение.
- **Исходящее**. Правило применяется для пакетов данных, передаваемым с вашего компьютера. Не применяется в правилах для приложений.
- **Исходящее (поток)**. Правило применяется только для сетевого соединения, открытого вашим компьютером.

Протокол. Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE. Если в качестве протокола был выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета.

Правилами для приложений контролируются соединения только по протоколам TCP и UDP.

Удаленные и локальные порты. Для протоколов TCP и UDP вы можете задать порты вашего и удаленного компьютера, соединение между которыми будет контролироваться.

В состав Kaspersky Internet Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения. При создании правил Сетевого экрана вы можете выбрать один из предустановленных сетевых сервисов или создать новый.

Чтобы настроить параметры сетевого соединения, которое обрабатывается правилом, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сетевые пакеты** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Сетевое правило** в блоке **Сетевой сервис** нажмите на ссылку **Добавить**.
6. В открывшемся окне **Сетевой сервис** настройте параметры сетевого соединения.

См. также

Выбор действия, совершаемого правилом 93

Выбор диапазона адресов 95

Изменение приоритета правила 96

Создание пакетного правила 91

Создание правила для приложения 92

Выбор диапазона адресов

Правило Сетевого экрана применяется к сетевым адресам:

- **Любой адрес**. Правило будет применяться к любому IP-адресу.
- **Адреса подсети со статусом**. Правило будет применяться к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный статус.
- **Адреса из группы**. Правило будет применяться к IP-адресам, входящим в заданный диапазон.

Чтобы задать диапазон IP-адресов, к которым будет применяться правило, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сетевые пакеты** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Сетевое правило** в блоке **Адреса** задайте диапазон адресов:
   a. В раскрывающемся списке выберите статус сети, если вы задали вариант **Адреса подсети со статусом**.

b. Выберите одну из существующих групп адресов, если вы задали вариант **Адреса из группы**. Если диапазон адресов ни одной из групп вам не подходит, создайте новую. Для этого нажмите на ссылку **Добавить** в нижней части блока и в открывшемся окне **Сетевые адреса** укажите адреса, входящие в группу.

См. также

Выбор действия, совершаемого правилом 93

Настройка параметров сетевого сервиса 94

Изменение приоритета правила 96

Создание пакетного правила 91

Создание правила для приложения 92

Изменение приоритета правила

Для каждого правила установлен приоритет выполнения. Приоритет правила определяется его положением в списке правил. Первое правило в списке обладает самым высоким приоритетом выполнения.

Каждое создаваемое вручную пакетное правило добавляется в конец списка пакетных правил.

Чтобы изменить приоритет правила, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Сетевой экран** нажмите на ссылку **Настройка**.
4. В открывшемся окне на закладке **Сетевые пакеты** выберите правило и переместите его на нужное место в списке с помощью ссылок **Вверх** и **Вниз**.

Правила для приложений сгруппированы по имени приложения, и приоритет правил распространяется только на определенную группу. Каждое создаваемое вручную правило для приложения имеет самый высокий приоритет.

См. также

Выбор действия, совершаемого правилом 93

Настройка параметров сетевого сервиса 94

Выбор диапазона адресов 95

Создание пакетного правила 91

Создание правила для приложения 92

Проактивная защита

Kaspersky Internet Security защищает не только от известных угроз, но и от новых, информация о которых отсутствует в базах приложения. Это обеспечивает специально разработанный компонент - *Проактивная защита*.

Превентивные технологии, на которых построена Проактивная защита, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред вашему компьютеру. В отличие от реактивных технологий, где анализ выполняется на основании записей баз приложения, превентивные технологии распознают новую угрозу на вашем компьютере по последовательности действий, выполняемой некоторой программой. Если в результате анализа активности последовательность действий приложения вызывает подозрение, Kaspersky Internet Security блокирует активность этого приложения.

Анализ активности производится для всех приложений, даже для выделенных в группу **Доверенных** компонентом Фильтрация активности (на стр. 77). Для таких приложений вы можете отключить уведомления Проактивной защиты.

В отличие от компонента Фильтрация активности, Проактивная защита реагирует именно на определенную последовательность действий программы. Например, при обнаружении таких действий как самокопирование некоторой программы на сетевые ресурсы, в каталог автозапуска, системный реестр, а также последующая рассылка копий, можно с большой долей вероятности предположить, что это программа – червь. К опасным последовательностям действий также относятся:

- действия, характерные для троянских программ;
- попытки перехвата ввода с клавиатуры;
- скрытая установка драйверов;
- попытки изменения ядра операционной системы;
- попытки создания скрытых объектов и процессов с отрицательными значениями идентификаторов (PID).

Чтобы изменить параметры работы Проактивной защиты, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Проактивная защита** нажмите на ссылку **Настройка**.
4. В открывшемся окне **Проактивная защита** внесите нужные изменения.

См. также

Настройка уведомлений об активности приложений

По умолчанию Проактивная защита реагирует на все подозрительные последовательности действий и уведомляет пользователя о тех из них, для которых установлены флажки.

Чтобы выбрать, о каких последовательностях действий вас будет уведомлять Проактивная защита, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Проактивная защита** нажмите на ссылку **Настройка**.
4. В открывшемся окне **Проактивная защита** установите флажки для тех последовательностей действий, о которых Проактивная защита будет информировать вас.

См. также

Группы приложений 81

Отключение уведомлений для доверенных приложений

Приложения, отнесенные компонентом **Фильтрация активности** в группу (см. раздел «Группы приложений» на стр. 81) **Доверенных**, не представляют опасности для системы. Однако их активность также контролируется Проактивной защитой.

Чтобы отключить уведомления Проактивной защиты об активности Доверенных приложений, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Для компонента **Проактивная защита** нажмите на ссылку **Настройка**.
4. В открывшемся окне **Проактивная защита** установите флажок **Не сообщать об обнаружении подозрительной активности приложений, имеющих цифровую подпись или содержащихся в базе известного ПО**.

ОНЛАЙН-ЗАЩИТА

Среди опасного программного обеспечения все большее распространение в последнее время получают программы, целью которых является:

- Кража вашей конфиденциальной информации (пароли, номера кредитных карт, важные документы и т.д.).
- Отслеживание ваших действий на компьютере, анализ установленного программного обеспечения.
- Несанкционированный доступ в интернет с вашего компьютера на веб-сайты различного содержания.

На кражу информации нацелены фишинг-атаки и перехватчики клавиатуры, на трату ваших средств и времени - программы автоматического дозвона на платные веб-сайты, программы-шутки, программы-рекламы. Защита от угроз, связанных с использованием сети интернет, является задачей компонентов группы Онлайн-защита.

В группу **Онлайн-защита** входят следующие компоненты:

Защита от сетевых атак (на стр. 99) предотвращает известные в настоящее время сетевые атаки (см. раздел «Виды обнаруживаемых сетевых атак» на стр. 100), которые используют как уязвимости операционной системы, так и иного установленного программного обеспечения системного и прикладного характера.

Анти-Фишинг (см. раздел «Защита от фишинга» на стр. 102) обеспечивает защиту от фишинг-атак.

Анти-Дозвон (см. раздел «Защита от скрытых телефонных звонков» на стр. 102) обеспечивает защиту от попыток несанкционированного модемного соединения.

По умолчанию все компоненты группы **Онлайн-защита** запускаются при старте операционной системы.

Чтобы отключить использование какого-либо из компонентов Онлайн-защиты, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. В правой части окна нажмите левой клавишей мыши на галочку рядом с названием нужного компонента.
4. В открывшемся меню выберите пункт **Выключить**.

Не рекомендуется отключать компоненты группы **Онлайн-защита**! Вы всегда можете настроить работу компонентов приложения таким образом, чтобы обеспечить безопасную и комфортную работу.

В ЭТОМ РАЗДЕЛЕ

ЗАЩИТА ОТ СЕТЕВЫХ АТАК

Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Если обнаружена попытка атаковать ваш компьютер, приложение

блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера. По умолчанию блокирование происходит на один час. На экран выводится уведомление (см. раздел «Уведомления» на стр. 193) о том, что была произведена попытка сетевой атаки с указанием информации об атакующем компьютере.

Описания известных на настоящее время сетевых атак (см. раздел «Виды обнаруживаемых сетевых атак» на стр. 100) и методы борьбы с ними приведены в базах приложения. Пополнение списка атак, обнаруживаемых **Защитой от сетевых атак**, выполняется в процессе обновления (см. раздел «Обновление» на стр. 142) баз.

См. также

Блокирование атакующих компьютеров

По умолчанию **Защита от сетевых атак** (на стр. 99) блокирует активность атакующего компьютера в течение часа.

- *Чтобы изменить время блокирования атакующего компьютера, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. Для компонента **Защита от сетевых атак** нажмите на ссылку с количеством заблокированных компьютеров.
4. В открывшемся окне **Заблокированные компьютеры** задайте время блокирования.

- *Чтобы отменить блокирование атакующего компьютера, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. Для компонента **Защита от сетевых атак** нажмите на ссылку с количеством заблокированных компьютеров.
4. В открывшемся окне **Заблокированные компьютеры** выберите заблокированный компьютер и нажмите на ссылку **Разблокировать**.

Виды обнаруживаемых сетевых атак

В настоящее время существует множество различных видов сетевых атак, которые используют как уязвимости операционной системы, так и иного установленного программного обеспечения системного и прикладного характера.

Чтобы своевременно обеспечивать безопасность компьютера, важно знать, какого рода сетевые атаки могут угрожать ему. Известные сетевые атаки можно условно разделить на три большие группы:

1. *Сканирование портов* – этот вид угроз сам по себе не является атакой, а обычно предшествует ей, поскольку является одним из основных способов получить сведения об удаленном компьютере. Этот способ заключается в сканировании UDP / TCP-портов, используемых сетевыми сервисами на интересующем 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

представление злоумышленнику о типе операционной системы на удаленном компьютере. А это, в свою очередь, еще сильнее ограничивает круг потенциальных атак и, соответственно, время, затрачиваемое на их проведение, а также позволяет попытаться использовать специфические для данной операционной системы уязвимости.

2. *DoS-атаки* или атаки, вызывающие отказ в обслуживании – это атаки, результатом которых является приведение атакуемой системы в нестабильное, либо полностью нерабочее состояние. Последствиями такого типа атак могут стать невозможность использования информационных ресурсов, 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 являются следующие атаки:

   - 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 и 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 тратит свои ресурсы полностью и перестает реагировать на другие попытки соединения.

3. *Атаки-вторжения*, целью которых является «захват» системы. Это самый опасный тип атак, поскольку в случае успешного выполнения система оказывается полностью под контролем злоумышленника.

   Данный тип атак применяется, когда необходимо получить конфиденциальную информацию с удаленного компьютера (например, номера кредитных карт, пароли) либо просто закрепиться в системе для последующего использования ее вычислительных ресурсов в целях злоумышленника (использование захваченной системы в зомби-сетях либо как плацдарма для новых атак).

   Данная группа является также самой большой по количеству включенных в нее атак. Их можно разделить на три подгруппы в зависимости от операционной системы: атаки на Microsoft Windows, атаки на Unix, а также общая группа для сетевых сервисов, использующихся в обеих операционных системах.

   Наиболее распространенными видами атак, использующих сетевые сервисы операционной системы, являются:

   - *атаки на переполнение буфера* – тип уязвимостей в программном обеспечении, возникающий из-за отсутствия контроля (либо недостаточном контроле) при работе с массивами данных. Это один из самых старых типов уязвимостей и наиболее простой для эксплуатации злоумышленником.

   - *атаки, основанные на ошибках форматных строк* – тип уязвимостей в программном обеспечении, возникающий 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, имея 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), в случае если они функционируют на компьютере пользователя.

Атаки под операционную систему 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 являются использование различного вида вредоносных скриптов, в том числе скриптов, обрабатываемых Microsoft Internet Explorer, а также разновидности червя Helkern. Суть последнего типа атаки заключается в отправке на удаленный компьютер UDP-пакета специального вида, способного выполнить вредоносный код.

ЗАЩИТА ОТ СКРЫТЫХ ТЕЛЕФОННЫХ ЗВОНКОВ

Анти-Дозвон контролирует попытки создания скрытых модемных соединений. Скрытым считается соединение, в параметрах которого задано не уведомлять пользователя о соединении, а также соединение, не инициируемое вами. Как правило, скрытые соединения устанавливают с платными телефонными номерами.

Каждый раз, когда выполняется попытка скрытого соединения, на экран выводится специальное уведомление (см. раздел «Уведомления» на стр. 193), сообщающее вам об этом. В данном уведомлении вам нужно определить, разрешить или запретить его. Если вы не инициировали такого соединения, высока вероятность, что это действие вредоносной программы. Если вы хотите разрешить скрытый дозвон на какой-либо номер, вам нужно включить его в список доверенных номеров.

Чтобы добавить номер в список доверенных, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. Для компонента **Анти-Дозвон** нажмите на ссылку с количеством доверенных номеров.
4. В открывшемся окне **Настройка: Доверенные номера** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Телефонный номер** задайте доверенный номер или маску.

ЗАЩИТА ОТ ФИШИНГА

Одним из видом мошенничества в интернете является создание копий сайтов финансовых структур с целью хищения денежных средств. Фишинг-атаки, как правило, представляют собой почтовые сообщения, содержащие ссылки на подложные сайты. Текст сообщения убеждает воспользоваться ссылкой и ввести на открывшемся сайте конфиденциальную информацию, например, номер кредитной карты или свои имя и пароль персональной страницы интернет-банка, где можно производить финансовые операции.

Частным примером фишинг-атаки является письмо от банка, клиентом которого вы являетесь, со ссылкой на официальный сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, однако реально находитесь на фиктивном сайте. Все ваши дальнейшие действия на сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Ссылка на фишинг-сайт может быть вам направлена не только письмом, но и другими доступными для этого способами, например, в тексте ICQ-сообщения.

Анти-Фишинг отслеживает попытки открытия фишинг-сайта и блокирует его. В состав баз Kaspersky Internet Security включены известные на настоящее время сайты, которые используются для фишинг-атак. Специалисты «Лаборатории Касперского» пополняют его адресами, предоставляемыми международной организацией по борьбе с фишингом (The Anti-Phishing Working Group). Данный список пополняется при обновлении баз приложения.

ФИЛЬТР СОДЕРЖИМОГО

В состав Kaspersky Internet Security входят компоненты, предназначенные для фильтрации трафика. При работе с электронной почты и интернет-ресурсами вы может столкнуться с фактами получения нежелательной информации (рекламные баннеры, текстовые рекламные объявления, навязчивые рассылки по электронной почте и др.). Получение нежелательных данных приводит к потере времени при загрузке веб-страниц и электронной почты и неоправданному увеличению объема интернет-трафика.

Анти-Спам (на стр. 103) обнаруживает нежелательную корреспонденцию (спам) и обрабатывает ее в соответствии с правилами вашего почтового клиента.

Анти-Баннер (на стр. 122) блокирует рекламную информацию, размещенную на баннерах в интернете или встроенных в интерфейс различных программ, установленных на вашем компьютере.

Родительский контроль (на стр. 124) позволяет контролировать доступ пользователей компьютера к интернет-ресурсам, содержащим информацию определенных категорий или являющимся потенциальной причиной потери денег.

По умолчанию все компоненты Фильтра содержимого, кроме Родительского контроля, запускаются при старте операционной системы. Вы можете отключить работу какого-либо компонента.

Не рекомендуется отключать компоненты **Фильтра содержимого**! Вы всегда можете настроить работу компонентов приложения таким образом, чтобы обеспечить безопасную и комфортную работу.

Чтобы отключить использование какого-либо из компонентов Фильтра содержимого, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. В правой части окна нажмите на галочку рядом с названием нужного компонента.
4. В открывшемся меню выберите пункт **Выключить**.

В ЭТОМ РАЗДЕЛЕ

Анти-Спам

В состав приложения включен компонент *Анти-Спам*, позволяющий обнаруживать нежелательную корреспонденцию (спам) и обрабатывать ее в соответствии с правилами вашего почтового клиента, экономя ваше время при работе с электронной почтой.

Анти-Спам использует самообучающийся алгоритм (см. раздел «Алгоритм работы компонента» на стр. 105), что позволяет компоненту с течением времени более точно различать спам и полезную почту. Источником данных для алгоритма является содержимое письма. Для того, чтобы Анти-Спам эффективно распознавал спам и полезную почту, обучите (см. раздел «Обучение Анти-Спама» на стр. 106) его.

Настоятельно рекомендуется изучить алгоритм работы Анти-Спама!

Анти-Спам встраивается в виде модуля расширения в следующие почтовые клиенты:

- Microsoft Office Outlook (см. раздел «Настройка обработки спама в Microsoft Office Outlook» на стр. 117).
- Microsoft Outlook Express (Windows Mail) (см. раздел «Настройка обработки спама в Microsoft Outlook Express (Windows Mail)» на стр. 119).
- The Bat! (см. раздел «Настройка обработки спама в The Bat!» на стр. 119).
- Thunderbird (см. раздел «Настройка обработки спама в Thunderbird» на стр. 120).

Путем формирования «белого» или «черного» списка адресов вы можете указать Анти-Спаму, письма с каких адресов считать полезными, а с каких - спамом. Кроме того, Анти-Спам может анализировать сообщение на наличие фраз из разрешенного (см. раздел «Формирование списка разрешенных фраз» на стр. 114) и запрещенного (см. раздел «Формирование списка запрещенных фраз» на стр. 116) списков.

Анти-Спам позволяет просматривать почту на сервере (см. раздел «Фильтрация писем на сервере. Диспетчер писем» на стр. 111) и удалять ненужные сообщения, не загружая их на ваш компьютер.

Чтобы изменить параметры работы Анти-Спама, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. Внесите необходимые изменения в настройки параметров компонента.

См. также

Алгоритм работы компонента

Работа компонента Анти-Спам разбита на два этапа:

- Сначала Анти-Спам применяет к сообщению жесткие критерии фильтрации. Эти критерии позволяют быстро определить, является сообщение спамом или нет. Анти-Спам присваивает сообщению статус **спам** или **не спам**, проверка останавливается и сообщение передается для обработки почтовому клиенту (см. ниже шаги 1 - 5).

- На следующих шагах работы алгоритма (см. ниже шаги 6 - 10) Анти-Спам изучает почтовые сообщения, прошедшие четкие критерии отбора предыдущих шагов. Такие сообщения уже нельзя однозначно расценивать как спам. Поэтому Анти-Спаму приходится вычислять *вероятность* того, что сообщение является спамом.

Рассмотрим подробнее алгоритм работы Анти-Спама:

1. Адрес отправителя почтового сообщения проверяется на присутствие в «черном» или «белом» списке адресов.

   - Если адрес отправителя находится в «белом» списке, сообщению присваивается статус **не спам**.

   - Если адрес отправителя находится в «черном» списке, почтовому сообщению присваивается статус **спам**.

2. Если сообщение было отправлено с помощью Microsoft Exchange Server и проверка таких сообщений отключена, то сообщению присваивается статус **не спам**.

3. Сообщение анализируется на наличие строк из «белого» списка. Если найдена хотя бы одна строка из этого списка, сообщению присваивается статус **не спам**.

4. Сообщение анализируется на наличие строк из «черного» списка. Обнаружение в сообщении слов из этого списка увеличивает вероятность того, что сообщение является спамом. Когда вычисленная вероятность превышает 100%, сообщению присваивается статус **спам**.

5. Если текст сообщения содержит адрес, входящий в базу **Анти-Фишинга** (см. раздел «Защита от фишинга» на стр. 102), письму присваивается статус **спам**.

6. Производится анализ почтового сообщения с помощью технологии PDB. При этом Анти-Спам сравнивает заголовки почтовых сообщений с образцами заголовков спам-сообщений. Каждое совпадение увеличивает вероятность того, что сообщение является спамом.

7. Производится анализ почтового сообщения с помощью технологии GSG. При этом Анти-Спам анализирует изображения в составе почтового сообщения. Если в изображениях, вложенных в сообщение, найдены признаки, характерные для спама, вероятность того, что сообщение является спамом, увеличивается.

8. Производится анализ почтового сообщения с помощью технологии Recent Terms. При этом Анти-Спам ищет в тексте сообщения фразы, характерные для спама. Эти фразы содержатся в обновляемых базах Анти-Спама. По окончанию анализа Анти-Спам вычисляет, насколько увеличилась вероятность того, что сообщение является спамом.

9. Выполняются проверки наличия дополнительных признаков (см. раздел «Использование дополнительных признаков фильтрации спама» на стр. 113), характерных для спама. Обнаружение каждого признака увеличивает вероятность того, что проверяемое сообщение является спамом.

10. Если было произведено обучение Анти-Спама, то сообщение проверяется с помощью технологии iBayes. Самообучающийся алгоритм iBayes подсчитывает вероятность того, что сообщение является спамом, на основе частоты появления в тексте сообщения фраз, характерных для спама.

Результатом анализа сообщения является **вероятность** того, что почтовое сообщение является спамом. Создатели спама постоянно совершенствуют маскировку спама, поэтому чаще всего вычисленная вероятность не достигает 100%. Для успешной фильтрации потока почтовых сообщений Анти-Спам использует два параметра:

- *фактор спама* - значение вероятности, при превышении которой сообщение считается **спамом**. Если вероятность меньше данного значения, то Анти-Спам присваивает сообщению статус **потенциальный спам**;

- *фактор потенциального спама* - значение вероятности, при превышении которой сообщение считается потенциальным спамом. Если вероятность меньше данного значения, то Анти-Спам расценивает сообщение как полезное.

В зависимости от заданных значений факторов спама и потенциального спама сообщения получают статус **спам** или **потенциальный спам**. Также сообщения получают метку **[!! SPAM]** или **[!! Probable Spam]** в поле **Тема** согласно присвоенному статусу. Затем они обрабатываются по правилам (см. раздел «Действия над нежелательной почтой» на стр. 117), которые вы задали для вашего почтового клиента.

ОБУЧЕНИЕ АНТИ-СПАМА

Одним из инструментов распознавания спама является самообучающийся алгоритм iBayes. Этот алгоритм выносит решение о статусе сообщения на основе входящих в него фраз. До начала работы алгоритму iBayes необходимо предоставить образцы строк, входящих в полезные и спам-сообщения, т.е. обучить его.

Существует несколько подходов к обучению Анти-Спама:

- Использование Мастера обучения (см. раздел «Обучение с помощью Мастера обучения» на стр. 107) (пакетное обучение). Обучение с помощью Мастера обучения предпочтительно в самом начале работы с Анти-Спамом.

- Обучение Анти-Спама на исходящих сообщениях (см. раздел «Обучение Анти-Спама на исходящих сообщениях» на стр. 108).
- Обучение непосредственно во время работы с электронной корреспонденцией (см. раздел «Обучение с помощью почтового клиента» на стр. 108), используя специальные кнопки в панели инструментов почтового клиента или пункты меню.
- Обучение при работе с отчетами Анти-Спама (см. раздел «Обучение с помощью отчетов» на стр. 109).

См. также

Обучение с помощью Мастера обучения

Мастер обучения позволяет провести обучение Анти-Спама в пакетном режиме, указав, какие папки учетных записей почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express содержат спам и полезную почту.

Для корректного распознавания спама необходимо произвести обучение как минимум на 50 письмах полезной почты и 50 письмах нежелательной корреспонденции. Без этого алгоритм iBayes работать не будет.

В целях экономии времени Мастер производит обучение только на 50 письмах в каждой выбранной папке.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку **обучить**.

При обучении на полезных письмах происходит добавление адреса отправителя письма в список разрешенных отправителей.

Чтобы отключить добавление адреса отправителя в «белый» список, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** снимите флажок **Добавлять адреса разрешенных отправителей при обучении Анти-Спама в почтовом клиенте**.

См. также

Обучение Анти-Спама на исходящих сообщениях

Вы можете обучить Анти-Спам на примере 50-ти исходящих сообщений. Адреса получателей этих сообщений будут автоматически занесены в «белый» список.

- *Чтобы обучить Анти-Спам на исходящих сообщениях, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. В блоке **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Исходящие сообщения** установите флажок **Обучаться на исходящих сообщениях**.

- *Чтобы отключить добавление адреса отправителя в «белый» список, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** снимите флажок **Добавлять адреса разрешенных отправителей при обучении Анти-Спама в почтовом клиенте**.

См. также

Обучение с помощью почтового клиента

Обучение в процессе непосредственной работы с электронной корреспонденцией предполагает использование специальных элементов интерфейса вашего почтового клиента.

Кнопки для обучения Анти-Спама появляются в интерфейсе почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express только после установки приложения. Если в процессе установки была отменена установка компонента Фильтр содержимого, кнопки для обучения Анти-Спама будут

недоступны.

Чтобы обучить Анти-Спам с помощью почтового клиента, выполните следующие действия:

1. Запустите почтовый клиент.
2. Выберите письмо, с помощью которого вы хотите обучить Анти-Спам.
3. Выполните одно из следующих действий в зависимости от того, каким почтовым клиентом вы пользуетесь:
   - Нажмите на кнопку **Спам** и **Не Спам** в панели инструментов Microsoft Office Outlook.
   - Нажмите на кнопку **Спам** и **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.

Анти-Спам проводит обучение на выбранном письме. Если вы выделяете несколько писем, то обучение происходит на всех выделенных письмах.

При отметке письма, как полезного, происходит добавление адреса отправителя письма в список разрешенных отправителей.

Чтобы отключить добавление адреса отправителя в «белый» список, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** снимите флажок **Добавлять адреса разрешенных отправителей при обучении Анти-Спама в почтовом клиенте**.

В случае, когда вы вынуждены выделять сразу несколько писем либо уверены, что некоторая папка содержит письма только одной группы (спам или не спам), возможен пакетный подход к обучению компонента с помощью Мастера обучения (см. раздел «Обучение Анти-Спама» на стр. 106).

См. также

Обучение с помощью отчетов

Предусмотрена возможность проводить обучение Анти-Спама, основываясь на его отчетах. Отчеты компонента позволяют сделать вывод о точности его настройки и, при необходимости, внести определенные коррективы в работу Анти-Спама.

Чтобы отметить некоторое письмо как спам или не спам, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. По ссылке **Отчеты** перейдите к окну отчетов приложения.
4. Для компонента **Анти-Спам** выберите письмо, на основе которого вы хотите провести дополнительное обучение.
5. Откройте контекстное меню для письма и выберите одно из следующих действий:
   - **Отметить как спам**.
   - **Отметить как не спам**.
   - **Добавить в «белый» список**.
   - **Добавить в «черный» список**.

См. также

Обучение с помощью Мастера обучения 107

Обучение Анти-Спама на исходящих сообщениях 108

Обучение с помощью почтового клиента 108

Изменение уровня агрессивности

Анти-Спам использует для фильтрации сообщений два показателя:

- *Фактор спама* - значение вероятности, при превышении которой сообщение считается спамом. Если вероятность меньше данного значения, то Анти-Спам присваивает сообщению статус **потенциальный спам**.
- *Фактор потенциального спама* - значение вероятности, при превышении которой сообщение считается потенциальным спамом. Если вероятность меньше данного значения, то Анти-Спам расценивает сообщение как полезное.

Под уровнем агрессивности понимается сочетание значений фактора спама и потенциального спама. Специалистами «Лаборатории Касперского» были сформированы три уровня агрессивности:

- **Высокий**. Данный уровень агрессивности следует использовать, если вы получаете спам слишком часто, например при использовании бесплатного почтового сервиса. При выборе этого уровня агрессивности может возрасти частота распознавания полезной почты как спама.
- **Средний**. Данный уровень агрессивности следует использовать в большинстве случаев.
- **Низкий**. Данный уровень агрессивности следует использовать, если вы редко получаете спам, например при работе в защищенной среде (системы корпоративной почты). При выборе этого уровня агрессивности может снизиться частота распознавания полезной почты как спама и потенциального спама.

Чтобы изменить установленный уровень агрессивности Анти-Спама, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. Для компонента **Анти-Спам** нажмите на ссылку с названием уровня агрессивности.

4. В раскрывшемся меню выберите нужный уровень агрессивности.

Фильтрация писем на сервере. Диспетчер писем

Вы можете просматривать список сообщений электронной почты на сервере, не загружая их на ваш компьютер. Это позволяет отказаться от приема некоторых сообщений, не только экономя ваше время и деньги при работе с электронной корреспонденцией, но и снижая вероятность загрузки спама и вирусов на ваш компьютер.

Для работы с письмами на сервере предназначен **Диспетчер писем**. Окно Диспетчера открывается каждый раз перед получением сообщений при условии, что он используется.

Окно Диспетчера писем открывается только при получении почты по протоколу POP3. Диспетчер писем не открывается, если POP3-сервер не поддерживает просмотр заголовков электронных сообщений, или все письма на сервере были отправлены пользователями из «белого» списка отправителей.

Список писем на сервере отображается в центральной части окна Диспетчера. Выберите сообщение в списке для детального изучения его заголовка. Просмотр заголовков может пригодиться, например, в следующей ситуации: спамеры устанавливают на компьютер вашего коллеги вредоносную программу, которая рассылает спам от его имени, пользуясь контакт-листом его почтового клиента. Вероятность того, что вы находитесь в контакт-листе вашего коллеги, весьма высока; это несомненно приведет к тому, что ваш ящик электронной почты будет переполнен спамом от вашего коллеги. В данной ситуации невозможно определить, используя лишь адрес отправителя, отправлено письмо вашим коллегой или спамером. Используйте заголовки письма! Просмотрите внимательно, кем отправлено данное письмо, когда и каков его объем. Проследите путь следования письма от отправителя до вашего почтового сервера. Вся эта информация должна быть в заголовках письма. Примите решение, действительно ли необходимо загружать данное письмо с сервера или все-таки лучше удалить его.

- *Чтобы использовать Диспетчер писем, выполните следующие действия:*

  1. Откройте главное окно приложения.

  2. В левой части окна выберите раздел **Фильтр содержимого**.

  3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.

  4. В раскрывшемся меню выберите пункт **Настройка**.

  5. В открывшемся окне на закладке **Общие** в блоке **Входящие сообщения** установите флажок **Открывать Диспетчер писем при получении почты по протоколу POP3**.

- *Чтобы удалить сообщения с сервера при помощи Диспетчера писем, выполните следующие действия:*

  1. В окне Диспетчера установите флажок напротив сообщения в столбце **Удалить**.

  2. В верхней части окна нажмите на кнопку **Удалить выбранные**.

Сообщение будут удалены с сервера. При этом вы получите уведомление, которое будет помечено как **[!! SPAM]** и обработано в соответствии с правилами вашего почтового клиента.

Исключение из проверки сообщений Microsoft Exchange Server

Вы можете исключить из проверки на спам почтовые сообщения, пересылаемые в рамках внутренней сети (например, корпоративная почта). Обратите внимание, что сообщения будут считаться внутренней почтой, если в качестве почтового клиента на всех компьютерах сети используется Microsoft Office Outlook, а почтовые ящики

пользователей расположены на одном Exchange-сервере, либо эти серверы должны соединяться X400-коннекторами.

По умолчанию Анти-Спам не проверяет сообщения Microsoft Exchange Server.

Чтобы Анти-Спам анализировал сообщения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Исключения** снимите флажок **Не проверять сообщения Microsoft Exchange Server**.

ВЫБОР ТЕХНОЛОГИЙ ФИЛЬТРАЦИИ СПАМА

Анализ почтовых сообщений на предмет спама осуществляется на основе использования современных технологий фильтрации.

По умолчанию используются все технологии фильтрации, что позволяет максимально полно проводить анализ почтового сообщения на спам.

Чтобы отключить использование какой-либо технологии фильтрации, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Алгоритмы** в блоке **Алгоритмы распознавания** снимите флажки напротив технологий фильтрации, которые вы не хотите использовать при анализе почтовых сообщений на спам.

ОПРЕДЕЛЕНИЕ ФАКТОРА СПАМА И ПОТЕНЦИАЛЬНОГО СПАМА

Специалисты «Лаборатории Касперского» постарались максимально полно настроить Анти-Спам на распознавание спама и потенциального спама.

Распознавание спама основано на использовании современных технологий фильтрации, позволяющих на определенном количестве писем вашего почтового ящика достаточно точно обучить Анти-Спам распознавать спам, потенциальный спам и полезную почту.

Обучение Анти-Спама производится при работе Мастера обучения, при обучении из почтовых клиентов. При этом каждому отдельному элементу полезной почты или спама присваивается некоторый коэффициент. Когда в ваш почтовый ящик поступает почтовое сообщение, по технологии iBayes, Анти-Спам проверяет письмо на наличие элементов спама и полезной почты. Коэффициенты каждого элемента спама (полезной почты) суммируются и вычисляется фактор спама и фактор потенциального спама.

Значение фактора потенциального спама определяет границу, после которой сообщению присваивается итоговый статус потенциальный спам. В случае использования **Рекомендуемого** уровня работы Анти-Спама любое письмо с фактором более 50% и менее 59% будет считаться потенциальным спамом. Полезной будет считаться почта, при проверке которой фактор будет менее 50%.

Значение фактора спама определяет границу, после которой сообщению присваивается итоговый статус спам. Любое письмо с фактором больше указанного, будет восприниматься как спам. По умолчанию для **Рекомендуемого** уровня фактор спама равен 59%. Это значит, что любое письмо с фактором более 59% будет отмечено как спам.

Чтобы откорректировать алгоритм работы Анти-Спама, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Алгоритмы** отрегулируйте факторы спама и потенциального спама в одноименных блоках.

Использование дополнительных признаков фильтрации спама

Кроме основных признаков, на основании которых производится фильтрация сообщений на спам (формирование «белого» и «черного» списков, анализ с помощью технологий фильтрации и др.), вы можете задавать дополнительные признаки. На основании этих признаков сообщению будет присвоен статус **спам** с той или иной степенью вероятности.

Спамом могут оказаться пустые сообщения (без темы и текста), сообщения содержащие ссылки на изображения или с вложенными изображениями, с текстом, совпадающим с цветом фона или с текстом, набранным мелким шрифтом. Также спамом могут быть письма с невидимыми символами (цвет текста совпадает с цветом фона), содержащие скрытые элементы (элементы не отображаются вообще) или некорректные html-теги, а также письма, содержащие скрипты (последовательности инструкций, выполняющихся при открытии письма пользователем).

Чтобы настроить дополнительные признаки фильтрации почты, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Алгоритмы** нажмите на кнопку **Дополнительно**.
6. В открывшемся окне **Дополнительно** установите флажок рядом с нужными признаками спам-сообщений. Для включенных дополнительных признаков задайте фактор спама (в процентах), который определяет вероятность, с которой письмо будет классифицировано как спам. По умолчанию фактор спама равен 80%. Сообщение будет отмечено как спам, если сумма вероятностей по всем дополнительным признакам превысит 100%.

   Если вы включаете фильтрацию по признаку «увеличивать спам-фактор для сообщений адресованных не мне», вам потребуется указать список ваших доверенных адресов. Для этого нажмите на кнопку **Мои адреса**. В открывшемся окне **Мои адреса** укажите нужные адреса или маски адресов. При анализе сообщения Анти-Спам проверит адрес получателя. В случае если адрес не совпадет ни с одним адресом из вашего списка, сообщению будет присвоен статус **спам**.

ФОРМИРОВАНИЕ «БЕЛОГО» СПИСКА АДРЕСОВ

В «белом» списке адресов хранятся адреса отправителей писем, от которых, как вы считаете, спама приходить не должно. Заполнение «белого» списка адресов выполняется автоматически во время обучения компонента Анти-Спам. Вы можете откорректировать данный список.

В качестве адреса вы можете задавать как адреса, так и маски адресов. При вводе маски можно использовать символы ***** и **?** (где ***** – любая последовательность символов, а **?** – любой один символ). Примеры масок адресов:

- *ivanov@test.ru* – почтовые сообщения от отправителя с таким адресом всегда классифицируются как полезная почта.
- **@test.ru* – почта от любого отправителя почтового домена *test.ru* является полезной; например: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@** – отправитель с таким именем, независимо от почтового домена, всегда отправляет только полезную почту; например: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test** – почта любого отправителя почтового домена, начинающегося с *test*, не является спамом; например: *ivanov@test.ru*, *petrov@test.com*.
- *ivan.*@test.???* – почта от отправителя, имя которого начинается на *ivan.* и имя почтового домена которого начинается на *test* и оканчивается на последние три любых символа, всегда является полезной; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Чтобы сформировать «белый» список адресов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** установите флажок **Считать полезными письма от следующих адресатов** и уажмите на ссылку **Добавить**.
6. В открывшемся окне **Маска адреса электронной почты** введите нужный адрес или маску.

ФОРМИРОВАНИЕ СПИСКА РАЗРЕШЕННЫХ ФРАЗ

В «белом» списке разрешенных фраз хранятся ключевые фразы писем, которые вы отметили как не спам. Вы можете сформировать такой список.

В качестве фразы можно использовать маски. При вводе маски вы можете использовать символы ***** и **?** (где ***** – любая последовательность символов, а **?** – любой один символ). Примеры фраз и масок фраз:

- *Привет, Иван!* – письмо, содержащее только этот текст, является полезным. Не рекомендуется использовать подобного рода строки.
- *Привет, Иван!** – письмо, начинающееся со строки *Привет, Иван!*, является полезным.
- *Привет, *! ** – почтовое сообщение, начинающееся с приветственного слова *Привет* и восклицательного знака в любом месте письма, не является спамом.
- ** Иван? ** – письмо содержит обращение к пользователю с именем Иван, после имени которого идет любой символ, и не является спамом.
- ** Иван\? ** – почтовое сообщение, содержащее строку *Иван?*, является полезным.

Если символы * и ? входят в состав фразы, чтобы не возникло ошибки их восприятия Анти-Спамом, следует использовать предшествующий отменяющий символ \. В этом случае вместо одного символа используются два: *и \?.

Чтобы сформировать список разрешенных фраз, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные фразы** установите флажок **Считать полезными письма со следующими фразами** и нажмите на ссылку **Добавить**.
6. В открывшемся окне **Разрешенная фраза** введите нужную строку или маску.

Импорт адресов «белого» списка

Для адресов «белого» списка предусмотрена возможность импорта из файлов формата **.txt*, **.csv* или адресной книги Microsoft Office Outlook / Microsoft Outlook Express.

Чтобы импортировать список разрешенных адресов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** нажмите на ссылку **Импортировать**.
6. В раскрывшемся меню выберите источник для импорта:
   - Если вы выбрали пункт меню **Импортировать из файла**, то вам будет предложено окно выбора файла. Приложение поддерживает импорт из файлов типа *.csv* или *.txt*.
   - Если вы выбрали пункт меню **Импортировать из адресной книги**, то откроется окно выбора адресной книги. Выберите в этом окне нужную адресную книгу.

Формирование «черного» списка адресов

В «черном» списке адресов хранятся адреса отправителей писем, которые вы отметили как спам. Список заполняется вручную.

В качестве адреса вы можете задавать как адреса, так и маски адресов. При вводе маски можно использовать символы ***** и **?** (где ***** – любая последовательность символов, а **?** – любой один символ). Примеры масок адресов:

- *ivanov@test.ru* – почтовые сообщения от отправителя с таким адресом всегда классифицируются как спам.
- **@test.ru* – почта от любого отправителя почтового домена *test.ru* является спамом; например: *petrov@test.ru*, *sidorov@test.ru*.

- *ivanov@** – отправитель с таким именем, независимо от почтового домена, всегда отправляет только спам; например: *ivanov@test.ru*, *ivanov@mail.ru*.

- **@test** – почта любого отправителя почтового домена, начинающегося с *test*, является спамом; например: *ivanov@test.ru*, *petrov@test.com*.

- *ivan.*@test.???* – почта от отправителя, имя которого начинается на *ivan.* и имя почтового домена которого начинается на *test* и оканчивается на последние три любых символа, всегда является спамом; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Чтобы сформировать «черный» список адресов и использовать его в своей дальнейшей работе, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **«Черный» список** в блоке **Запрещенные отправители** установите флажок **Считать спамом письма от следующих адресатов** и нажмите на ссылку **Добавить**.
6. В открывшемся окне **Маска адреса электронной почты** введите нужный адрес или маску.

ФОРМИРОВАНИЕ СПИСКА ЗАПРЕЩЕННЫХ ФРАЗ

В «черном» списке отправителей хранятся ключевые фразы писем, которые, как вы считаете, являются спамом. Список заполняется вручную.

В качестве фразы можно использовать маски. При вводе маски вы можете использовать символы ***** и **?** (где ***** – любая последовательность символов, а **?** – любой один символ). Примеры фраз и масок фраз:

- *Привет, Иван!* – письмо, содержащее только этот текст, является спамом. Не рекомендуется использовать подобного рода строки.

- *Привет, Иван!** – письмо, начинающееся со строки *Привет, Иван!*, является спамом.

- *Привет, *! ** – почтовое сообщение, начинающееся с приветственного слова *Привет* и восклицательного знака в любом месте письма, является спамом.

- *** Иван? *** – письмо содержит обращение к пользователю с именем Иван, после имени которого идет любой символ, и является спамом.

- *** Иван\? ** – почтовое сообщение, содержащее строку *Иван?*, является спамом.

Если символы * и ? входят в состав фразы, чтобы не возникло ошибки их восприятия Анти-Спамом, следует использовать предшествующий отменяющий символ \. В этом случае вместо одного символа используются два: *и \?.

Чтобы сформировать список запрещенных фраз, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Спам** нажмите на ссылку с установленным уровнем агрессивности.
4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **«Черный» список** в блоке **Запрещенные фразы** установите флажок **Считать спамом письма со следующими фразами** и нажмите на ссылку **Добавить**.

6. В открывшемся окне **Запрещенная фраза** введите нужную строку или маску.

Действия над нежелательной почтой

Если в результате проверки выясняется, что письмо является спамом или потенциальным спамом, дальнейшие операции Анти-Спама зависят от статуса объекта и выбранного действия. По умолчанию электронные сообщения, являющиеся спамом или потенциальным спамом, модифицируются: в поле **Тема** письма добавляется метка **[!! SPAM]** или **[?? Probable Spam]**, соответственно.

Вы можете выбрать дополнительные действия над спамом и потенциальным спамом. В почтовых клиентах Microsoft Office Outlook (см. раздел «Настройка обработки спама в Microsoft Office Outlook» на стр. 117) и Microsoft Outlook Express (Windows Mail) (см. раздел «Настройка обработки спама в Microsoft Outlook Express (Windows Mail)» на стр. 119) для этого предусмотрены специальные модули расширения. Для почтовых клиентов The Bat! (см. раздел «Настройка обработки спама в The Bat!» на стр. 119) и Thunderbird (см. раздел «Настройка обработки спама в Thunderbird» на стр. 120) вы можете настроить правила фильтрации.

См. также

Настройка обработки спама в Microsoft Office Outlook

Окно настройки обработки спама открывается автоматически при первой загрузке почтового клиента после установки приложения.

По умолчанию почтовая корреспонденция, которая классифицируетсяАнти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**.

Как для спама, так и для потенциального спама вы можете задать следующие правила обработки:

- **Поместить в папку** - нежелательная почта перемещается в указанную вами папку почтового ящика.
- **Скопировать в папку** - создается копия почтового сообщения и помещается в указанную папку. Оригинальное письмо остается в папке **Входящие**.
- **Удалить** - удалить нежелательную почту из почтового ящика пользователя.
- **Пропустить** - оставить почтовое сообщение в папке **Входящие**.

Для этого в блоке **Спам** или **Потенциальный спам** выберите соответствующее значение из раскрывающегося списка.

При обучении Анти-Спамас помощью почтового клиента (см. раздел «Обучение с помощью почтового клиента» на стр. 108) отмеченное письмо отправляется в «Лабораторию Касперского» как образец спама. Нажмите на ссылку **Дополнительно при отметке вручную писем как спам**, чтобы выбрать режим отправки образцов спама в открывшемся окне.

Также вы можете указать алгоритм совместной работы программы Microsoft Office Outlook и плагина Анти-Спама:

- **Проверять при получении**. Все сообщения, поступающие в почтовый ящик пользователя, сначала обрабатываются в соответствии с настроенными правилами Microsoft Office Outlook. По завершении этой обработки оставшиеся сообщения, не подпадающие ни под одно правило, передаются на обработку модулю расширения Анти-Спама. То есть обработка сообщений происходит в соответствии с очередностью. Иногда эта очередность может нарушаться, например, при одновременном поступлении большого количества писем в почтовый ящик. В результате этого могут возникать ситуации, что информация о письме, обработанном правилом Microsoft Office Outlook, заносится в отчет Анти-Спама со статусом **спам**. Во избежание этого мы рекомендуем настроить работу плагина Анти-Спама в качестве правила Microsoft Office Outlook.

- **Использовать правило Microsoft Office Outlook**. В данном случае обработка сообщений, поступающих в почтовый ящик пользователя, осуществляется на основе иерархии сформированных правил программы Microsoft Office Outllok. В качестве одного из правил должно быть создано правило обработки сообщений Анти-Спамом. Это оптимальный алгоритм работы, при котором не возникает конфликтов между программами Microsoft Outlook и модулем расширения Анти-Спама. Единственный недостаток данного алгоритма: создание и удаление правила обработки сообщений на спам через программу Microsoft Office Outlook осуществляется вручную.

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 приложения. Команда вызова мастера зависит от вашей версии Microsoft Office Outllok. 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**. И в открывшемся окне выберите из раскрывающегося списка 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 каждому правилу. Правила начинают применяться с начала списка, каждое последующее правило имеет приоритет ниже, чем предыдущее. Вы можете понижать или повышать приоритет применения правил к сообщению.

Если вы не хотите, чтобы после выполнения какого-либо правила сообщение дополнительно обрабатывалось правилом Анти-Спама, требуется в параметрах этого правила установить флажок **остановить дальнейшую обработку правил** (см. шаг третий окна создания правил).

Если вы имеете опыт создания правил обработки электронных сообщений в Microsoft Office Outlook, вы можете создать собственное правило для Анти-Спама на основе предложенного выше алгоритма.

Параметры обработки спама и потенциального спама в Microsoft Office Outlook приведены на специальной закладке **Анти-Спам** в меню **Сервис→Параметры**.

Настройка обработки спама в Microsoft Outlook Express (Windows Mail)

Окно настройки обработки спама открывается при первом запуске почтового клиента после установки приложения.

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**.

Как для спама, так и для потенциального спама вы можете задать следующие правила обработки:

- **Поместить в папку** - нежелательная почта перемещается в указанную вами папку почтового ящика.
- **Скопировать в папку** - создается копия почтового сообщения и помещается в указанную папку. Оригинальное письмо остается в папке **Входящие**.
- **Удалить** - удалить нежелательную почту из почтового ящика пользователя
- **Пропустить** - оставить почтовое сообщение в папке **Входящие**.

Для этого в блоке **Спам** или **Потенциальный спам** выберите соответствующее значение из раскрывающегося списка.

При обучении Анти-Спама с помощью почтового клиента (см. раздел «Обучение с помощью почтового клиента» на стр. 108) отмеченное письмо отправляется в «Лабораторию Касперского» как образец спама. Нажмите на ссылку **Дополнительно при отметке вручную писем как спам**, чтобы выбрать режим отправки образцов спама в открывшемся окне.

Окно настройки обработки спама доступно по кнопке **Настройка**, расположенной рядом с другими кнопками Анти-Спама в панели задач: **Спам** и **Не Спам**.

Настройки обработки спама хранятся в виде правил Microsoft Outlook Express, поэтому для сохранения изменений необходимо перезапустить Microsoft Outlook Express.

Настройка обработки спама в The Bat!

Действия над спамом и потенциальным спамом в почтовом клиенте The Bat! определяются средствами самого клиента.

Для того 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 пункт **Защита от спама**.

Представленные параметры защиты от спама распространяются на все установленные на компьютере анти-спам-модули, поддерживающие работу с The Bat!

Вам нужно определить уровень рейтинга и указать, как поступать с сообщениями определенного рейтинга (в случае Анти-Спама - вероятности того, что письмо является спамом):

- Удалять сообщения с рейтингом более указанной величины.
- 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 статус спама и потенциального спама письму 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. Для того чтобы не было расхождений между фактором спама в Kaspersky Internet Security и в The Bat!, все проверенные Анти-Спамом письма приводятся к рейтингу, соответствующему статусу письма: полезная почта - 0%, потенциальный спам - 50%, спам - 100%.

Таким образом, рейтинг письма в почтовом клиенте The Bat! соответствует не фактору письма, заданному в Анти-Спаме, а фактору соответствующего статуса.

Подробнее о рейтинге спама и правилах обработки см. документацию к почтовому клиенту The Bat!

НАСТРОЙКА ОБРАБОТКИ СПАМА В THUNDERBIRD

По умолчанию, почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. В Thunderbird для выполнения действий над такими письмами необходимо воспользоваться правилами меню **Инструменты→Фильтры сообщений** (подробнее о работе с почтовым клиентом см. справку Mozilla Thunderbird).

Модуль расширения Анти-Спама для Thunderbird позволяет осуществлять 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-Спамдля их проверки при выполнении команды меню **Инструменты→Запустить в папке антиспам-фильтры**. Таким образом, вместо Thunderbird проверкой сообщений занимается Kaspersky Internet Security. При этом функционал 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 (на стр. 103) отключен. При двойном нажатии на значок открывается окно настройки параметров Kaspersky Internet Security. По нажатию на кнопку **Настройка** в блоке **Анти-Спам** вы можете перейти к настройке параметров работы Анти-Спама.

СОВЕТЫ ПО РАБОТЕ С АНТИ-СПАМОМ

В данном разделе собраны ответы на вопросы, часто возникающие при использовании Анти-Спама.

См. также

НУЖНЫЕ ПИСЬМА ИНОГДА РАСПОЗНАЮТСЯ КАК СПАМ. ЧТО ДЕЛАТЬ?

Анти-Спам включен и распознает полезные письма как спам. Почему такое происходит?

Дело в том, что распространители спама предпринимают множество усилий для маскировки своей деятельности: вымогательство денег в виде сбора средств на благотворительность, в текст спам-сообщения добавляют блок случайных слов или отрывок из классического произведения, рекламные сообщения содержат только изображения без текста. Более того, спам-сообщения составляются программами, которые изменяют текст одного и того же сообщения при многократной отправке, что также затрудняет фильтрацию.

Есть несколько способов увеличения эффективности работы Анти-Спама:

1. Дополнительное обучение (см. раздел «Обучение Анти-Спама» на стр. 106) Анти-Спама.
2. Выбор уровня агрессивности (см. раздел «Изменение уровня агрессивности» на стр. 110).
3. Выбор фактора спама (см. раздел «Определение фактора спама и потенциального спама» на стр. 112).
4. Использование дополнительных критериев фильтрации (см. раздел «Использование дополнительных признаков фильтрации спама» на стр. 113).

Анти-Спам распознает не все спам-сообщения. Что делать?

Анти-Спам обучен и работает, но спам-сообщения продолжают атаковать ваш почтовый ящик. Почему такое происходит?

Дело в том, что распространители спама предпринимают множество усилий для маскировки своей деятельности: вымогательство денег в виде сбора средств на благотворительность, в текст спам-сообщения добавляют блок случайных слов или отрывок из классического произведения, рекламные сообщения содержат только изображения без текста. Более того, спам-сообщения составляются программами, которые изменяют текст одного и того же сообщения при многократной отправке, что также затрудняет фильтрацию.

Есть несколько способов увеличения эффективности работы Анти-Спама:

1. Дополнительное обучение (см. раздел «Обучение Анти-Спама» на стр. 106) Анти-Спама.
2. Выбор уровня агрессивности (см. раздел «Изменение уровня агрессивности» на стр. 110).
3. Выбор фактора спама (см. раздел «Определение фактора спама и потенциального спама» на стр. 112).
4. Использование дополнительных критериев фильтрации (см. раздел «Использование дополнительных признаков фильтрации спама» на стр. 113).

Спам чаще всего приходит в определенном формате. Как увеличить вероятность распознавания такого спама?

Анти-Спам включен, прошел обучение, но периодически он пропускает спам-сообщения в определенном формате. Как увеличить эффективность распознавания такого спама?

Спам-сообщения часто имеют особенности, отличающие их от обычных писем. Например они могут: не иметь темы и текста, содержать ссылки на изображения или вложенные изображения, содержать текст, имеющий цвет фона или текст, набранный мелким шрифтом. Также спамом могут быть письма с невидимыми символами (цвет текста совпадает с цветом фона), содержащие скрытые элементы (элементы не отображаются вообще) или некорректные html-теги, а также письма, содержащие скрипты (последовательности инструкций, выполняющихся при открытии письма пользователем).

Для более эффективного распознавания такого рода спам-сообщений вы можете задать дополнительные критерии фильтрации (см. раздел «Использование дополнительных признаков фильтрации спама» на стр. 113) спама.

Я точно знаю, с каких адресов не приходит спам. Что делать?

Анти-Спам использует вероятностные критерии (см. раздел «Алгоритм работы компонента» на стр. 105) для фильтрации почтового трафика, поэтому полезные письма могут быть распознаны как спам. Если вы абсолютно

уверены, что с некоторых почтовых адресов невозможно получить спам, вы можете исключить из фильтрации сообщения с этих адресов.

Для этого добавьте нужные адреса в «белый» список (см. раздел «Формирование “белого” списка адресов» на стр. 114).

Я точно знаю, с каких адресов приходит спам. Что делать?

Анти-Спам обучен и работает. С одного почтового адреса постоянно приходит спам, но Анти-Спам иногда не распознает сообщения с этого адреса нужным образом. Как увеличить эффективность работы Анти-Спама?

Такое поведение Анти-Спама является следствием использования вероятностных критериев (см. раздел «Алгоритм работы компонента» на стр. 105) для распознавания спама. Распространители спама предпринимают множество усилий для маскировки своей деятельности: вымогательство денег в виде сбора средств на благотворительность, в текст спам-сообщения добавляют блок случайных слов или отрывок из классического произведения, рекламные сообщения содержат только изображения без текста. Более того, спам-сообщения составляются программами, которые изменяют текст одного и того же сообщения при многократной отправке, что также затрудняет фильтрацию.

Если вы точно знаете, с какого почтового адреса приходит спам, вы можете использовать четкий критерий фильтрации для сообщений с этого адреса. Для этого добавьте этот адрес в «черный» список (см. раздел «Формирование “черного” списка адресов» на стр. 115).

Анти-Баннер

Анти-Баннер блокирует рекламную информацию, размещенную на специальных баннерах в интернете или встроенных в интерфейс различных программ, установленных на вашем компьютере.

Рекламная информация на баннерах не только не содержит полезной информации, но и отвлекает вас от дел и повышает объем скачиваемого трафика. Анти-Баннер блокирует самые распространенные на настоящее время баннеры, маски которых включены в поставку приложения. Вы можете отключить блокировку баннеров либо сформировать собственные списки разрешенных и запрещенных баннеров.

Список масок наиболее распространенных рекламных баннеров составлен специалистами «Лаборатории Касперского» на основании специально проведенного исследования и включен в поставку приложения. Рекламные баннеры, подпадающие под маски этого списка, будут блокироваться приложением, если блокировка баннеров не отключена. Для блокирования баннеров, маски адресов которых отсутствуют в стандартном списке используется эвристический анализатор (см. раздел «Использование эвристического анализа» на стр. 123).

Кроме того, вы можете создать «белый» (см. раздел «Формирование списка разрешенных адресов баннеров» на стр. 123) и «черный» списки баннеров, на основании которых трансляция баннера будет разрешена или запрещена.

Обратите внимание, что при наличии маски домена в списке запрещенных баннеров или «черном» списке доступ к корню сайта не блокируется.

Например, если в список запрещенных баннеров внесена маска truehits.net, то доступ к сайту http://truehits.net будет разрешен, а доступ к http://truehits.net/a.jpg - заблокирован.

См. также

Использование эвристического анализа

Баннеры, адреса которых не входят в стандартный список, могут быть проанализированы с помощью эвристического анализа. При его использовании приложение будет анализировать загружаемые изображения на предмет наличия признаков, характерных для баннеров. На основании этого анализа изображение может быть идентифицировано как баннер и заблокировано.

Чтобы начать использовать эвристический анализ, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Баннер** нажмите на ссылку с количеством списков.
4. На закладке **Общие** установите флажок **Использовать эвристический анализ**.

См. также

Анти-Баннер 122

Формирование списка разрешенных адресов баннеров

«Белый» список баннеров формируется пользователем в процессе работы с приложением, если возникает необходимость не блокировать некоторые баннеры. Этот список содержит маски разрешенных к трансляции баннеров.

Чтобы добавить новую маску в «белый» список, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Анти-Баннер** нажмите на ссылку с количеством списков.
4. В открывшемся окне на закладке **«Белый» список** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Маска адреса (URL)** введите маску разрешенного баннера. Чтобы отказаться от использования какой-либо маски, необязательно удалять ее из списка, достаточно снять флажок рядом с ней.

См. также

Экспорт / импорт списков баннеров 123

Экспорт / импорт списков баннеров

Вы можете копировать сформированные списки разрешенных / запрещенных баннеров с одного компьютера на другой. При экспорте списка вам будет предложено копировать только выбранный элемент списка или весь список целиком. При импорте вы можете добавить новые адреса в список или заменить существующий список импортируемым.

Чтобы копировать сформированные списки разрешенных / запрещенных баннеров, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента Анти-Баннер нажмите на ссылку с количеством списков.
4. В открывшемся окне на закладке **«Белый» список** (или на закладке **«Черный» список**) воспользуйтесь ссылками **Импортировать** или **Экспортировать**.

См. также

Формирование списка разрешенных адресов баннеров 123

Родительский контроль

Родительский контроль - компонент приложения, выполняющий функции контроля доступа пользователей компьютера к интернет-ресурсам. Основной задачей Родительского контроля является ограничение доступа, в первую очередь, к следующим ресурсам:

- Веб-сайтам, предназначенным для взрослой аудитории, либо веб-сайтам, затрагивающим темы порнографии, оружия, наркотиков, провоцирует жестокость, насилие и т.д.
- Веб-сайтам, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы).

Часто подобные веб-сайты содержат большое количество вредоносных программ, а загрузка данных с таких ресурсов, как игровые сайты, приводит к серьезному увеличению интернет-трафика.

После установки Kaspersky Internet Security Родительский контроль отключен. При включении Родительского контроля вам будет предложено настроить защиту приложения паролем (см. раздел «Самозащита приложения» на стр. 170), чтобы исключить несанкционированное отключение компонента.

Ограничение доступа пользователя к веб-ресурсам выполняется путем назначения ему одного из трех предустановленных профилей (см. раздел «Работа с профилями» на стр. 126) для работы в интернете.

По умолчанию всем пользователям присваивается профиль **Ребенок**, содержащий максимальный набор ограничений. Профиль можно связать с учетными записями Microsoft Windows. В этом случае пользователь получает доступ к веб-ресурсам в соответствии с параметрами своего профиля.

Доступ к профилю **Родитель** или **Подросток** нужно защитить паролем. Переключение на профиль (см. раздел «Переключение профилей» на стр. 127), защищенный паролем, возможно только после ввода этого пароля.

Каждый профиль регулирует доступ к веб-сайтам на одном из предустановленных уровней ограничения (см. раздел «Изменение уровня ограничения» на стр. 127). Уровень ограничения представляет собой набор параметров, регламентирующих доступ к какому-либо веб-ресурсу.

Чтобы изменить параметры работы Родительского контроля, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
4. В раскрывшемся меню выберите пункт **Настройка**.

5. Внесите необходимые изменения в настройки параметров компонента.

См. также

Алгоритм работы компонента

Рассмотрим общий алгоритм работы компонента **Родительский контроль**:

1. При аутентификации пользователя после загрузки системы загружается профиль, соответствующий данному пользователю.

2. При попытке пользователя обращения к веб-сайту Родительский контроль выполняет следующие действия:

   - проверка на наличие ограничения по времени (см. раздел «Ограничение доступа по времени» на стр. 130);

   - проверка на совпадение URL запрашиваемой страницы с одним из элементов «черного» (см. раздел «Формирование списка запрещенных адресов» на стр. 129) и «белого» (см. раздел «Формирование списка разрешенных адресов» на стр. 128) списков;

   - анализ содержимого веб-страницы на предмет принадлежности страницы к запрещенным категориям (см. раздел «Выбор категорий запрещенных сайтов» на стр. 128).

3. Если хотя бы одно из этих условий не выполняется, доступ к веб-странице блокируется. В противном случае, веб-страница загружается в окне браузера.

Если в вашей сети используется прокси-сервер (см. раздел «Параметры прокси-сервера» на стр. 180), который использует нестандартный порт, то данный порт необходимо добавить в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 178). Иначе Родительский контроль может работать некорректно и пропускать запрещенные веб-страницы.

См. также

РАБОТА С ПРОФИЛЯМИ

Профиль - это набор правил, регламентирующих доступ пользователя к определенным интернет-ресурсам. Вы можете выбрать один из профилей: **Ребенок** (используется по умолчанию), **Подросток** или **Родитель**.

Для каждого из профилей разработан оптимальный набор правил с учетом возраста, опыта и других характеристик каждой группы. Так, например, профиль **Ребенок** обладает максимальным набором ограничений, а в профиле **Родитель** ограничений нет. Создавать собственные и удалять предустановленные профили нельзя, но вы можете изменять параметры профилей **Ребенок** и **Подросток** по своему усмотрению.

- *Чтобы использовать профили Подросток и Родитель, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Подросток** или закладке **Родитель** установите флажок **Использовать профиль**.

- *Чтобы связать профиль с учетной записью Microsoft Windows, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Подросток** или закладке **Родитель** нажмите на кнопку **Пользователи**.
  6. В открывшемся окне **Пользователи** нажмите на ссылку **Добавить** и в стандартном окне Microsoft Windows укажите необходимую учетную запись (подробнее см. справку к операционной системе).

     Для того чтобы настраиваемый профиль не применялся к учетной записи пользователя, выберите этого пользователя в списке и нажмите на кнопку ✖ в правой части списка.

См. также

Переключение профилей

Активный в текущий момент профиль можно поменять. Это может понадобиться в случае, если активный профиль имеет ограничения на доступ к веб-ресурсам и не позволяет вам свободно работать в интернете.

Переключение профилей можно ограничить с помощью пароля.

- *Чтобы сменить профиль пользователя, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным профилем пользователя.
  4. В открывшемся окне **Смена профиля пользователя** выберите название профиля и, если необходимо, укажите пароль.

- *Чтобы задать пароль для профиля пользователя, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Подросток** или закладке **Родитель** задайте пароль в соответствующем поле блока **Идентификация пользователя**. Для переключения на профиль **Ребенок** пароль не требуется.

Изменение уровня ограничения

Родительский контроль обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам на одном из предустановленных уровней.

Если ни один из уровней ограничения не соответствует вашим требованиям, вы можете выполнить дополнительную настройку его параметров. Для этого выберите наиболее близкий к вашим пожеланиям уровень в качестве базового и отредактируйте его параметры.

- *Чтобы изменить уровень ограничения, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
  4. В раскрывшемся меню выберите уровень ограничения.

- *Чтобы изменить параметры уровня ограничения, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Фильтр содержимого**.
  3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
  4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне нажмите на кнопку **Настройка** в блоке **Уровень ограничения**.

6. На закладке **Категории** выберите запрещенные категории веб-сайтов. В результате будет сформирован уровень ограничения - **Другой**, содержащий параметры защиты, заданные вами. Для возврата к стандартным параметрам ограничения нажмите на кнопку **По умолчанию** в блоке **Родительский контроль**.

ВЫБОР КАТЕГОРИЙ ЗАПРЕЩЕННЫХ САЙТОВ

Родительский контроль анализирует содержимое веб-страниц по ключевым словам, относящимся к определенным тематическим категориям. Если количество слов нежелательной категории превышает допустимый пороговый уровень, доступ к такому ресурсу блокируется.

База ключевых слов входит в поставку Kaspersky Internet Security и обновляется вместе с базами и модулями приложения.

Примечание! Список запрещенных категорий ограничивается списком по умолчанию. Создание собственных запрещенных категорий не предусмотрено.

Чтобы выбрать категории запрещенных сайтов, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне в разделе **Уровень ограничения** нажмите на кнопку **Настройка**.

6. В открывшемся окне на закладке **Категории** установите нужные флажки.

ФОРМИРОВАНИЕ СПИСКА РАЗРЕШЕННЫХ АДРЕСОВ

Вы можете разрешить доступ к определенным веб-сайтам. Для этого нужные адреса нужно добавить в «белый» список.

Сайт, добавленный в «белый» список, может относиться к одной из категорий запрещенных сайтов (см. раздел «Выбор категорий запрещенных сайтов» на стр. 128). В таком случае этот сайт будет доступен, даже если включена фильтрация сайтов соответствующей категории.

Пример: вы хотите оградить своего ребенка от посещения веб-сайтов, предназначенных для взрослой аудитории, а также сайтов, которые являются потенциальной причиной потери времени или денег. Но вместе с тем, вам необходимо отправлять ребенку почтовые сообщения.

Выберите профиль **Ребенок**. В качестве базового предустановленного уровня ограничений вы можете использовать **Рекомендуемый** уровень со следующими изменениями: установить ограничение на посещение чатов и интернет-почты, и добавить в «белый» список внешний почтовый сервис, на котором у вашего ребенка зарегистрирован почтовый ящик. Таким образом, ваш ребенок будет иметь доступ только к этому почтовому сервису.

Чтобы добавить новый адрес или маску в «белый» список, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.

4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне в разделе **Уровень ограничения** нажмите на кнопку **Настройка**.
6. В открывшемся окне на закладке **«Белый» список н**ажмите на ссылку **Добавить.**
7. В открывшемся окне **Маска адреса (URL)** задайте адрес или маску.

Если вы хотите исключить адрес или маску из списка без удаления, снимите флажок рядом с адресом в списке.

См. также

Формирование списка запрещенных адресов 129

Формирование списка запрещенных адресов

Родительский контроль ограничивает доступ к веб-сайтам, основываясь на принадлежности сайтов к определенным категориям (см. раздел «Выбор категорий запрещенных сайтов» на стр. 128). Вы можете явно ограничить доступ к определенным веб-сайтам. Для этого нужные адреса нужно добавить в «черный» список.

Чтобы добавить новый адрес или маску в «черный» список, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне в разделе **Уровень ограничения** нажмите на кнопку **Настройка**.
6. В открывшемся окне на закладке **«Черный» список** нажмите на ссылку **Добавить**.
7. В открывшемся окне **Маска адреса (URL)** задайте адрес или маску.

Если вы хотите исключить адрес или маску из списка без удаления, снимите флажок рядом с адресом в списке.

См. также

Формирование списка разрешенных адресов 128

Выбор действия при попытке доступа к запрещенным сайтам

При попытке пользователя получить доступ к запрещенному веб-ресурсу Родительский контроль выполняет заданное действие.

Чтобы выбрать действие, которое будет выполняться компонентом при попытке доступа к запрещенному сайту, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.

3. Для компонента **Родительский контроль** нажмите на ссылку с установленным уровнем ограничения.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне выберите действие в одноименном блоке.

ОГРАНИЧЕНИЕ ДОСТУПА ПО ВРЕМЕНИ

Вы можете ограничить время пребывания пользователя в интернете.

Пример:

Для профиля **Ребенок** вы ограничили суммарное суточное время работы в интернете тремя часами и дополнительно разрешили доступ в интернет только с 14.00 до 15.00. В итоге доступ к веб-сайтам будет разрешен только в течение этого временного интервала, несмотря на общее разрешенное количество часов.

Чтобы ограничить время пребывания в интернете, выполните следующие действия:

1. Откройте главное окно приложения.

2. В левой части окна выберите элемент **Фильтр содержимого**.

3. Для компонента **Родительский контроль** нажмите на ссылку с названием установленного уровня ограничения.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне нажмите на кнопку **Настройка** в блоке **Ограничение времени**.

   Чтобы установить ограничение на работу в интернете по суммарному количеству времени в течение суток, установите флажок **Ограничить суточное время работы в интернете** и задайте условие ограничения.

   Чтобы ограничить доступ к интернету определенными часами в течение суток, установите флажок **Разрешить доступ к интернету в указанное время** и задайте временные интервалы, когда работа в интернете разрешена. Для этого воспользуйтесь кнопкой **Добавить** и в открывшемся окне укажите временные рамки. Для редактирования списка разрешенных интервалов работы используйте соответствующие кнопки.

   

   Если вы задали оба временных ограничения, причем значение одного из них превышает другое по количеству отведенного времени, то будет выбрано наименьшее значение из заданных.

ПРОВЕРКА НА ВИРУСЫ

Поиск вирусов - одна из важнейших функций обеспечения безопасности компьютера. В результате поиска предотвращается распространение вредоносного кода, по каким-либо причинам не обнаруженного защитой от вредоносного ПО.

Специалистами ЗАО «Лаборатория Касперского» выделены несколько задач поиска вирусов. В их число входят:

Проверка на вирусы

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

Задачи полной проверки компьютера, проверки при запуске системы и поиска руткитов являются специфическими задачами. Не рекомендуется вносить изменения в списки объектов для проверки в ходе этих задач.

Каждая задача поиска выполняется в заданной области с определенными параметрами, набор которых задает уровень безопасности. По умолчанию предусмотрено три уровня.

После запуска задачи поиска прогресс ее выполнения отображается с нижней части главного окна Kaspersky Internet Security. При обнаружении угрозы приложение выполняет заданное действие.

В ходе выполнения поиска угроз информация о результатах поиска записывается в отчет приложения.

Кроме того, вы можете выбрать объект для проверки стандартными средствами операционной системы Microsoft Windows, например, в окне программы **Проводник** или на **Рабочем столе** и т.д. Для этого установите курсор мыши на имени выбранного объекта, правой клавишей мыши откройте контекстное меню Microsoft Windows и выберите пункт **Проверить на вирусы**.

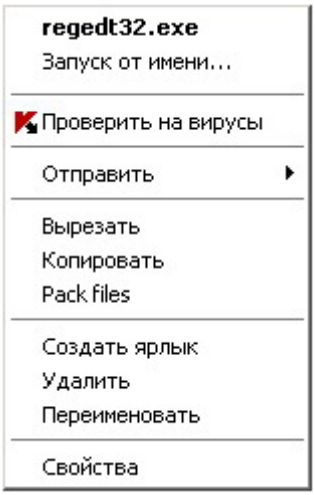

Рисунок 15: Контекстное меню Microsoft Windows

Также вы можете перейти к отчету о проверке, где будет представлена полная информация о событиях, произошедших в ходе выполнения задач.

- *Чтобы изменить параметры какой-либо задачи проверки на вирусы, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
  3. Нажмите на ссылку с установленным уровнем безопасности.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В настройки параметров для выбранной задачи внесите необходимые изменения.

- *Чтобы перейти к отчету о проверке на вирусы, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
  3. Нажмите на кнопку **Отчеты**.

В ЭТОМ РАЗДЕЛЕ

ЗАДАЧИ ПРОВЕРКИ НА ВИРУСЫ

Вы можете ознакомиться со статусом каждой задачи (см. раздел «Проверка на вирусы» на стр. 131) проверки на вирусы перед ее запуском. Статус задачи отображается в строке **Последний запуск** в главном окне.

До первого запуска задача имеет статус **Не запускалось**.

После запуска задачи прогресс ее выполнения отображается в главном окне.

Если задача была остановлена пользователем, то ее статус меняется на **Остановлено**.

По окончании работы задачи проверки в строке **Последний запуск** отображается дата и время последнего запуска.

Чтобы запустить / остановить задачу проверки на вирусы, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на кнопку **Запустить проверку**, чтобы запустить проверку. Нажмите на кнопку **Остановить проверку** во время выполнения задачи, если возникла необходимость остановить ее работу.

Запуск проверки на вирусы

Запустить задачу проверки на вирусы вы можете:

- из контекстного меню (см. раздел «Контекстное меню» на стр. 35) Kaspersky Internet Security;
- из главного окна (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36) Kaspersky Internet Security.

Информация о процессе выполнения задачи будет отображаться в главном окне Kaspersky Internet Security.

Кроме того, вы можете выбрать объект для проверки стандартными средствами операционной системы Microsoft Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

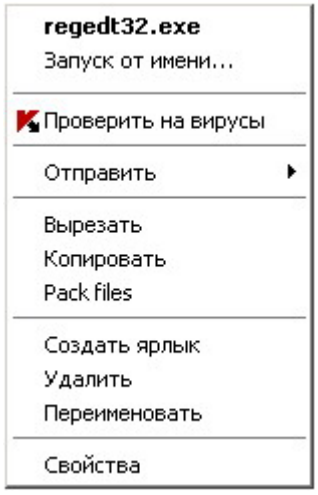

Рисунок 16: Контекстное меню Microsoft Windows

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

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок приложения.
2. В раскрывшемся меню выберите пункт **Проверка на вирусы**. В открывшемся главном окне Kaspersky Internet Security выберите нужную задачу **Проверка** (**Полная проверка**, **Быстрая проверка**). Произведите, если необходимо, настройку параметров выбранной задачи и нажмите на кнопку **Запустить проверку**.

3. Либо в контекстном меню выберите пункт **Проверка Моего компьютера**. Будет запущена полная проверка компьютера. Прогресс выполнения задачи будет отображаться в главном окне Kaspersky Internet Security.

Чтобы запустить задачу проверки на вирусы из главного окна приложения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на кнопку **Запустить проверку**. Прогресс выполнения задачи будет отображаться в главном окне приложения.

Чтобы запустить задачу проверки на вирусы для выбранного объекта из контекстного меню Microsoft Windows, выполните следующие действия:

1. Нажмите правой клавишей мыши на имени выбранного объекта.
2. В раскрывшемся меню выберите пункт **Проверить на вирусы**. Прогресс и результат выполнения задачи будет отображаться в открывшемся окне.

Изменение уровня безопасности

Под уровнем безопасности понимается предустановленный набор параметров проверки. Специалистами «Лаборатории Касперского» были сформированы три уровня безопасности. Решение о том, какой уровень выбрать принимается вами на основе ваших предпочтений:

- Если вы подозреваете, что вероятность заражения вашего компьютера очень высока, выберите высокий уровень безопасности.
- Рекомендуемый уровень подходит для большинства случаев и рекомендуется для использования специалистами «Лаборатории Касперского».
- Если вы работаете с приложениями, требующими значительных ресурсов оперативной памяти, выберите низкий уровень безопасности, поскольку набор проверяемых файлов на данном уровне сокращен.

Рисунок 17: Изменение уровня безопасности

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы проверки самостоятельно. В результате название уровня безопасности изменится на **Другой**. Чтобы восстановить параметры работы проверки по умолчанию, выберите один из предустановленных уровней.

Чтобы изменить установленный уровень безопасности, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите нужный уровень безопасности.

Изменение действия при обнаружении угрозы

При обнаружении угрозы Kaspersky Internet Security присваивает ей определенный статус:

- статус одной из вредоносных программ (например, *вирус*, *троянская программа*);
- *возможно зараженный*, когда в результате проверки однозначно не-возможно определить, заражен объект или нет. Вероятно, в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

После присвоения статуса Kaspersky Internet Security осуществляет над обнаруженной угрозой определенное действие. По умолчанию приложение запрашивает вас о необходимых действиях по окончанию проверки.

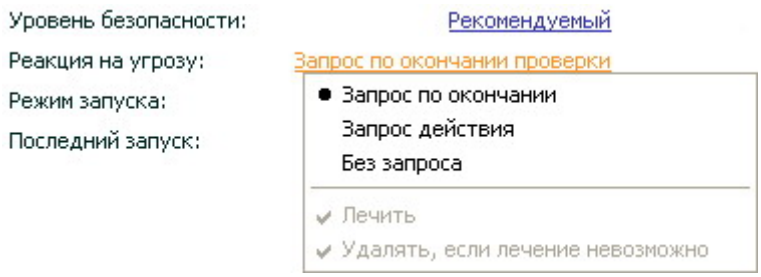

Рисунок 18: Изменение действия при обнаружении угрозы

Перед лечением или удалением объекта приложение формирует его резервную копию на тот случай, если понадобится восстановить объект или появится возможность его вылечить.

Если вы работаете в автоматическом режиме (см. раздел «Шаг 2. Выбор режима защиты» на стр. 43), то приложение будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов. Для вредоносных объектов таким действием будет **Лечить. Удалять, если лечение невозможно**, для подозрительных - **Пропускать**.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным действием.
4. В раскрывшемся меню выберите нужное действие.

Режим запуска: формирование расписания

Во время первоначальной настройки Kaspersky Internet Security вы можете выбрать, с какой частотой выполнять автоматический запуск задач полной проверки компьютера и проверки объектов автозапуска. Остальные задачи поиска угроз выполняются по вашему запросу. Если вас не устраивает такой режим работы задач, отредактируйте параметры их расписания.

Главное, что вам нужно определить - это интервал, с которым должно выполняться событие (запуск задачи или отправка уведомления). Для этого необходимо указать параметры расписания для выбранного варианта.

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

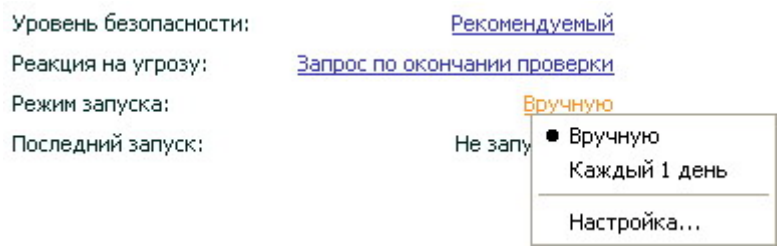

Рисунок 19: Формирование расписания

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

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
  3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне **Режим запуска** в блоке **Расписание** выберите **Вручную**, если хотите, чтобы задача проверки запускалась вами в удобный для вас момент времени. Чтобы задача выполнялась периодически, выберите **Расписание** и сформируйте расписание запуска задачи.

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

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
  3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне **Режим запуска** в блоке **Расписание** установите флажок **Запускать пропущенные задачи**.

РЕЖИМ ЗАПУСКА: ЗАДАНИЕ УЧЕТНОЙ ЗАПИСИ

Вы можете задать учетную запись, с правами которой будет производиться поиск.

- *Чтобы задать учетную запись, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
  3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
  4. В раскрывшемся меню выберите пункт **Настройка**.
  5. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами другого пользователя**. В полях ниже задайте имя пользователя и пароль.

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 изменения в этот список.

Добавленный объект сразу же появляется в списке. Если при добавлении объекта был отмечен флажок **Включая вложенные папки**, то проверка будет проводится рекурсивно.

Для удаления объекта из списка выберите объект и нажмите на кнопку ✖ в правой части списка.

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

Помимо удаления объектов из списка можно временно исключать их из проверки. Для этого выберите объект в списке и снимите флажок слева от имени объекта.

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

Чтобы сформировать список объектов для проверки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку **Добавить**.
4. В открывшемся окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**. Чтобы исключить какие-либо объекты из списка проверки, снимите флажок рядом с ними.

Изменение типа проверяемых объектов

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

При выборе типа файлов следует помнить следующее:

- Существует ряд файловых форматов, вероятность внедрения в которые вредоносного кода и его последующая активация достаточно низка. Примером такого файла является файл *txt*-формата. И наоборот, есть файловые форматы, которые не содержат или могут содержать исполняемый код. Примером таких объектов являются файлы форматов *exe*, *dll*, *doc*. Риск внедрения и активации в такие файлы вредоносного кода достаточно высок.
- Не стоит забывать, что злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, хотя на самом деле он может быть исполняемым файлом, переименованным в *txt*-файл. Если вы выберите вариант Файлы, проверяемые по расширению, то такой файл будет пропущен в процессе проверки. Если же выбран вариант Файлы, проверяемые по формату, невзирая на расширение, защита файлов проанализирует заголовок файла, в результате чего выяснится, что файл имеет exe-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **Область действия** в блоке **Типы файлов** выберите нужный параметр.

ОПТИМИЗАЦИЯ ПРОВЕРКИ

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

Также вы можете задать временное ограничение на длительность проверки. По истечении заданного времени проверка файлов будет прекращена.

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

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).

3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

- *Чтобы задать временное ограничение на длительность проверки, выполните следующие действия:*

1. Откройте главное окно приложения.

2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).

3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.

4. В раскрывшемся меню выберите пункт **Настройка**.

5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Остановить проверку, если она длится более** и задайте длительность проверки в поле рядом.

ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ

Распространенной практикой сокрытия вирусов является их внедрение в составные файлы: архивы, базы данных, и т.д. 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, проверять все файлы или только новые. Для этого воспользуйтесь ссылкой рядом с названием объекта. Она меняет свое значение при щелчке по ней левой клавишей мыши. Если установлен режим проверки только новых и измененных файлов (см. раздел «Оптимизация проверки» на стр. 138), выбор типа проверяемых составных файлов будет недоступен.

Вы можете ограничить максимальный размер проверяемого составного файла. Составные файлы больше заданного размера проверяться не будут.

Проверка файлов больших размеров при извлечении из архивов будет производиться даже если флажок **Не распаковывать составные файлы большого размера** установлен.

Чтобы изменить список проверяемых составных файлов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** выберите нужный тип проверяемых составных файлов.

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.
6. В открывшемся окне **Составные файлы** установите флажок **Не распаковывать составные файлы больших размеров** и укажите максимальный размер проверяемых файлов в поле ниже.

Изменение метода проверки

Вы можете настроить параметры проверки, влияющие на ее тщательность. По умолчанию всегда включен режим поиска угроз с помощью записей в базах приложения. Кроме этого вы можете задействовать различные методы и технологии проверки (см. раздел «Технология проверки» на стр. 140).

Режим поиска, когда Kaspersky Internet Security сравнивает найденный объект с записями в базах, называется *сигнатурным анализом* и используется всегда. Кроме него вы можете использовать *эвристический анализ*. Суть метода в анализе активности, которую объект производит в системе. Если активность типична для вредоносных объектов, то с достаточной долей вероятности объект будет признан вредоносным или подозрительным.

Дополнительно вы можете выбрать уровень детализации эвристического анализа, для этого передвиньте ползунок в одну из позиций: поверхностный, средний или глубокий.

Кроме этих вы методов проверки вы можете использовать:

- *Сигнатурный поиск уязвимостей*. Поиск осуществляется на основе регулярно обновляемых баз данных уязвимостей. Информация о уязвимости включает:
  - направление воздействия для использования уязвимости (например, от одной из учетных записей в системе, от компьютера в той же локальной сети);
  - уровень опасности для компьютера;
  - вид воздействия на систему (например, незаконное присвоение прав администратора системы, манипулирование информацией на удаленном компьютере, подмена данных на веб-сайте, и т.д.).
- *Поиск руткитов*. Руткит (rootkit) - это набор утилит, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, папок, ключей реестра других вредоносных программ, описанных в конфигурации руткита. Если поиск включен, вы можете установить детальный уровень обнаружения

руткитов (углубленный анализ). В этом случае будет выполняться тщательный поиск данных программ путем анализа большего количества объектов разного типа.

Чтобы использовать нужные методы проверки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выберите нужные значения параметра.

ТЕХНОЛОГИЯ ПРОВЕРКИ

Дополнительно вы можете задать технологию, которая будет использоваться при проверке:

- **iChecker**. Технология позволяет увеличить скорость проверки за счет исключения некоторых объектов. Исключение объекта из проверки осуществляется по специальному алгоритму, учитывающему дату выпуска баз приложения, дату предыдущей проверки объекта, а также изменение параметров проверки.

  Например, у вас есть файл архива, который был проверен Kaspersky Internet Security и ему 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 базы приложения, архив будет проверен повторно.

  Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а также применима только к объектам с известной приложению структурой (например, файлы exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Технология является развитием технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе, а также применима только к объектам, расположенным в файловой системе NTFS.

Чтобы изменить технологию проверки объектов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужное значение параметра.

НАЗНАЧЕНИЕ ЕДИНЫХ ПАРАМЕТРОВ ПРОВЕРКИ ДЛЯ ВСЕХ ЗАДАЧ

Каждая задача проверки выполняется в соответствии со своими параметрами. По умолчанию задачи, сформированные при установке Kaspersky Internet Security на компьютер, выполняются с рекомендуемыми экспертами «Лаборатории Касперского» параметрами.

Вы можете настроить единые параметры проверки для всех задач. За основу будет взят набор параметров, использующихся при проверке на вирусы отдельного объекта.

Чтобы назначить единые параметры проверки для всех задач, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Проверка**.
3. В правой части окна в блоке **Параметры других задач** нажмите на кнопку **Применить**. Подтвердите назначение единых параметров в окне запроса подтверждения.

ОБНОВЛЕНИЕ

Поддержка защиты в актуальном состоянии – залог безопасности вашего компьютера. Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы, поэтому крайне важно быть уверенным в том, что ваша информация находится под надежной защитой. Информация об угрозах и способах их нейтрализации содержится в базах приложения, поэтому важнейшим элементом обеспечения актуальности защиты является обновление баз.

Обновление приложения загружает и устанавливает на ваш компьютер:

- Базы приложения.

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

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

- Модули приложения.

  Помимо баз приложения вы можете обновлять и модули приложения. Пакеты обновлений устраняют уязвимости Kaspersky Internet Security, добавляют новые функции или улучшают существующие.

Основным источником обновлений Kaspersky Internet Security являются специальные серверы обновлений «Лаборатории Касперского».

Для успешной загрузки обновлений с серверов необходимо, чтобы ваш компьютер был подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если параметры прокси-сервера не определяются автоматически, настройте параметры подключения к нему.

В процессе обновления модули приложения и базы на вашем компьютере сравниваются с расположенными в источнике обновлений. В случае если на вашем компьютере установлена последняя версия баз и модулей, на экран выдается информационное сообщение об актуальности защиты вашего компьютера. Если базы и модули отличаются, на ваш компьютер будет установлена именно недостающая часть обновлений. Полное копирование баз и модулей не производится, что позволяет существенно увеличить скорость обновления и заметно снизить объем трафика.

Перед обновлением баз приложение создает их резервную копию, если по каким-либо причинам вы захотите вернуться к их использованию.

Возможность отката обновления необходима, например, в том случае, если вы обновили базы и в процессе работы они были повреждены. Вы сможете вернуться к предыдущему варианту баз, а позже попробовать обновить их еще раз.

Одновременно с обновлением Kaspersky Internet Security вы можете выполнять копирование полученных обновлений в локальный источник. Данный сервис позволяет обновлять базы и модули приложения на компьютерах сети в целях экономии интернет-трафика.

Вы также можете настроить режим автоматического запуска обновления.

В разделе **Обновление** отображается информация о текущем состоянии баз приложения:

- дата и время выпуска;
- количество записей в базах;
- статус баз (актуальны или устарели).

Вы можете перейти к отчету об обновлении, где будет представлена полная информация о событиях, произошедших в ходе выполнения задачи обновления (кнопка **Отчеты**). Также вы можете ознакомиться с обзором вирусной активности на сайте www.kaspersky.com (ссылка **Обзор вирусной активности**).

В этом разделе

Запуск обновления

В любой момент вы можете запустить обновление Kaspersky Internet Security. Оно будет производиться из выбранного вами источника обновлений (см. раздел «Выбор источника обновлений» на стр. 144).

Запустить обновление Kaspersky Internet Security вы можете:

- из контекстного меню (см. раздел «Контекстное меню» на стр. 35);
- из главного окна приложения (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36).

Информация о процессе обновления будет отображаться в главном окне приложения.

Чтобы запустить обновление Kaspersky Internet Security из контекстного меню:

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок приложения.
2. В раскрывшемся меню выберите пункт **Обновление**.

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Запустить обновление**. Прогресс выполнения задачи будет отображаться в главном окне приложения.

ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

Каждый раз, когда вы запускаете обновление, Kaspersky Internet Security создает резервную копию используемых баз и модулей и только потом приступает к их обновлению. Это позволяет вам вернуться к использованию предыдущих баз после неудачного обновления.

Возможность отката полезна, например, в том случае, если часть баз была повреждена. Локальные базы могут быть повреждены либо самим пользователем либо вредоносной программой, что возможно только в том случае, если самозащита (см. раздел «Самозащита приложения» на стр. 170) приложения отключена. Вы сможете вернуться к предыдущим базам, а позже попробовать обновить их еще раз.

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку **Откат**.

ВЫБОР ИСТОЧНИКА ОБНОВЛЕНИЙ

Источник обновлений – это ресурс, содержащий обновления баз и модулей Kaspersky Internet Security. Источником обновлений могут быть http- или ftp-серверы, локальные или сетевые папки.

Основным источником для обновлений являются серверы обновлений «Лаборатории Касперского». Это специальные интернет-сайты, на которые выкладываются обновления баз и модулей приложения для всех продуктов «Лаборатории Касперского».

Если у вас нет доступа к серверам обновлений «Лаборатории Касперского» (например, нет доступа к интернету), вы можете позвонить в наш центральный офис по телефонам +7 (495) 797-87-00, +7 (495) 645-79-39 и узнать адреса партнеров «Лаборатории Касперского», которые смогут предоставить вам обновления на дискетах или дисках в zip-формате.

Полученные на съемном диске обновления вы можете разместить как на некотором ftp-, http-сайте, так и в локальной или сетевой папке.

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

По умолчанию список источников обновлений содержит только серверы обновлений «Лаборатории Касперского».

Если в качестве источника обновлений выбран ресурс, расположенный вне локальной сети, для обновления необходимо соединение с интернетом.

Если в качестве источников обновлений выбрано несколько ресурсов, то в процессе обновления приложение обращается к ним строго по списку и обновляется с первого доступного источника.

Чтобы выбрать источник обновлений, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Источник** нажмите на ссылку **Добавить**.

6. В открывшемся окне **Выбор источника обновлений** выберите ftp-, http-сайт или укажите его IP-адрес, символьное имя или URL-адрес.

Использование прокси-сервера

Если для выхода в интернет используется прокси-сервер (см. раздел «Параметры прокси-сервера» на стр. 180), необходимо настроить его параметры.

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Источник** нажмите на кнопку **Прокси-сервер**.
6. В открывшемся окне **Прокси-сервер** настройте параметры прокси-сервера.

Региональные настройки

Если в качестве источника обновлений вы используете серверы обновлений «Лаборатории Касперского», вы можете выбрать предпочтительное для вас местоположение сервера для загрузки обновлений. «Лаборатория Касперского» имеет серверы в нескольких странах мира. Выбор географически ближайшего к вам сервера обновления «Лаборатории Касперского» поможет сократить время и увеличить скорость получения обновлений.

Чтобы выбрать ближайший сервер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Источник** в блоке **Региональные настройки** установите флажок **Выбрать из списка** и в раскрывающемся списке выберите ближайшую к вашему текущему местоположению страну.

   Если установить флажок **Определять автоматически**, то при обновлении будет использоваться информация о текущем регионе из реестра операционной системы.

Выбор предмета обновления

По умолчанию во время обновления с серверов «Лаборатории Касперского» копируются не только базы, но и модули Kaspersky Internet Security.

Если на момент обновления в источнике присутствует пакет модулей приложения, Kaspersky Internet Security получит и установит его после перезагрузки компьютера. До перезагрузки полученные обновления модулей установлены не будут.

Если следующее обновление приложения происходит до перезагрузки компьютера и установки полученных ранее обновлений модулей приложения, то будет произведено только обновление баз приложения.

Чтобы выбрать предмет обновления, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Во время обновления** выберите режим **Обновлять только базы приложения**. В этом случае модули приложения не будут скачиваться и устанавливаться во время обновления. Если вы хотите вернуться к настройкам, принятым по умолчанию, выберите режим **Обновлять базы и программные модули приложения**.

Действия после обновления

Kaspersky Internet Security также позволяет задать действия, выполняемые автоматически после обновления:

- **Проверять файлы на карантине**

  На карантин помещаются объекты, при проверке которых не удалось точно определить, какими вредоносными программами они поражены. Возможно после обновления баз приложение сможет однозначно определить опасность и обезвредить ее. По этой причине приложение проверяет объекты на карантине после каждого обновления. Рекомендуем вам периодически просматривать объекты на карантине. В результате проверки у них может измениться статус. Ряд объектов можно будет восстановить в прежнее местоположение и продолжить работу с ними.

- **Копировать обновления в папку**

  Если компьютеры объединены в локальную сеть, нет необходимости скачивать и устанавливать обновления на каждый из них отдельно, поскольку в этом случае увеличивается сетевой трафик. Вы можете воспользоваться механизмом копирования обновлений, который позволяет уменьшить трафик за счет того, что обновления скачиваются только один раз.

Чтобы после обновления проверять файлы, помещенные на карантин, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **После обновления** установите флажок **Проверять файлы на карантине**.

Обновление из локальной папки

Процедура получения обновлений из локальной папки организована следующим образом:

1. Один из компьютеров сети получает пакет обновлений Kaspersky Internet Security с веб-серверов «Лаборатории Касперского» в интернете либо другого веб-ресурса, содержащего актуальный набор обновлений. Полученные обновления помещаются в папку общего доступа.
2. Другие компьютеры сети для получения обновлений приложения обращаются к папке общего доступа.

Чтобы включить режим копирования обновлений, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **После обновления** установите флажок **Копировать обновления в папку** и в поле ниже укажите путь к папке общего доступа, куда будут помещаться полученные обновления. Также вы можете выбрать путь в окне, открывающемся по кнопке **Обзор**.

Чтобы обновление приложения выполнялось из выбранной папки общего доступа, выполните на всех компьютерах сети следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с названием текущего набора параметров.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Источник** нажмите на ссылку **Добавить**.
6. В открывшемся окне **Выбор источника обновлений** выберите папку или введите полный путь к ней в поле **Источник**.
7. На закладке **Источник** снимите флажок **Серверы обновлений «Лаборатории Касперского»**.

Изменение режима запуска задачи обновления

Режим запуска задачи обновления Kaspersky Internet Security вы выбираете в ходе работы мастера настройки приложения (см. раздел «Шаг 3. Настройка обновления приложения» на стр. 43). Если выбранный режим запуска обновления вас не устраивает, вы можете изменить его.

Запуск задачи обновления может производиться в одном из следующих режимов:

- **Автоматически**. Kaspersky Internet Security проверяет наличие пакета обновлений в источнике обновлений с заданной периодичностью. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений приложение скачивает их и устанавливает на компьютер.
- **По расписанию** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию.
- **Вручную**. В этом случае вы будете самостоятельно запускать обновление Kaspersky Internet Security.

Рисунок 20: Формирование расписания запуска задачи

Чтобы настроить режим запуска задачи обновления, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с установленным режимом запуска задачи обновления.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите режим запуска задачи обновления. Если выбран режим **По расписанию** сформируйте расписание.

   Если по каким-либо причинам запуск обновления был пропущен (например, в это время компьютер был выключен), вы можете настроить автоматический запуск пропущенной задачи как только это станет возможным. Для этого установите флажок **Запускать пропущенные задачи** в нижней части окна. Этот флажок доступен для всех вариантов расписания, кроме **Часы**, **Минуты** и **При запуске приложения**.

ЗАПУСК ОБНОВЛЕНИЯ С ПРАВАМИ ДРУГОГО ПОЛЬЗОВАТЕЛЯ

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

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

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на ссылку с установленным режимом запуска задачи обновления.
4. В раскрывшемся меню выберите пункт **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами другого пользователя**. В полях ниже задайте имя пользователя и пароль.

ЗАДАЧИ

В состав Kaspersky Internet Security включен ряд мастеров:

- Мастер Анализа безопасности (см. раздел «Анализ безопасности» на стр. 150), выполняющий диагностику безопасности компьютера и поиск уязвимостей в операционной системе и программах, установленных на компьютере.
- Мастер Настройки браузера (см. раздел «Настройка браузера» на стр. 151), выполняющий анализ параметров браузера Microsoft Internet Explorer, оценивая их в первую очередь с точки зрения безопасности.
- Мастер Восстановления после заражения (см. раздел «Восстановление после заражения» на стр. 155), устраняющий следы пребывания в системе вредоносных объектов.
- Мастер Устранения следов активности (на стр. 157), производящий поиск и устранение следов активности пользователя в системе и параметров операционной системы, способствующих накоплению информации об активности пользователя.
- Мастер создания Диска аварийного восстановления (см. раздел «Диск аварийного восстановления» на стр. 155), предназначенный для восстановления работоспособности системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка.
- Анализ сетевых пакетов (на стр. 152), перехватывающий сетевые пакеты и отображающий подробную информацию о них.
- Мониторинг сети (на стр. 149), предоставляющий подробную информацию о сетевой активности на вашем компьютере.
- Виртуальная клавиатура (на стр. 158), предотвращающая перехват данных, вводимых с клавиатуры.

В ЭТОМ РАЗДЕЛЕ

Мониторинг сети

Мониторинг сети - инструмент, предназначенный для просмотра информации о сетевой активности в реальном времени.

Информация о сетевом трафике разделена на категории:

- информация об активных соединениях и открытых портах;
- информация о примененных пакетных правилах для приложений;
- информация об объеме входящего и исходящего трафика.

Данные по каждой категории отображаются на отдельных закладках **Мониторинга сети**.

Чтобы запустить Мониторинг сети, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Запустите задачу **Мониторинг сети**.

Анализ безопасности

Мастер анализа безопасности осуществляет поиск уязвимостей в установленных приложениях, а также поиск повреждений и аномалий в настройках параметров операционной системы и браузера. Причиной появления таких повреждений может быть активность вредоносных программ, системные сбои и др.

Работа мастера разбита на два этапа:

- поиск потенциальных уязвимостей приложений;
- диагностика безопасности.

Поиск потенциальных уязвимостей ведется с помощью баз уязвимостей компании Secunia. В ходе работы мастером проверяются установлены ли последние обновления для операционной системы Microsoft Windows и для таких программ, как Firefox, Opera, Adobe Reader, QuickTime и др. Если последние обновления не установлены, такие программы могут быть потенциально уязвимыми для злоумышленников, и, как следствие, не безопасными. Результат работы мастера - прямые ссылки на описание проблемы и на критические исправления. Устранение потенциальных уязвимостей в популярных приложениях предотвращает возможность проведения хакерской атаки на ваш компьютер.

Диагностика безопасности ведется по многим направлениям, например: поиск Rootkit (программ для скрытого контроля взломанной системы), поиск клавиатурных шпионов (Keylogger), поиск вредоносных объектов по косвенным признакам (файлы с характерными именами, отладчики системных процессов), поиск потенциально уязвимых служб, настроек и проч.

Также мастер отслеживает представляют ли собой настройки параметров системы и браузера (Microsoft Internet Explorer) потенциальные уязвимости, которые могут быть использованы злоумышленниками с целью нанесения вреда вашему компьютеру. Например:

- **Заблокирован пункт Управление меню Мой компьютер**

  Некоторые трояны блокируют пункт **Управление** меню **Мой компьютер**, вследствие чего пользователь не может получить доступ к работе с пользователями, службами и проч.

- **Обнаружен отладчик системного процесса**

  Отладчики системного процесса позволяют блокировать запуск системных утилит и скрыто запускать трояны.

- **Невозможно использовать работу с системой из командной строки (cmd.exe)**

  Блокирование интерфейса командной строки (cmd.exe) используется вредоносными объектами для самозащиты.

После проведенного исследования мастер выполняет анализ собранной информации, с целью оценить, есть ли проблемы в безопасности системы, которые требуют немедленного вмешательства. Результатом исследования является список действий, которые следует выполнить, чтобы устранить слабые места в системе. Действия группируются по категориям, исходя из серьезности найденных проблем в безопасности.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. Запустите задачу **Анализ безопасности**.

Настройка браузера

Мастер настройки браузера выполняет анализ настроек параметров браузера Microsoft Internet Explorer, оценивая их в первую очередь с точки зрения безопасности, поскольку некоторые настройки параметров, заданные пользователем или установленные по умолчанию, могут приводить к проблемам в безопасности.

В ходе работы мастер проверяет установлены ли последние обновления для браузера, а также представляют ли настройки его параметров потенциальные уязвимости, которые могут быть использованы злоумышленниками с целью нанесения вреда вашему компьютеру. Например:

- **Кеш работы Microsoft Internet Explorer**

  Кеш содержит конфиденциальные данные, а также предоставляет возможность узнать, какие ресурсы посещал пользователь. Ряд вредоносных объектов при сканировании диска, сканируют также и кеш, в результате чего могут быть получены почтовые адреса пользователей. Рекомендуется очищать кеш после завершения работы браузера.

- **Отображение расширений для файлов известных форматов**

  Для пользователя полезно видеть реальное расширение файла. Многие вредоносные объекты используют двойные расширения. В этом случае пользователь видит только часть названия файла, без реального расширения. Такая схема широко практикуется злоумышленниками. Рекомендуется включать отображение расширений для файлов известных форматов.

- **Список доверенных сайтов**

  Вредоносные объекты могут добавлять в такой список ссылки на сайты.

Перед началом диагностики закройте все окна браузера Microsoft Internet Explorer.

После проведенного исследования мастер выполняет анализ собранной информации, с целью оценить, есть ли проблемы безопасности в настройках параметров браузера, которые требуют немедленного вмешательства. Результатом исследования является список действий, которые следует выполнить, чтобы устранить проблемы. Действия группируются по категориям, исходя из серьезности найденных проблем.

Также по окончании работы мастера формируется отчет, который может быть отправлен в «Лабораторию Касперского» для анализа.

Следует учитывать, что некоторые настройки параметров могут привести к проблемам с отображением некоторых сайтов (например, в случае использования на них ActiveX). Решением проблемы является включение подобных сайтов в доверенную зону.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. Запустите задачу **Настройка браузера**.

АНАЛИЗ СЕТЕВЫХ ПАКЕТОВ

Инструмент **Анализ сетевых пакетов** предназначен для опытных пользователей, обладающих знаниями о принципах построения сетей и сетевых протоколах.

В состав Kaspersky Internet Security входит инструмент *Анализ сетевых пакетов*. Этот инструмент предназначен для сбора и анализа сетевой активности в сети, в которую входит ваш компьютер.

После запуска Анализ сетевых пакетов перехватывает все пакеты, передаваемые по сети. Число захваченных пакетов может быть очень большим. Для облегчения анализа собранной информации вы можете использовать фильтрацию по адресам источника и назначения (см. раздел «Фильтрация пакетов по адресам источника и назначению» на стр. 153) пакета и по протоколу передачи (см. раздел «Фильтрация пакетов по протоколу передачи» на стр. 154).

После установки приложения Анализ сетевых пакетов недоступен в главном окне приложения. До начала работы с Анализом сетевых пакетов необходимо открыть доступ к нему (см. раздел «Доступ к Анализу сетевых пакетов» на стр. 152).

Чтобы запустить Анализ сетевых пакетов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Запустите задачу **Анализ сетевых пакетов**.

ДОСТУП К АНАЛИЗУ СЕТЕВЫХ ПАКЕТОВ

По умолчанию Анализ сетевых пакетов недоступен в главном окне Kaspersky Internet Security.

Чтобы открыть доступ к Анализу сетевых пакетов, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Анализ сетевых пакетов** установите флажок **Показывать монитор «Анализ сетевых пакетов»**.

Анализ сетевых пакетов отображается в списке задач для функции Фильтр содержимого (на стр. 103).

См. также

Анализ сетевых пакетов.....152

Запуск / остановка перехвата пакетов

Анализ сетевых пакетов работает на основе статистики, собранной из перехватываемых пакетов.

Чтобы запустить перехват пакетов, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Запустите задачу **Анализ сетевых пакетов**.
4. В открывшемся окне нажмите на кнопку **Запустить**.

Процесс перехвата пакетов отображается в левой части окна.

Нажмите на кнопку **Остановить**, чтобы прекратить перехват пакетов.

Вы не сможете отфильтровать собранные данные или закрыть окно Анализа сетевых пакетов до остановки перехвата пакетов.

См. также

Анализ сетевых пакетов.....152

Доступ к Анализу сетевых пакетов.....152

Фильтрация пакетов по адресам источника и назначению

Большое количество информации, собираемое Анализом сетевых пакетов, затрудняет ее обработку и анализ. Для облегчения анализа информации вы можете применить фильтрацию по адресам источника и назначению пакетов.

Чтобы применить фильтрацию пакетов по адресам источника и назначения, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Запустите задачу **Анализ сетевых пакетов**.
4. В открывшемся окне нажмите на кнопку **Запустить**. Нажмите на кнопку **Остановить**, чтобы остановить перехват пакетов.
5. В полях **Источник** и **Назначение** укажите нужные IP-адреса.
6. В верхней части окна нажмите на кнопку **Фильтровать**.

Результаты фильтрации отображаются в левой части окна.

Чтобы изменить критерий фильтрации, выполните следующие действия:

1. Внесите изменения в значения полей **Источник** и **Назначение**.
2. В верхней части окна нажмите на кнопку **Фильтровать**.

- *Чтобы отменить фильтрацию, выполните следующие действия:*

1. Очистите значения полей **Источник** и **Назначение**.
2. В верхней части окна нажмите на кнопку **Фильтровать**.

Данные, собранные Анализом активности, будут возвращены к состоянию на момент остановки перехвата пакетов.

См. также

ФИЛЬТРАЦИЯ ПАКЕТОВ ПО ПРОТОКОЛУ ПЕРЕДАЧИ

Большое количество информации, собираемое Анализом сетевых пакетов, затрудняет ее обработку и анализ. Для облегчения анализа информации вы можете применить фильтрацию по протоколу передачи пакета.

- *Чтобы применить фильтрацию пакетов по протоколу передачи, выполните следующие действия:*

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Запустите задачу **Анализ сетевых пакетов**.
4. В открывшемся окне нажмите на кнопку **Запустить**. Нажмите на кнопку **Остановить**, чтобы остановить перехват пакетов.
5. В раскрывающемся списке **Протокол** выберите нужный протокол.

Результаты фильтрации отображаются в левой части окна.

Выберите новый протокол в раскрывающемся списке **Протокол** , чтобы изменить критерий фильтрации.

- *Чтобы отменить фильтрацию, выполните следующие действия:*

1. Выберите пустое значение в раскрывающемся списке **Протокол**.
2. В верхней части окна нажмите на кнопку **Фильтровать**.

Данные, собранные Анализом активности, будут возвращены к состоянию на момент остановки перехвата пакетов.

См. также

Восстановление после заражения

Мастер восстановления после заражения позволяет устранить следы пребывания в системе вредоносных объектов. Специалисты «Лаборатории Касперского» рекомендуют запускать мастер после лечения компьютера с целью убедиться, что все угрозы и повреждения, возникшие из-за них, устранены. Также мастер можно использовать при подозрении на то, что ваш компьютер заражен.

В ходе работы мастер проверяет наличие каких-либо повреждений в системе, например: заблокирован доступ к сетевому окружению, изменены расширения файлов известных форматов, заблокирована панель управления и т. п. Причиной появления таких повреждений может быть активность вредоносных программ, системные сбои, а также применение некорректно работающих оптимизаторов системы.

После проведенного исследования мастер выполняет анализ собранной информации, с целью оценить, есть ли повреждения в системе, которые требуют немедленного вмешательства. Результатом исследования является список действий, которые следует выполнить, чтобы устранить повреждения. Действия группируются по категориям, исходя из серьезности найденных проблем.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Запустите задачу **Восстановление после заражения**.

Диск аварийного восстановления

В Kaspersky Internet Security реализован сервис создания диска аварийного восстановления.

Диск аварийного восстановления предназначен для восстановления работоспособности системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка. Этот диск включает:

- системные файлы Microsoft Windows XP Service Pack 2;
- набор утилит для диагностики операционной системы;
- файлы приложения;
- файлы, содержащие базы приложения.

Диск аварийного восстановления предназначен для того компьютера, на котором он был создан. Использование диска на других компьютерах может привести к непредсказуемым последствиям, поскольку на нем содержится информация о параметрах конкретного компьютера (например, информация о boot-секторах).

Создание диска аварийного восстановления доступно только в приложении, установленом на компьютере под управлением операционной системы Microsoft Windows XP и Microsoft Windows Vista. На компьютерах под управлением других поддерживаемых систем, в том числе и Microsoft Windows XP Professional x64 Edition и Microsoft Windows Vista x64, создание диска не предусмотрено.

См. также

Создание диска аварийного восстановления

Для создания диска аварийного восстановления вам потребуется установочный диск Microsoft Windows XP Service Pack 2.

Диск аварийного восстановления создается с помощью специальной программы – **PE Builder**.

Для создания диска с помощью PE Builder требуется предварительно установить эту программу на компьютер.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. Запустите задачу **Диск аварийного восстановления**.

Использование диска аварийного восстановления

Обратите внимание, что в режиме аварийного восстановления Kaspersky Internet Security работает, только если запущено главное окно. При закрытии главного окна приложение будет выгружено.

В программе Bart PE, установленной по умолчанию, отсутствует поддержка chm-файлов и интернет-браузеров, поэтому в режиме аварийного восстановления недоступны просмотр справочной системы приложения, а также ссылки в интерфейсе приложения.

При возникновении ситуации, когда в результате вирусной атаки невозможно загрузить операционную систему, выполните следующие действия:

1. Создайте диск аварийного восстановления, используя приложение на незараженном компьютере.
2. Вставьте диск аварийного восстановления в дисковод зараженного компьютера и перезагрузитесь. В результате будет запущена операционная система Microsoft Windows XP Service Pack 2 с интерфейсом программы Bart PE.

Программа Bart PE имеет встроенную сетевую поддержку для использования локальной сети. При запуске программы на экран будет выведен запрос на ее включение. Согласитесь с включением сетевой поддержки, если перед проверкой компьютера вы планируете обновить базы приложения из локальной сети. Если обновление не требуется, отмените включение сетевой поддержки.

3. Для запуска приложения выполните команду **GO→Programs→Kaspersky Internet Security 2009→Start**.

   В результате будет запущено главное окно Kaspersky Internet Security. В режиме аварийного восстановления доступны только задачи поиска вирусов и обновление баз приложения из локальной сети (в случае, если включена сетевая поддержка Bart PE).

4. Запустите проверку компьютера на вирусы.

Обратите внимание, что для проверки по умолчанию используются базы приложения, актуальные на дату создания диска аварийного восстановления. Поэтому перед началом проверки рекомендуется обновить базы.

Также обращаем внимание, что обновленные базы будут использоваться приложением только в текущем сеансе работы с диском аварийного восстановления, до перезагрузки компьютера.

Если при проверке компьютера были обнаружены зараженные или возможно зараженные объекты, и была проведена их обработка с последующим помещением на карантин и в резервное хранилище, рекомендуется завершить обработку данных объектов в текущем сеансе работы с диском аварийного восстановления.

В противном случае данные объекты будут утрачены после перезагрузки компьютера.

Мастер устранения следов активности

При работе на компьютере действия пользователя регистрируются в системе в виде:

- истории посещения веб-сайтов;
- истории запуска приложения;
- истории поисковых запросов;
- истории открытия и сохранения файлов различными приложениями;
- записей в системном журнале Microsoft Windows;
- временных файлов и т.д.

Все эти источники информации об активности пользователя могут содержать конфиденциальные данные, в том числе пароли, и доступны для анализа злоумышленниками. В то же время, пользователь зачастую не обладает достаточными знаниями для того, чтобы предотвратить такой способ хищения ценной информации.

В состав Kaspersky Internet Security входит мастер **Устранения следов активности**. Этот мастер производит поиск следов активности пользователя в системе и параметров операционной системы, способствующих накоплению информацию об активности.

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. Для того, чтобы удалить эти файлы, мастер предложит перезагрузить систему. Однако, в ходе перезагрузки такие файлы могут быть созданы заново, что приведет к повторному обнаружению этих файлов как следов активности.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Фильтр содержимого**.
3. Запустите задачу **Устранение следов активности**.

ВИРТУАЛЬНАЯ КЛАВИАТУРА

При работе за компьютером часто возникают ситуации, когда необходимо указать ваши личные данные, а также имя пользователя и пароль: при регистрации на интернет-сайтах, при пользовании интернет-магазинами и т.д.

В таких случаях существует опасность перехвата конфиденциальной информации с помощью клавиатурных шпионов - программ, регистрирующих нажатие клавиш, или с помощью аппаратных перехватчиков.

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Для использования виртуальной клавиатуры, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. Запустите **Виртуальную клавиатуру**.
4. Убедитесь, что ввод данных будет произведен в нужное поле. Введите нужные данные, нажимая на кнопки виртуальной клавиатуры.

При нажатии функциональных клавиш (Shift, Alt, Ctrl) виртуальной клавиатуры специальный режим ввода фиксируется (например, при нажатии Shift все символы будут вводиться в верхнем регистре). Для отмены специального режима нажмите функциональную клавишу повторно.

Виртуальная клавиатура не может обезопасить ваши конфиденциальные данные в случае взлома сайта, требующего ввод таких данных, так как в данном случае информация попадет непосредственно в руки злоумышленников.

НАСТРОЙКА ПАРАМЕТРОВ ПРИЛОЖЕНИЯ

Окно настройки параметров приложения предназначено для быстрого доступа к основным настройкам Kaspersky Internet Security.

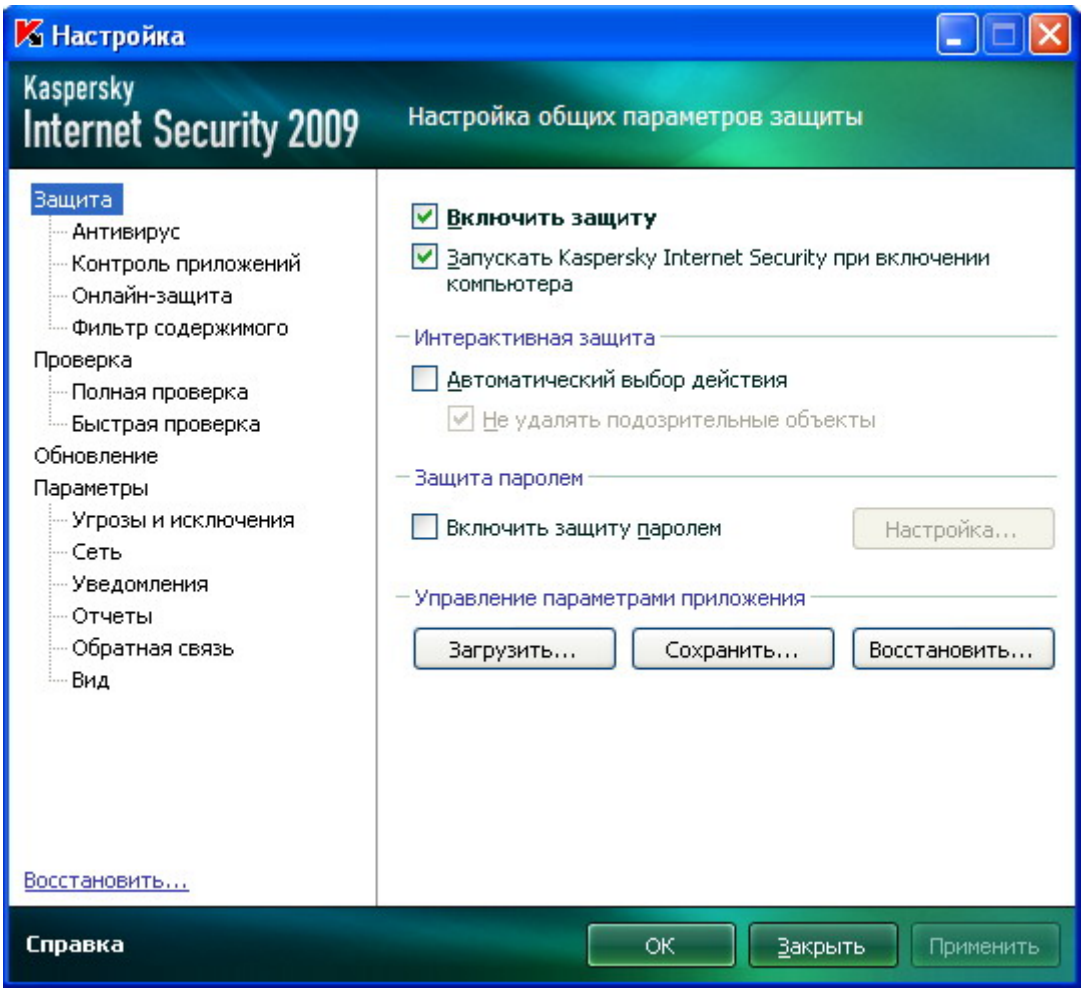

Рисунок 21: Окно настроек параметров приложения

Окно настройки состоит из двух частей:

- левая часть окна обеспечивает доступ к компонентам Kaspersky Internet Security, задачам поиска вирусов, обновления и др;
- правая часть окна содержит перечень параметров выбранного в левой части компонента, задачи и т. п.

Открыть окно можно следующими способами:

- Из главного окна приложения (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36). Для этого нажмите на кнопку **Настройка** в верхней части главного окна.

- Из контекстного меню (см. раздел «Контекстное меню» на стр. 35). Для этого выберите пункт **Настройка** в контекстном меню приложения.

Рисунок 22: Контекстное меню

- Из контекстного меню для отдельных компонентов. Для этого выберите пункт **Настройка** в меню.

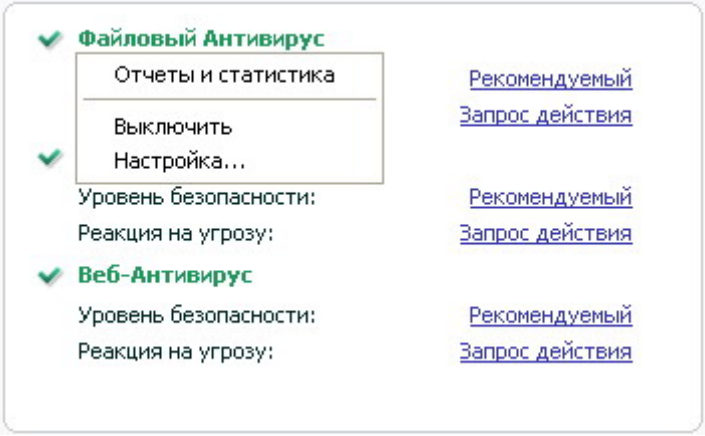

Рисунок 23: Вызов окна настройки параметров

В ЭТОМ РАЗДЕЛЕ

ЗАЩИТА

В окне **Защита** вы можете воспользоваться следующими дополнительными функциями Kaspersky Internet Security:

- Включение / отключение защиты приложения.
- Запуск приложения при старте операционной системы.
- Использование интерактивного режима защиты.
- Ограничение доступа к приложению.
- Экспорт / импорт параметров работы приложения.
- Восстановление параметров работы приложения по умолчанию.

См. также

ОТКЛЮЧЕНИЕ / ВКЛЮЧЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

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 отключить защиту, обеспечиваемую приложением, полностью или частично.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют **не отключать защиту**, поскольку это может привести к заражению вашего компьютера и потере данных.

В результате отключения защиты работа всех ее компонентов останавливается. Об этом свидетельствуют:

- Неактивные (черного цвета) названия выключенных компонентов в главном окне приложения (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36).
- Неактивный (серый) значок приложения (см. раздел «Значок в области уведомлений» на стр. 34) в области уведомлений панели задач.
- Красный цвет индикатора безопасности (см. раздел «Выбор типа событий» на стр. 186).

Обратите внимание, что в данном случае защита рассматривается именно в контексте компонентов защиты. Отключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки на вирусы и обновления Kaspersky Internet Security.

Чтобы отключить защиту полностью, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. Снимите флажок **Включить защиту**.

ЗАПУСК ПРИЛОЖЕНИЯ ПРИ СТАРТЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Если по какой-либо причине вам требуется полностью завершить работу Kaspersky Internet Security, выберите пункт **Выход** контекстного меню (см. раздел «Контекстное меню» на стр. 35) приложения. В результате приложение будет выгружено из оперативной памяти, что подразумевает, что ваш компьютер на данный период работает в незащищенном режиме.

Теперь включить защиту компьютера снова вы можете, загрузив приложение из меню **Пуск → Программы → Kaspersky Internet Security 2009 → Kaspersky Internet Security 2009**.

Также защита может быть запущена автоматически после перезагрузки операционной системы.

Чтобы включить этот режим, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. Установите флажок **Запускать Kaspersky Internet Security при включении компьютера**.

ИСПОЛЬЗОВАНИЕ ИНТЕРАКТИВНОГО РЕЖИМА ЗАЩИТЫ

Kaspersky Internet Security взаимодействует с пользователем в двух режимах:

- **Интерактивный режим защиты**. Приложение уведомляет пользователя о всех опасных и подозрительных событиях в системе. В этом режиме пользователю предстоит самостоятельно принимать решение о разрешении или запрещении каких-либо действий.
- **Автоматический режим защиты**. Приложение будет автоматически применять рекомендуемое экспертами «Лаборатории Касперского» действие при возникновении опасных событий.

Чтобы использовать автоматический режим защиты, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Интерактивная защита** установите флажок **Автоматический выбор действия**. Если вы не хотите, чтобы приложение удаляло подозрительные объекты при работе в автоматическом режиме, установите флажок **Не удалять подозрительные объекты**.

ОГРАНИЧЕНИЕ ДОСТУПА К ПРИЛОЖЕНИЮ

Персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности. Открытый доступ к приложению, его параметрам может значительно снизить уровень безопасности компьютера в целом.

Чтобы повысить безопасность компьютера, используйте пароль для доступа к Kaspersky Internet Security. Вы можете заблокировать любые операции с приложением, за исключением работы с уведомлениями об обнаружении опасных объектов, или запретить выполнение одного из следующих действий:

- Изменить параметры работы приложения.
- Завершить работу приложения.

Каждое из перечисленных выше действий приводит к снижению уровня защиты вашего компьютера, поэтому постарайтесь определить, кому из пользователей вашего компьютера вы доверяете выполнять такие действия.

Чтобы защитить доступ к приложению с помощью пароля, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. 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. Теперь при попытке любого пользователя на вашем компьютере выполнить выбранные вами действия приложение всегда будет запрашивать пароль.

ЭКСПОРТ / ИМПОРТ ПАРАМЕТРОВ РАБОТЫ ПРИЛОЖЕНИЯ

Kaspersky Internet Security предоставляет вам возможность экспорта и импорта своих параметров.

Это полезно, например, в том случае, когда приложение установлено у вас на домашнем компьютере и в офисе. Вы можете настроить приложение на удобный для вас режим работы дома, сохранить эти параметры на диск и с помощью функции импорта быстро загрузить их на свой рабочий компьютер. Параметры хранятся в специальном конфигурационном файле.

Чтобы экспортировать текущие параметры работы приложения, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами приложения** нажмите на кнопку **Сохранить**.
4. В открывшемся окне введите название конфигурационного файла и укажите место его сохранения.

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

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами приложения** нажмите на кнопку **Загрузить**.
4. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры приложения.

ВОССТАНОВЛЕНИЕ ПАРАМЕТРОВ ПО УМОЛЧАНИЮ

Вы всегда можете вернуться к рекомендуемым параметрам работы Kaspersky Internet Security. Они считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского». Восстановление настроек осуществляется Мастером первоначальной настройки (см. раздел «Мастер настройки приложения» на стр. 41) приложения.

В открывшемся окне вам предлагается определить, какие параметры и для каких компонентов следует или не следует сохранять параллельно с восстановлением рекомендуемого уровня безопасности.

В списке представлены компоненты Kaspersky Internet Security, параметры которых были изменены пользователем или накоплены приложением в результате обучения компонентов Сетевой экран и Анти-Спам. Если для какого-либо из компонентов в процессе работы были сформированы уникальные параметры, они также будут представлены в списке.

Такими уникальными параметрами являются «белые» и «черные» списки фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, используемых компонентами Веб-Антивирус и Онлайн-защита, сформированные правила исключений защиты для компонентов приложения, правила фильтрации пакетов и приложений Сетевого экрана.

Данные списки формируются в процессе работы с приложением, исходя из индивидуальных задач и требований безопасности, и их формирование зачастую занимает много времени. Поэтому мы рекомендуем сохранять их при восстановлении первоначальных настроек приложения.

По завершении работы мастера для всех компонентов защиты будет установлен **Рекомендуемый** уровень безопасности с учетом тех параметров, которые вы решили сохранить при восстановлении. Кроме того, будут применены настройки, которые вы выполнили в ходе работы мастера.

Чтобы восстановить параметры защиты, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами приложения** нажмите на кнопку **Восстановить**.
4. В открывшемся окне установите флажки для тех параметров, для которых требуется сохранение. Нажмите на кнопку **Далее**. Будет запущен Мастер первоначальной настройки, следуйте его указаниям.

Антивирус

В окне **Антивирус** собраны настройки для трех компонентов защиты:

- **Файлового Антивируса**. Файловый Антивирус перехватывает обращение пользователя или некоторой программы к каждому файлу при открытии, сохранении и запуске и проверяет этот файл.
- **Почтового Антивируса**. Почтовый Антивирус проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP, MAPI и NNTP.
- **Веб-Антивируса**. Веб-Антивирус защищает информацию, поступающую на ваш компьютер по HTTP-протоколу, а также предотвращает запуск на компьютере опасных скриптов.

По умолчанию компоненты защиты запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить постоянную защиту полностью или частично.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют **не отключать защиту**, поскольку это может привести к заражению вашего компьютера и потере данных.

Кроме этого, для каждого компонента вы можете:

- выбрать уровень безопасности, на основе параметров которого будет работать компонент;
- выбрать действие, которое будет применено Kaspersky Internet Security при обнаружении зараженного / возможно зараженного объекта;
- сформировать область защиты для каждого компонента;
- задать использование эвристического анализа;
- настроить другие специфические для каждого компонента параметры.

Чтобы отключить защиту от вредоносного ПО полностью, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. В правой части окна снимите флажок **Включить Антивирус**. В результате все компоненты прекратят свою работу.

Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. В правой части окна снимите флажок **Включить <название компонента>** для соответствующего компонента.

Чтобы перейти к настройке параметров компонента, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Антивирус**.
3. В правой части окна выберите уровень безопасности и реакцию на угрозу для компонента, параметры которого вы хотите изменить. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров компонента.

Контроль приложений

В окне **Контроль приложений** собраны настройки для трех компонентов Kaspersky Internet Security:

- **Фильтрации активности**. Фильтрация активности контролирует доступ приложений к важным системным ресурсам и разрешает или запрещает действие приложения, исходя из опасности приложения для системы.
- **Сетевого экрана**. Сетевой экран контролирует сетевую активность на вашем компьютере с помощью правил, разрешающих или запрещающих передачу данных в зависимости от направления, протокола передачи и адресов и портов назначения передачи.
- **Проактивной защиты**. Проактивная защита регистрирует последовательность действий, совершаемых приложением в системе, и в случае обнаружения подозрительной активности блокирует ее.

По умолчанию компоненты Контроля приложений запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить Контроль приложений полностью или частично.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют не отключать Контроль приложений, поскольку это может привести к заражению вашего компьютера и потере данных.

Кроме этого, для каждого компонента вы можете настроить параметры его работы.

Чтобы отключить Контроль приложений полностью, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. В правой части окна снимите флажок **Включить Контроль приложений**. В результате все компоненты Контроля приложений прекратят свою работу.

Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. В правой части окна снимите флажок **Включить <название компонента>** для соответствующего компонента.

Чтобы перейти к настройке параметров компонента, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Контроль приложений**.
3. В правой части окна нажмите на кнопку **Настройка**, чтобы перейти к настройкам параметров нужного компонента.

ОНЛАЙН-ЗАЩИТА

В окне **Онлайн-защита** собраны настройки для трех компонентов Kaspersky Internet Security:

- **Защиты от сетевых атак**. Защита от сетевых атак распознает во входящем сетевом трафике активность, характерную для известных сетевых атак, и блокирует действия удаленного компьютера в отношении вашего.
- **Анти-Дозвона**. Анти-Дозвон обнаруживает попытки установить скрытое модемное соединение и блокирует эту активность.
- **Анти-Фишинга**. Анти-Фишинг отслеживает попытки открытия фишинг-сайта и блокирует его.

По умолчанию компоненты Онлайн-защиты запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить Онлайн-защиту полностью или частично.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют не отключать Онлайн-защиту, поскольку это может привести к атакам хакеров и мошенников на ваш компьютер.

Кроме этого, для каждого компонента вы можете настроить параметры его работы.

Чтобы отключить Онлайн-защиту полностью, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. В правой части окна снимите флажок **Включить Онлайн-защиту**. В результате все компоненты Онлайн-защиты прекратят свою работу.

Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Онлайн-защита**.
3. В правой части окна снимите флажок **Включить <название компонента>** для соответствующего компонента.

Чтобы перейти к настройке параметров компонента, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Онлайн-защита**.

3. В правой части окна нажмите на кнопку **Настройка**, чтобы перейти к настройкам параметров компонента.

ФИЛЬТР СОДЕРЖИМОГО

В окне **Фильтр содержимого** собраны настройки для трех компонентов Kaspersky Internet Security:

- **Анти-Спама**. Анти-Спам обнаруживает нежелательную корреспонденцию (спам) и обрабатывает ее в соответствии с правилами вашего почтового клиента.

- **Анти-Баннера.** Анти-Баннер блокирует рекламную информацию, размещенную на баннерах в интернете или встроенных в интерфейс различных программ, установленных на вашем компьютере.

- **Родительского контроля**. Родительский контроль позволяет контролировать доступ пользователей компьютера к интернет-ресурсам, содержащим информацию определенных категорий или являющимся потенциальной причиной потери денег.

По умолчанию компоненты Фильтра содержимого запускаются при старте операционной системы и защищают ваш компьютер в течение всего сеанса работы. Вы можете отключить Фильтра содержимого полностью или частично.

Специалисты ЗАО «Лаборатории Касперского» настоятельно рекомендуют не отключать Фильтр содержимого, поскольку это может привести к получению нежелательных данных.

Кроме этого, для каждого компонента вы можете настроить параметры его работы.

Чтобы отключить Фильтр содержимого полностью, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. В правой части окна снимите флажок **Включить Фильтр содержимого**. В результате все компоненты Фильтра содержимого прекратят свою работу.

Чтобы отключить использование какого-либо из компонентов защиты, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. В правой части окна снимите флажок **Включить <название компонента>** для соответствующего компонента.

Чтобы перейти к настройке параметров компонента, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Фильтр содержимого**.

3. В правой части окна нажмите на кнопку **Настройка**, чтобы перейти к настройкам параметров компонента.

ПРОВЕРКА

То, каким образом осуществляется проверка объектов на вашем компьютере, определяется набором параметров, заданных для каждой задачи.

Специалистами ЗАО «Лаборатория Касперского» выделены несколько задач поиска вирусов. В их число входят:

Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

В окне настройки для каждой из задач вы можете:

- выбрать уровень безопасности, на основе параметров которого будет выполняться задача;
- выбрать действие, которое будет применено приложением при обнаружении зараженного / возможно зараженного объекта;
- сформировать расписание автоматического запуска задачи;
- определить типы файлов, подвергаемые анализу на вирусы;
- определить параметры проверки составных файлов;
- выбрать методы и технологии проверки;
- назначить единые параметры проверки для всех задач.

Чтобы перейти к настройке параметров задачи, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. В правой части окна выберите нужный уровень безопасности, реакцию на угрозу и настройте режим запуска. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров задач. Чтобы восстановить настройки параметров, принятые по умолчанию, нажмите на кнопку **Восстановить**.

См. также

Обновление

Обновление Kaspersky Internet Security осуществляется в соответствии с параметрами, определяющими:

- с какого ресурса производится копирование и установка обновлений приложения;
- в каком режиме запускается процесс обновления приложения и что именно обновляется;
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию;
- от имени какой учетной записи будет запущено обновление;
- требуется ли копировать полученные обновления в локальный источник;
- какие действия нужно выполнять после обновления приложения.

Чтобы перейти к настройке параметров обновления, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Обновление**.
3. В правой части окна выберите нужный режим запуска. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров задачи. Чтобы восстановить настройки параметров, принятые по умолчанию, нажмите на кнопку **Восстановить**.

См. также

ПАРАМЕТРЫ

В окне **Параметры** вы можете воспользоваться следующими дополнительными функциями приложения:

- Самозащита приложения.
- Использование технологии лечения активного заражения.
- Сервис экономии заряда аккумулятора.
- Отложенное выполнение задач поиска вирусов при замедлении работы других программ.

См. также

САМОЗАЩИТА ПРИЛОЖЕНИЯ

Kaspersky Internet Security обеспечивает безопасность компьютера от вредоносных программ, и в силу этого само становится объектом интереса со стороны вредоносного программного обеспечения, пытающегося заблокировать работу приложения или даже удалить его с компьютера.

Чтобы обеспечить стабильность системы безопасности вашего компьютера, в приложение добавлены механизмы самозащиты и защиты от удаленного воздействия.

Под управлением 64-разрядных операционных систем и Microsoft Windows Vista доступно только управление механизмом самозащиты приложения от изменения или удаления собственных файлов на диске, а также записей в системном реестре.

При использовании защиты от удаленного воздействия возникает необходимость предоставить доступ к управлению приложением программ удаленного администрирования (например, RemoteAdmin). Для этого необходимо добавить эти программы в список доверенных приложений и включить для них параметр **Исключить контроль активности приложения**.

Чтобы включить использование механизмов самозащиты приложения, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Самозащита** установите флажок **Включить самозащиту**, чтобы задействовать механизм защиты приложения от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

   В блоке **Самозащита** установите флажок **Отключить возможность внешнего управления системной службой**, чтобы заблокировать любую попытку удаленного управления сервисами приложения.

   При попытке выполнить какое-либо из перечисленных действий над значком приложения в области уведомлений панели задач Microsoft Windows будет открыто уведомление (если сервис уведомлений не отключен пользователем).

ТЕХНОЛОГИЯ ЛЕЧЕНИЯ АКТИВНОГО ЗАРАЖЕНИЯ

Современные вредоносные программы могут внедряться на самые низкие уровни операционной системы, что делает процесс их удаления практически невозможным. Kaspersky Internet Security при обнаружении угрозы, которая в данный момент активна в системе, предлагает провести специальную расширенную процедуру лечения, в результате которой угроза будет обезврежена и удалена с компьютера.

По окончании процедуры будет произведена обязательная перезагрузка компьютера. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы.

Для применения процедуры расширенного лечения, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Совместимость** установите флажок **Применять технологию активного лечения**.

РАБОТА ПРИЛОЖЕНИЯ НА ПОРТАТИВНОМ КОМПЬЮТЕРЕ

В целях экономии питания аккумулятора портативного компьютера вы можете отложить выполнение задач поиска вирусов.

Поскольку поиск вирусов на компьютере и обновление приложения подчас требуют достаточного количества ресурсов и занимают некоторое время, рекомендуем вам отключать запуск таких задач по расписанию. Это позволит вам сэкономить заряд аккумулятора. По мере необходимости вы сможете самостоятельно обновить приложение или запустить проверку на вирусы.

Чтобы воспользоваться сервисом экономии заряда аккумулятора, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Параметры**.

3. В блоке **Совместимость** установите флажок **Не запускать проверки по расписанию при работе от аккумуляторов**.

ПРОИЗВОДИТЕЛЬНОСТЬ КОМПЬЮТЕРА ПРИ ВЫПОЛНЕНИИ ЗАДАЧ

В целях ограничения нагрузки на центральный процессор и дисковые подсистемы, вы можете отложить выполнение задач поиска вирусов.

Выполнение задач поиска вирусов 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 поиска вирусов и высвобождает ресурсы системы для приложений пользователя.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Для того чтобы поиск вирусов не зависел от работы таких программ, не следует уступать им ресурсы системы.

Обратите внимание, что данный параметр можно настраивать индивидуально для каждой задачи поиска вирусов. В этом случае настройка параметра, произведенная для конкретной задачи, имеет более высокий приоритет.

Чтобы отложить выполнение задач поиска вирусов при замедлении работы других программ, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Параметры**.

3. В блоке **Совместимость** установите флажок **Уступать ресурсы другим приложениям**.

УГРОЗЫ И ИСКЛЮЧЕНИЯ

В разделе **Угрозы и исключения** окна настройки Kaspersky Internet Security вы можете:

- выбрать категории обнаруживаемых угроз (см. раздел «Выбор категорий обнаруживаемых угроз» на стр. 173);

- сформировать доверенную зону приложения.

Доверенная зона - это перечень объектов, сформированный пользователем, который приложение не контролирует в процессе своей работы. Другими словами, это набор исключений из защиты приложения.

Доверенная зона формируется на основе списка доверенных приложений (см. раздел «Выбор доверенных приложений» на стр. 173) и правил исключений.

Доверенную зону формирует пользователь, исходя из особенностей объектов, с которыми он работает, а также программ, установленных на компьютере. Создание такого списка исключений может потребоваться, например, в случае, если приложение блокирует доступ к какому-либо объекту или программе, а вы уверены, что данный объект/ программа абсолютно безвредны.

См. также

ВЫБОР КАТЕГОРИЙ ОБНАРУЖИВАЕМЫХ УГРОЗ

Kaspersky Internet Security предлагает вам защиту от разных видов вредоносного программного обеспечения. Вне зависимости от установленных параметров приложение всегда проверяет и обезвреживает вирусы, троянские программы и хакерские утилиты. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера вы можете расширить список обнаруживаемых угроз, включив контроль за разного рода потенциально-опасными программами.

Чтобы выбрать категории обнаруживаемых угроз, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Угрозы и исключения**.
3. В блоке **Угрозы** нажмите на кнопку **Настройка**.
4. В открывшемся окне **Угрозы** выберите категории угроз, от которых вы хотите защищать ваш компьютер.

ВЫБОР ДОВЕРЕННЫХ ПРИЛОЖЕНИЙ

Вы можете формировать список доверенных программ, активность которых, в том числе и подозрительная, а также файловая, сетевая активность и обращение к системному реестру не будут контролироваться.

Например, вы считаете объекты, используемые стандартной программой Microsoft Windows - Блокнот, безопасными и не требующими проверки. Другими словами, вы доверяете этой программе. Чтобы исключить проверку объектов, используемых данным процессом, добавьте программу Блокнот в список доверенных приложений. Однако исполняемый файл и процесс доверенного приложения по-прежнему будут проверяться на вирусы. Для полного исключения приложения из проверки следует пользоваться правилами исключений.

Кроме того, некоторые действия, классифицирующиеся как опасные, являются нормальными в рамках функциональности ряда программ. Так, например, перехват текста, вводимого вами с клавиатуры, является нормальным действием для программ автоматического переключения раскладок клавиатуры (Punto Switcher и др.). Для того чтобы учесть специфику таких программ и отключить контроль их активности, мы рекомендуем добавить их в список доверенных.

Также использование исключения доверенных программ из проверки позволяет решать возможные проблемы совместимости приложения с другими программами (например, сетевой трафик с другого компьютера, уже проверенный антивирусным приложением), а также увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

По умолчанию приложение проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и сетевой трафик, создаваемый ими.

Чтобы добавить приложение в список доверенных, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Доверенные приложения** нажмите на ссылку **Добавить**.
5. В раскрывшемся меню выберите приложение. При выборе пункта **Обзор** открывается окно, в котором необходимо указать путь к исполняемому файлу. При выборе пункта **Приложения** открывается список приложений, работающих в данный момент.
6. В открывшемся окне **Исключения для приложения** задайте параметры правила для приложения.

Обратите внимание, что при установленном флажке **Исключать проверку сетевого трафика** не проверяется трафик указанного приложения только на вирусы и спам. Однако это не влияет на проверку трафика компонентом Сетевой экран, в соответствии с параметрами которого анализируется сетевая активность данного приложения.

Вы можете изменить или удалить доверенное приложение из списка с помощью одноименных ссылок в нижней части закладки. Для того, чтобы исключить приложение из списка, не удаляя его, снимите флажок рядом с приложением.

Правила исключений

Потенциально опасное программное обеспечение не имеет какой-либо вредоносной функции, но может быть использовано в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и ошибки. В эту категорию попадают, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, всевозможные утилиты для остановки процессов или скрытия их работы, клавиатурные шпионы, программы вскрытия паролей, автоматического дозвона на платные сайты и т.д. Данное программное обеспечение не классифицируется как вирусы (not-a-virus), но его можно разделить на типы, например, Adware, Joke, Riskware и др. (подробную информацию о потенциально опасных программах, обнаруживаемых приложением, смотрите в Вирусной энциклопедии на сайте www.viruslist.ru). В результате проверки такие программы могут быть заблокированы. А поскольку некоторые из них широко используются пользователями, то предусмотрена возможность исключить их из проверки.

Например, вы часто используете в своей работе программу Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. Такая активность рассматривается приложением как потенциально опасная и может быть заблокирована. Чтобы исключить блокировку приложения, нужно сформировать правило исключения для приложения, распознаваемого, как not-a-virus:RemoteAdmin.Win32.RAdmin.22 согласно Вирусной энциклопедии.

Правило исключения - это совокупность условий, при которых объект не будет проверяться приложением.

Исключать из проверки можно файл определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии.

Тип угрозы - это статус, который присвоен объекту Kaspersky Internet Security при проверке. Статус присваивается на основании классификации вредоносных и потенциально-опасных программ, представленных в Вирусной энциклопедии «Лаборатории Касперского».

При добавлении исключения формируется правило, которое потом может использоваться некоторыми компонентами приложения (Файловый Антивирус (см. раздел «Защита файлов и памяти» на стр. 55), Почтовый Антивирус (см. раздел «Защита почты» на стр. 65), Веб-Антивирус (см. раздел «Защита веб-трафика» на стр. 71), Фильтрация активности (на стр. 77)), а также при выполнении задач поиска вирусов.

Чтобы создать правило исключения, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Правила исключений** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Правила исключений** задайте параметры правила исключения.

Дополнительные параметры исключения

Для некоторых объектов по типу угрозы в поле **Дополнительные параметры** можно задать дополнительные условия применения правила. Указание дополнительных параметров может потребоваться, например, в следующих случаях:

- *Invader (внедрение в процессы программ)*. Для данной угрозы в качестве дополнительного условия исключения вы можете указать имя, маску либо полный путь к внедряемому объекту (например, файлу dll).

- *Launching Internet Browser (запуск браузера с параметрами)*. Для данной угрозы в качестве дополнительного условия исключения вы можете указать параметры запуска браузера. Например, в анализе активности приложений Проактивной защиты вы запретили запуск браузера с параметрами. Но в качестве правила исключения вы хотите разрешить запуск браузера для домена www.kasperky.com по ссылке из Microsoft Office Outlook. Для этого в качестве Объекта исключения укажите программу Microsoft Office Outlook, в качестве Типа угрозы укажите Launching Internet Browser, а в поле **Дополнительные параметры** введите маску разрешенного домена.

РАЗРЕШЕННЫЕ МАСКИ ИСКЛЮЧЕНИЙ ФАЙЛОВ

Рассмотрим примеры разрешенных масок, которые вы можете использовать при формировании списка исключаемых файлов:

1. Маски без путей к файлам:

   - ***.exe** - все файлы с расширением *exe*

   - ***.ex?** - все файлы с расширением *ex?*, где вместо **?** может использоваться любой один символ

   - **test** - все файлы с именем *test*

2. Маски с абсолютными путями к файлам:

   - **C:\dir*.*** или **C:\dir*** или **C:\dir** – все файлы в папке *C:\dir*

   - **C:\dir*.exe** - все файлы с расширением exe в папке *C:\dir*

   - **C:\dir*.ex?** - все файлы с расширением *ex?* в папке *C:\dir*, где вместо **?** может использоваться любой один символ

   - **C:\dir\test** - только файл *C:\dir\test*

     Для того чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок **Включая вложенные папки**.

3. Маски с относительными путями к файлам:

   - **dir*.*** или **dir*** или **dir** – все файлы во всех папках *dir*

   - **dir\test** - все файлы *test* в папках *dir*

   - **dir*.exe** - все файлы с расширением *exe* во всех папках *dir*

   - **dir*.ex?** - все файлы с расширением *ex?* во всех папках *dir*, где вместо **?** может использоваться любой один символ

     Для того чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок **Включая вложенные папки**.

Использовать маски исключения ***.*** или * допустимо только при указании типа исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данных масок без указания типа угрозы равносильно отключению защиты.

Также не рекомендуется в качестве исключения выбирать виртуальный диск, сформированный на основе каталога файловой системы посредством команды subst. Это не имеет смысла, поскольку во время проверки приложение воспринимает этот виртуальный диск как каталог, следовательно, проверяет его.

РАЗРЕШЕННЫЕ МАСКИ ТИПОВ УГРОЗ

При добавлении в качестве исключения угрозы с определенным статусом по классификации Вирусной энциклопедии вы можете указать:

- полное имя угрозы, как оно представлено в вирусной энциклопедии на сайте www.viruslist.ru (например, not-a-virus:RiskWare.RemoteAdmin.RA.311 или Flooder.Win32.Fuxx);
- имя угрозы по маске, например:
  - **not-a-virus*** - исключать из проверки легальные, но потенциально опасные программы, а также программы-шутки.
  - ***Riskware.*** - исключать из проверки все потенциально опасные программы типа Riskware.
  - ***RemoteAdmin.*** - исключать из проверки все версии программы удаленного администрирования.

УВЕДОМЛЕНИЯ

В процессе работы Kaspersky Internet Security возникают различного рода события. Они могут быть информационного характера, а также нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении приложения, а может фиксировать ошибку в работе некоторого компонента, которую необходимо срочно устранить.

Для того чтобы быть в курсе событий в работе приложения, вы можете воспользоваться сервисом уведомлений.

По умолчанию уведомление пользователя происходит с помощью всплывающих сообщений в комбинации со звуковым сигналом.

Уведомления могут быть реализованы одним из следующих способов:

- Всплывающие сообщения над значком приложения в системной панели.
- Звуковое оповещение.
- Сообщения электронной почты.

Чтобы отключить доставку уведомлений, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Уведомления**.
3. Снимите флажок **Уведомлять о событиях**.

Даже если доставка уведомлений отключена, информация о событиях, возникающих в ходе работы приложения, будет записана в отчет о работе приложения.

Чтобы выбрать способ доставки уведомлений, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Уведомления** и нажмите на кнопку **Настройка**.
3. В открывшемся окне **Уведомления** выберите способ доставки уведомлений.

См. также

Отключение звукового сопровождения уведомлений

По умолчанию все уведомления сопровождаются звуковым сигналом; в качестве звукового сопровождения используется звуковая схема Microsoft Windows. Флажок **Использовать классическую звуковую схему Windows Default** позволяет изменить использующуюся схему. Если флажок снят, в качестве звукового сопровождения будет использоваться звуковая схема предыдущих версий приложения.

Чтобы отключить звуковое сопровождение уведомлений, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Уведомления**.
3. Снимите флажок **Включить звуковое сопровождение уведомлений**.

Доставка уведомлений с помощью электронной почты

Для доставки уведомлений с помощью электронной почты необходимо настроить параметры доставки.

Чтобы настроить параметры электронной почты для доставки уведомлений, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Уведомления**.
3. Установите флажок **Отправлять почтовые сообщения о событиях** и нажмите на кнопку **Настройка e-mail**.
4. В открывшемся окне **Настройка почтовых уведомлений** задайте параметры доставки.

Сеть

В разделе **Сеть** окна настройки приложения вы можете выбрать порты, контролируемые Kaspersky Internet Security, и настроить проверку защищенных соединений:

- Сформировать список контролируемых портов.
- Включить/отключить режим проверки защищенных соединений (по протоколу SSL).
- Настроить параметры прокси-сервера.
- Открыть доступ к Анализу сетевых пакетов.

См. также

Формирование списка контролируемых портов

В работе таких компонентов защиты как Почтовый Антивирус (см. раздел «Защита почты» на стр. 65), Веб-Антивирус (см. раздел «Защита веб-трафика» на стр. 71) и Анти-Спам (на стр. 103) контролируются потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые порты вашего компьютера. Так, например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, Веб-Антивирус - HTTP-пакеты.

Вы можете выбрать один из двух режимов контроля портов:

- **Контролировать все сетевые порты**;
- **Контролировать только выбранные порты**. Список портов, которые обычно используются для передачи почты и HTTP-трафика, включен в поставку приложения.

Чтобы добавить порт в список контролируемых портов, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Контролируемые порты** нажмите на кнопку **Выбрать**.
4. В открывшемся окне **Сетевые порты** нажмите на ссылку **Добавить**.
5. В открывшемся окне **Сетевой порт** укажите необходимые данные.

Чтобы исключить порт из списка контролируемых портов, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Контролируемые порты** нажмите на кнопку **Выбрать**.
4. В открывшемся окне **Сетевые порты** снимите флажок рядом с описанием порта.

Проверка защищенных соединений

Соединение с использованием протокола SSL обеспечивает защиту канала обмена данными в интернете. Протокол SSL позволяет идентифицировать обменивающиеся данными стороны на основе электронных сертификатов, осуществлять шифрование передаваемых данных и обеспечивать их целостность в процессе передачи.

Эти особенности протокола используются злоумышленниками для распространения вредоносных программ, поскольку большинство антивирусных продуктов не проверяет SSL-трафик.

Kaspersky Internet Security реализует проверку защищенных соединений с помощью установки сертификата «Лаборатории Касперского». Этот сертификат всегда будет использоваться для проверки безопасности соединения.

В дальнейшем проверка трафика по протоколу SSL будет производиться с помощью установленного сертификата «Лаборатории Касперского». В случае обнаружения некорректного сертификата при соединении с сервером (например, при подмене сертификата злоумышленником) на экран будет выведено уведомление, в котором вам будет предложено принять или отвергнуть сертификат, или просмотреть информацию о сертификате. Если приложение работает в автоматическом режиме, соединение, использующее некорректный сертификат, будет разорвано без запроса.

Чтобы включить проверку защищенных соединений, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Сеть**.
3. Установите флажок **Проверять защищенные соединения**.
4. Нажмите на кнопку **Установить сертификат**.
5. В открывшемся окне нажмите на кнопку **Установить сертификат**. Будет запущен мастер, следуя указаниям которого вы установите сертификат.

Автоматическая установка сертификата работает только при работе с браузером Microsoft Internet Explorer. Для проверки защищенных соединений в браузерах Mozilla Firefox и Opera установите сертификат «Лаборатории Касперского» вручную.

См. также

Проверка защищенных соединений в Mozilla Firefox 179

Проверка защищенных соединений в Opera 180

ПРОВЕРКА ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В MOZILLA FIREFOX

Браузер Mozilla Firefox не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при пользовании Firefox 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 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\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. В открывшемся окне установите флажки для выбора действий, для проверки которых будет применяться установленный сертификат. Для просмотра информации о сертификате воспользуйтесь кнопкой **Просмотр**.

См. также

Проверка защищенных соединений 178

Проверка защищенных соединений в Opera 180

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\AVP8\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**.

См. также

Проверка защищенных соединений 178

Проверка защищенных соединений в Mozilla Firefox 179

Параметры прокси-сервера

Если выход в интернет осуществляется через прокси-сервер, может возникнуть необходимость настроить параметры подключения к нему. Приложение использует эти параметры в работе некоторых компонентов защиты, а также для обновления баз и модулей приложения.

Если в вашей сети используется прокси-сервер, который использует нестандартный порт, то данный порт необходимо добавить в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 178).

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте окно настройки приложения.
2. В левой части окна выберите раздел **Сеть**.

3. В блоке **Прокси-сервер** нажмите на кнопку **Настройка прокси-сервера**.

4. В открывшемся окне **Параметры прокси-сервера** измените параметры прокси-сервера.

Доступ к Анализу сетевых пакетов

Инструмент **Анализ сетевых пакетов** предназначен для опытных пользователей, обладающих знаниями о принципах построения сетей и сетевых протоколах.

В состав Kaspersky Internet Security входит инструмент *Анализ сетевых пакетов*. Этот инструмент предназначен для сбора и анализа сетевой активности в сети, в которую входит ваш компьютер.

По умолчанию Анализ сетевых пакетов недоступен в главном окне приложения.

Чтобы открыть доступ к Анализу сетевых пакетов, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Сеть**.

3. В блоке **Анализ сетевых пакетов** установите флажок **Показывать монитор Анализ сетевых пакетов**.

Анализ сетевых пакетов отображается в списке задач для функции Фильтр содержимого (на стр. 103).

Отчеты

Работа каждого компонента Kaspersky Internet Security и выполнение каждой задачи поиска вирусов и обновления фиксируется в отчете. В разделе **Отчеты** окна настройки приложения вы можете задать параметры хранения файлов отчетов и статистики, а также указать какие события должны выводиться в отчет. Вы можете добавить в отчет защиты записи о некритических событиях, событиях реестра и файловой системы. По умолчанию эти записи в отчет не добавляются.

В блоке **События** вы можете задать время хранения файлов отчетов приложения и максимальный размер файла отчета. При достижении максимального размера содержимое файла переписывается новыми записями.

В блоке **Статистика** вы можете задать время хранения файлов статистики приложения и максимальный размер файла статистики. При достижении максимального размера содержимое файла переписывается новыми записями.

Нажмите на кнопку **Очистить** в блоках **События**, чтобы очистить отчеты о работе приложения.

См. также

Отчеты 185

Очистка отчетов приложения 181

Статистика работы приложения 192

Добавление в отчет записей о событиях 182

Очистка отчетов приложения

Информация о работе приложения фиксируется в отчете (см. раздел «Отчеты» на стр. 185). Вы можете очистить отчеты о работе Kaspersky Internet Security.

- *Чтобы очистить отчеты* приложения, *выполните следующие действия*:

  1. Откройте окно настройки приложения.
  2. В левой части окна выберите раздел **Отчеты**.
  3. В блоке **События** нажмите на кнопку **Очистить**.
  4. В открывшемся окне **Удаление информации из отчетов** установите флажки для тех категорий отчетов, которые вы хотите очистить.

ДОБАВЛЕНИЕ В ОТЧЕТ ЗАПИСЕЙ О СОБЫТИЯХ

Вы можете добавлять в отчет защиты записи о некритических событиях, событиях реестра и файловой системы. По умолчанию эти записи в отчет не добавляются.

- *Чтобы добавлять в отчет записи о некритических событиях, событиях реестра и / или файловой системы, выполните следующие действия:*

  1. Откройте окно настройки приложения.
  2. В левой части окна выберите раздел **Отчеты**.
  3. В блоке **События** установите нужный флажок.

ОБРАТНАЯ СВЯЗЬ

Каждый день в мире появляются множество новых угроз. Для ускорения сбора статистики о типе новых угроз, их источнике и разработки способа нейтрализации «Лаборатория Касперского» предоставляет вам право воспользоваться услугой *Kaspersky Security Network*.

Использование Kaspersky Security Network подразумевает отправку «Лаборатории Касперского» следующей информации:

- Уникального идентификатора, присваиваемого вашему компьютеру приложением «Лаборатории Касперского». Этот идентификатор характеризует аппаратные параметры вашего компьютера и не содержит никакой личной информации.
- Информации об угрозах, обнаруженных компонентами приложения. Состав информации зависит от типа обнаруженной угрозы.
- Информации о системе: версии операционной системы, установленные пакеты обновлений, загружаемые сервисы и драйверы, версии браузеров и почтовых клиентов, расширения браузеров, номер версии установленного приложения «Лаборатории Касперского».

- *Чтобы включить отправку статистики в Kaspersky Security Network, выполните следующие действия:*

  1. Откройте окно настройки приложения.
  2. В левой части окна выберите раздел **Обратная связь**.
  3. Установите флажок **Я согласен участвовать в Kaspersky Security Network**.

Помимо данных об угрозах, Kaspersky Internet Security собирает расширенную статистику: информацию о скачанных вами исполняемых файлах и подписанных приложений, а также о приложениях, запускаемых на вашем компьютере.

- *Чтобы включить отправку расширенной статистики, выполните следующие действия:*

  1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Обратная связь**.

3. Установите флажок **Я согласен отправлять расширенную статистику в рамках Kaspersky Security Network**.

Отправка собранной статистики производится в конце каждого обновления.

Сбор, обработка и хранение персональных данных пользователя не производится в рамках Kaspersky Security Network .

ВНЕШНИЙ ВИД ПРИЛОЖЕНИЯ

Вы можете изменять внешний вид Kaspersky Internet Security, создавая и используя различные графические элементы и цветовую палитру. Также предполагается возможность настройки использования активных элементов интерфейса, таких как значок приложения в области уведомлений панели задач Microsoft Windows и всплывающие сообщения.

См. также

АКТИВНЫЕ ЭЛЕМЕНТЫ ИНТЕРФЕЙСА

Чтобы настроить активные элементы интерфейса, такие как значок приложения в системной панели и всплывающие сообщения, вы можете использовать следующие возможности Kaspersky Internet Security:

Использовать полупрозрачность окон уведомлений.

Все операции приложения, требующие вашего немедленного уведомления или принятия решения, оформлены в виде всплывающих сообщений над значком приложения в системной панели. Окна сообщений полупрозрачны, чтобы не мешать вашей работе. При наведении на окно сообщения курсора мыши прозрачность исчезает.

Использовать анимацию значка при выполнении задач.

В зависимости от выполняемой приложением операции значок в системной панели меняется. Так, например, если выполняется проверка скрипта, на фоне значка появляется небольшая пиктограмма со скриптом, а при проверке почтового сообщения - пиктограмма письма. По умолчанию анимация значка приложения используется. В этом случае значок будет отражать только статус защиты вашего компьютера: если защита включена, значок - цветной, если защита приостановлена или выключена, значок становится серого цвета.

Уведомлять о новостях.

По умолчанию при получении новостей в системной панели появляется специальный значок, при нажатии на который открывается окно с текстом новости.

Показывать значок поверх экрана приветствия Microsoft Windows.

По умолчанию такой индикатор появляется в правом верхнем углу экрана в момент запуска Kaspersky Internet Security. Он информирует вас о том, что защита вашего компьютера от любого рода угроз включена.

Чтобы настроить активные элементы интерфейса, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Вид**.

3. В блоке **Значок в панели задач** установите или снимите соответствующие флажки.

ГРАФИЧЕСКАЯ ОБОЛОЧКА ПРИЛОЖЕНИЯ

Все используемые в интерфейсе Kaspersky Internet Security цвета, шрифты, пиктограммы, тексты могут быть изменены. Вы можете создавать собственные графические оболочки для приложения, можете локализовать ее на другой язык.

Чтобы использовать другую графическую оболочку, выполните следующие действия:

1. Откройте окно настройки приложения.

2. В левой части окна выберите раздел **Вид**.

3. В блоке **Папка с описанием графической оболочки** установите флажок **Использовать альтернативные графические оболочки**, чтобы подключить графическую оболочку. В поле ввода укажите каталог с параметрами графической оболочки. Для выбора каталога нажмите на кнопку **Обзор**.

ОТЧЕТЫ

Работа каждого компонента Kaspersky Internet Security и выполнение каждой задачи проверки на вирусы и обновления фиксируется в отчете.

При работе с отчетами вы можете:

- выбирать компонент / задачу (см. раздел «Выбор компонента или задачи для формирования отчета» на стр. 185), по которому вам необходимо просмотреть отчет о событиях;
- управлять группировкой данных (см. раздел «Управление группировкой информации в отчете» на стр. 186) и их представлением на экране (см. раздел «Представление данных на экране» на стр. 187);
- выбирать по какому типу событий (см. раздел «Выбор типа событий» на стр. 186) необходимо сформировать отчет;
- выбирать в каком виде будет отображаться статистическая информация на экране - табличном или графическом (см. раздел «Табличное или графическое представление статистики» на стр. 188);
- сохранять отчет в файл (см. раздел «Сохранение отчета в файл» на стр. 189);
- задавать сложные условия фильтрации (см. раздел «Использование сложной фильтрации» на стр. 189);
- организовывать поиск событий (на стр. 190), произошедших в системе и обработанных приложением.

В ЭТОМ РАЗДЕЛЕ

ВЫБОР КОМПОНЕНТА ИЛИ ЗАДАЧИ ДЛЯ ФОРМИРОВАНИЯ ОТЧЕТА

Вы можете получить информацию о событиях, произошедших в работе каждого компонента Kaspersky Internet Security или в ходе выполнения задач (например, Файловый Антивирус, обновление и т. п.).

Отчет формируется для функции приложения (**Защита**, **Контроль приложений**, **Антивирус** и т. п.) или задачи (проверка и обновление). Отчет для функции содержит в себе отчет по компонентам, которые в этой функции содержатся. Таким образом, если вам необходим отчет о работе Файлового Антивируса, вам следует сформировать отчет для функции приложения **Антивирус**.

Чтобы получить отчет по какому-либо компоненту или задаче, выполните следующие действия:

1. Откройте главное окно приложения.
2. В левой части окна выберите функцию приложения (в состав которой входит нужный компонент) или задачу (проверка или обновление).
3. Нажмите на кнопку **Отчеты**.
4. В открывшемся окне будет сформирован отчет для выбранной функции приложения или задачи.

УПРАВЛЕНИЕ ГРУППИРОВКОЙ ИНФОРМАЦИИ В ОТЧЕТЕ

Вы можете управлять группировкой данных, представленных в отчете. Информация может быть сгруппирована по различным признакам. Набор признаков для каждой функции приложения неодинаков. Возможны следующие варианты:

- **Без группировки** - будут отображены все события.
- **Группировка по задаче** - данные будут сгруппированы по задачам, которые выполнялись компонентами Kaspersky Internet Security.
- **Группировка по приложению** - данные будут сгруппированы по приложениям, проявившим активность в системе и обработанным Kaspersky Internet Security.
- **Группировка по результату проверки** - данные будут сгруппированы исходя из результата проверки или обработки объекта.

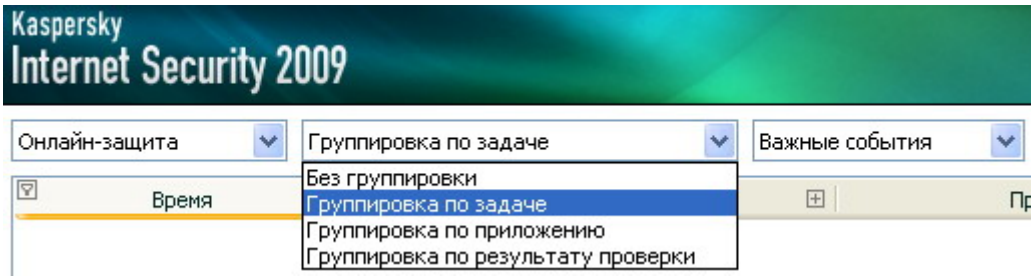

Рисунок 24: Признаки группировки информации в отчете

Для быстрого получения необходимой информации и сокращения размеров группировки предусмотрен поиск (см. раздел «Поиск событий» на стр. 190) по ключевому слову или задайте критерий поиска.

Чтобы воспользоваться группировкой по какому-либо признаку, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне выберите в раскрывающемся меню признак группировки.

ВЫБОР ТИПА СОБЫТИЙ

Полный список всех важных событий в работе компонента защиты или при выполнении задачи проверки либо обновления баз приложения фиксируется в отчете. Вы можете выбрать тип событий, которые будут отображаться в отчете.

События могут быть следующих типов:

- **Критические события** - события критической важности, указывающие на проблемы в работе Kaspersky Internet Security или на уязвимости в защите вашего компьютера. Например, обнаружен вирус, сбой в работе.

- **Важные события** - события, на которые обязательно нужно обратить внимание, поскольку они отображают важные ситуации в работе приложения. Например, прервано.

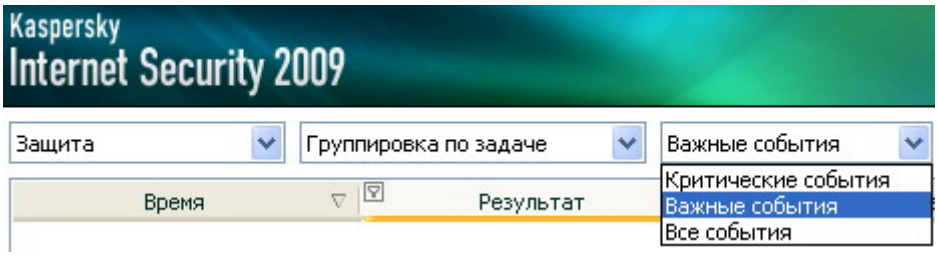

Рисунок 25: Выбор типа событий

При выборе пункта **Все события**, в отчете будут отображаться все события, если в разделе **Отчеты** в блоке **События** установлены флажки (см. раздел «Добавление в отчет записей о событиях» на стр. 182), позволяющие выводить в отчет записи о некритических событиях, а также событиях файловой системы и реестра. Если эти флажки не установлены, рядом с раскрывающимся списком выбора типов событий отображается знак предупреждения и ссылка **Отключено**. Воспользуйтесь этой ссылкой, чтобы перейти в окно настройки отчетов и установить соответствующие флажки.

Чтобы выбрать тип событий, по которым необходимо сформировать отчет, выполните следующие действия:

1. Откройте главное окно приложения.

2. Нажмите на кнопку **Отчеты**.

3. В открывшемся окне выберите в раскрывающемся меню тип событий. Если необходимо сформировать отчет по всем событиям, выберите значение **Все события**.

Представление данных на экране

События, попавшие в отчет, представлены в табличном виде. Вы можете создать выборку информации путем задания ограничивающего условия. Для этого щелкните левой клавишей мыши слева от заголовка того столбца таблицы, по которому вы хотите ввести ограничение. В раскрывающемся списке представлены ограничения, например, **Вчера -** для столбца **Время**, **Почтовое сообщение -** для столбца **Объект** и т. п. Выберите нужное. Выборка данных будет проведена с учетом заданного ограничения. При необходимости просмотра всех данных выберите в списке ограничений пункт **Все**.

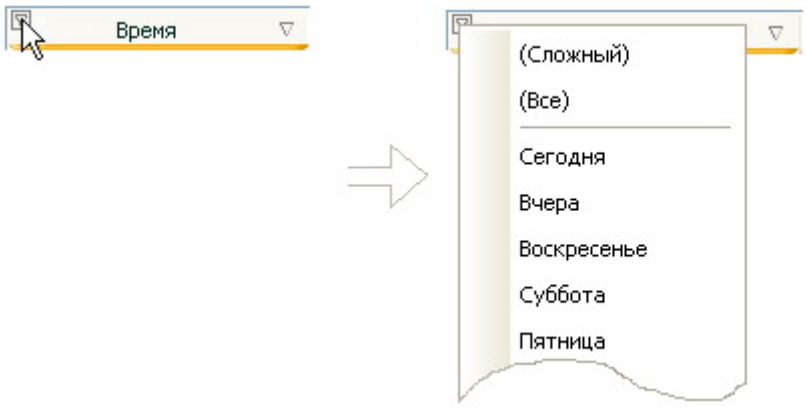

Рисунок 26: Задание ограничивающего условия

Также вы можете задать параметры сложного поиска в виде интервала, в пределах которого необходимо произвести выборку данных о произошедших событиях. Для этого в раскрывающемся списке ограничений выберите пункт **Сложный**. В открывшемся окне задайте нужный интервал (см. раздел «Использование сложной фильтрации» на стр. 189).

Для удобства и просторы работы с закладкой предусмотрено контекстное меню, с помощью которого можно осуществить быстрый доступ к любому признаку, позволяющему проводить группировку и выборку событий.

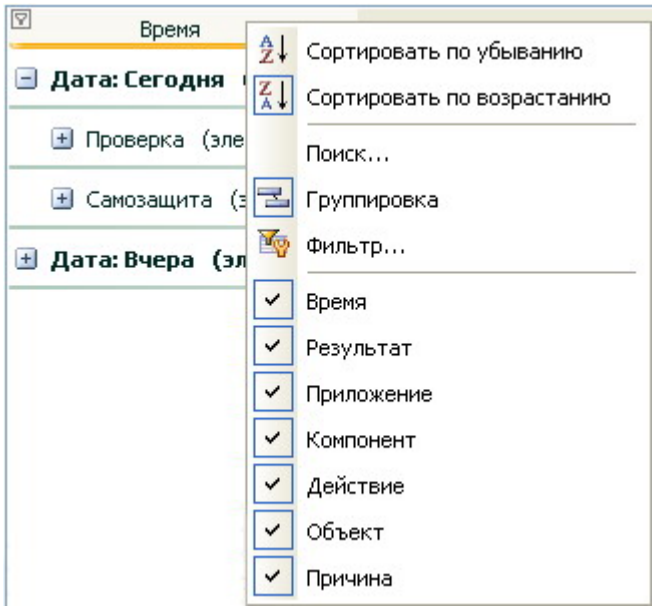

Рисунок 27: Контекстное меню

- *Чтобы задать ограничивающее условие, выполните следующие действия:*

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне щелкните левой клавишей мыши слева от заголовка того столбца таблицы, по которому вы хотите ввести ограничение. Выберите в раскрывающемся списке ограничение из представленных. При выборе пункта **Сложный**, вы сможете задать сложные условия фильтрации (см. раздел «Использование сложной фильтрации» на стр. 189).

- *Чтобы скрыть / показать столбцы таблицы, выполните следующие действия:*

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне щелкните правой клавишей мыши справа от заголовка любого столбца таблицы. Для того, чтобы скрыть какие-либо столбцы таблицы, снимите флажки рядом с соответствующими названиями в контекстном меню. Установите их для того, чтобы столбцы снова были видны.

ТАБЛИЧНОЕ ИЛИ ГРАФИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ СТАТИСТИКИ

В нижней части окна отчетов представлена статистика работы выбранной функции или задаче Kaspersky Internet Security. Вы можете просматривать статистику и выбирать формат ее представления - графический (для функций) или табличный. Выбор представления осуществляется с помощью кнопок  и  в верхней части

окна. Статистика отображается за текущий день и за весь период, в течение которого приложение работает на вашем компьютере.

Чтобы выбрать тип представления статистики, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне выберите функцию приложения, по которой вы хотите просмотреть статистику и воспользуйтесь кнопками и в верхней части окна.

Сохранение отчета в файл

Вы можете сохранить полученный отчет в файл.

Чтобы сохранить полученный отчет в файл, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне сформируйте необходимый отчет и нажмите на кнопку **Сохранить**.
4. В открывшемся окне выберите место на диске, куда следует сохранить файл отчета, и введите название файла.

Использование сложной фильтрации

Окно **Сложный фильтр** (см. рис. ниже) предназначено для задания сложных условий фильтрации данных. В окне вы можете задать интервалы поиска данных для любого столбца таблицы. Рассмотрим принципы работы в окне на примере столбца **Время**.

Выборка данных с помощью сложного фильтра основана на логических операциях конъюнкции (логическое И) и дизъюнкции (логическое ИЛИ), с помощью которых можно управлять выборкой данных.

В полях, расположенных в правой части окна, задаются границы выборки - в данном случае время. Для задания времени вы можете использовать клавиши стрелок на клавиатуре. В левой части - в раскрывающихся списках **Условие** - выбирается условие выборки событий, например, больше, то есть больше указанной границы в поле справа.

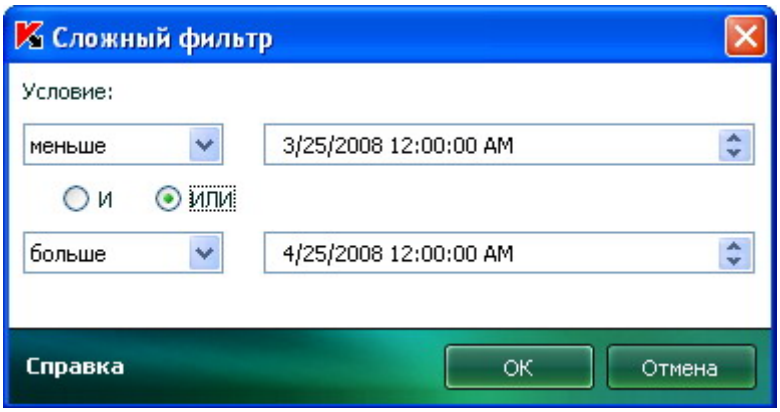

Рисунок 28: Задание сложных условий фильтрации

Если вы хотите, чтобы выборка данных удовлетворяла обоим заданным условиям, выберите **И**. Если достаточно хотя бы одного условия, выберите **ИЛИ**.

Для ряда столбцов границей интервала поиска является не числовое или временное значение, а слово (например, результат проверки **ОК** для графы **Результат**). В таком случае слово, заданное в качестве границы, сравнивается с другими словами-значениями для выбранного столбца по алфавиту.

Чтобы задать сложные условия фильтрации, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.
3. В открывшемся окне щелкните левой клавишей мыши слева от заголовка того столбца таблицы, по которому вы хотите задать сложные условия фильтрации. Выберите в раскрывшемся меню пункт **Сложный**. Также вы можете выбрать пункт **Фильтр** в контекстном меню (см. раздел «Представление данных на экране» на стр. 187), доступном при щелчке правой клавишей мыши по нужному столбцу таблицы.
4. В открывшемся окне **Сложный фильтр** задайте необходимые условия фильтрации.

Поиск событий

Данное окно (см. рис. ниже) предназначено для поиска событий, произошедших в системе и обработанных Kaspersky Internet Security.

Рассмотрим принципы работы в окне:

- Поле **Строка** предназначено для ввода ключевого слова (например, explorer). Чтобы начать поиск нажмите на кнопку **Искать дальше**. Поиск нужных данных может занять некоторое время. По окончании поиска вам будут представлены события, соответствующие заданному ключевому слову. Нажатие на кнопку **Отметить все** приведет к тому, что будут выделены все найденные данные, отвечающие заданному ключевому слову.
- Поле **Графа** позволяет выбрать столбец таблицы, по которому будет вестись поиск ключевого слова. Такой выбор приведет к уменьшению времени, затраченному на процесс поиска (если, конечно, не выбрано значение **Все**).

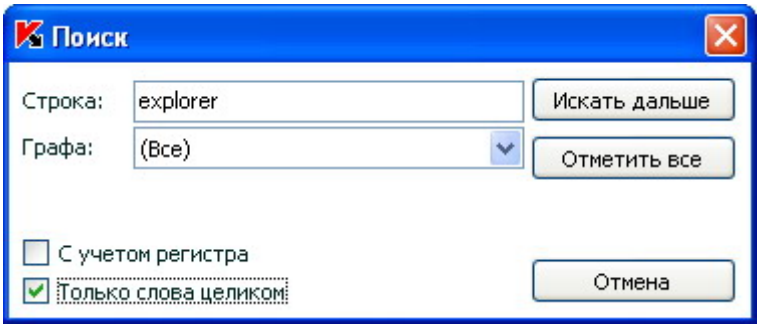

Рисунок 29: Поиск событий

Если вы хотите, чтобы поиск проводился с учетом регистра для ключевого слова, установите флажок **С учетом регистра**. Флажок **Только слова целиком** позволяет ограничить поиск и сделать его доступным только для целых слов из заданного ключевого слова.

Чтобы использовать поиск событий, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Отчеты**.

3. В открывшемся окне щелкните правой клавишей мыши справа от заголовка любого столбца таблицы. В раскрывшемся меню выберите пункт **Поиск**.

4. В открывшемся окне **Поиск** задайте критерии поиска.

СТАТИСТИКА РАБОТЫ ПРИЛОЖЕНИЯ

Работа компонентов Kaspersky Internet Security или задач проверки на вирусы фиксируется в разделе статистики. Здесь вы можете узнать сколько было найдено опасных и подозрительных объектов в результате работы приложения, какие из них были вылечены, удалены или помещены на карантин.

О том, что приложением были найдены вредоносные объекты, сигнализирует статус защиты компьютера (см. раздел «Главное окно Kaspersky Internet Security» на стр. 36) окна **Обнаружено** посредством изменения цвета значка статуса защиты и панели, на которой он расположен. При обнаружении вредоносных объектов цвет значка и панели становится красным. Следует немедленно устранить все возникшие угрозы.

Рисунок 30: Обнаружены опасные объекты

В ЭТОМ РАЗДЕЛЕ

ЗАКЛАДКА «СТАТУС»

На закладке **Статус** представлен список проблем, возникших в защите вашего компьютера. Также на закладке приведено их описание и возможные пути решения. Проблемы расположены исходя из важности их решения: сначала наиболее важные, затем менее важные и последними - информационные сообщения. Для каждой проблемы дается ее подробное описание и предлагаются следующие варианты действий:

- **Немедленно устранить**. Данное действие является рекомендуемым.
- **Отложить устранение**.

Чтобы устранить проблемы, возникшие в защите компьютера, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Обнаружено**.
3. В открывшемся окне на закладке **Статус** выполните необходимые действия. Чтобы ранее скрытые сообщения были вновь отображены в общем списке, установите флажок **Показать скрытые сообщения**.

СМ. ТАКЖЕ

Закладка «Обнаруженные угрозы»

На закладке **Обнаруженные угрозы** представлен список найденных опасных объектов и отражены действия Kaspersky Internet Security над ними. Объекты сгруппированы согласно принятой классификации (см. раздел «Угрозы компьютерной безопасности» на стр. 17) угроз компьютерной безопасности.

Для каждого объекта указывается его полное имя и статус, присвоенный приложением при его проверке / обработке.

На закладке вы можете просмотреть объекты, используя следующие признаки группировки:

- **Активные**. Опасные объекты, обнаруженные приложением, в отношении которых не было предпринято никаких действий. Такие объекты представляют угрозу безопасности для вашего компьютера. Рекомендуется предпринять действия по устранению угроз.

- **Карантин**. Объекты, помещенные пользователем на карантин с целью их дальнейшего лечения. Чтобы поместить зараженный объект на карантин, воспользуйтесь ссылкой **Поместить на карантин**.

- **Вылеченные**. Объекты, которые были успешно вылечены Kaspersky Internet Security.

Чтобы просмотреть все объекты, выберите признак **Все**.

Чтобы выполнить действие над найденным объектом, выполните следующие действия:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Обнаружено**.
3. В открывшемся окне в списке объектов выберите нужный и щелкните по нему правой клавишей мыши.
4. В раскрывшемся контекстном меню выберите необходимое действие.

Закладка «Статистика»

На данной закладке фиксируется статистика работы компонентов защиты: **Антивирус**, **Онлайн-защита** и **Фильтр содержимого**. Здесь вы можете узнать сколько опасных и подозрительных объектов (см. раздел «Угрозы компьютерной безопасности» на стр. 17) было обнаружено приложением с момента его установки на компьютер.

Уведомления

При возникновении событий в процессе работы Kaspersky Internet Security на экран выводятся специальные уведомления. В зависимости от степени важности события, с точки зрения безопасности компьютера, уведомления могут быть следующих типов:

- **Тревога**. Произошло событие критической важности, например, обнаружен вредоносный объект или опасная активность в системе. Необходимо немедленно принять решение о дальнейших действиях. Окно уведомления такого типа имеет красный цвет.

- **Внимание**. Произошло потенциально опасное событие, например, обнаружен возможно зараженный объект или подозрительная активность в системе. Необходимо принять решение, насколько данное событие опасно на ваш взгляд. Окно уведомления такого типа имеет желтый цвет.

- **Информация**. Уведомление информирует о событии, не имеющем первостепенной важности. Окно уведомления такого типа имеет зеленый цвет.

Окно уведомления состоит из четырех частей:

- *Заголовок окна*. В заголовке окна уведомления отображается краткое описание события, например: запрос прав, подозрительная активность, новая сеть, тревога, вирус.

- *Описание события*. В блоке описания события отображается подробная информация о причине возникновения уведомления: название вызвавшего событие приложения, имя обнаруженной угрозы, параметры обнаруженного сетевого соединения и другие.

- *Область выбора действия*. В этом блоке вам предлагается выбрать одно из возможных для данного события действий. Предложенные варианты действий зависят от типа события, например: **Лечить**, **Удалить**, **Пропустить** - в случае обнаружения вируса, **Разрешить**, **Запретить** - в случае запроса прав приложения на выполнения потенциально опасных действий. Действие, рекомендуемое специалистами «Лаборатории Касперского» выделено жирным шрифтом.

  При выборе действия **Разрешить** или **Запретить**, открывается окно, где вы можете выбрать *режим применения действия*. Для действия **Разрешать** вы можете выбрать один из следующих режимов:

  - **Разрешать всегда**. Выберите этот вариант, чтобы разрешать обнаруженную активность программы путем внесения изменений в правило доступа программы к ресурсам системы.

  - **Разрешить сейчас**. Выберите этот вариант, чтобы применять выбранное действие ко всем аналогичным событиям, обнаруженным в течение сессии работы приложения. Сессией работы приложения считается время работы от момента его запуска до момента выключения либо перезапуска приложения.

  - **Сделать доверенным**. Выберите этот вариант, чтобы переместить приложение в группу **Доверенные**.

  Для действия **Запрещать** вы можете выбрать один из следующих режимов:

  - **Запрещать всегда**. Выберите этот вариант, чтобы запрещать обнаруженную активность программы путем внесения изменений в правило доступа программы к ресурсам системы.

  - **Запретить сейчас**. Выберите этот вариант, чтобы применять выбранное действие ко всем аналогичным событиям, обнаруженным в течение сессии работы приложения. Сессией работы приложения считается время работы от момента его запуска до момента выключения либо перезапуска приложения.

  - **Завершить**. Выберите этот вариант, чтобы прервать работу программы.

- *Область выбора дополнительного действия*. В этом блоке вы можете выбрать дополнительное действие:

  - **Добавить к исключениям**. Если вы уверены, что обнаруженный объект не является опасным, рекомендуется, во избежание повторных срабатываний приложения при работе с этим объектом, добавить его в доверенную зону (см. раздел «Угрозы и исключения» на стр. 172).

  - **Применить ко всем объектам**. Установите этот флажок, чтобы заданное действие применялось ко всем объектам с тем же статусом в аналогичных ситуациях.

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ ПРИЛОЖЕНИЯ

После установки и настройки приложения вы можете проверить с помощью тестового «вируса» и его модификаций, правильно ли выполнена настройка параметров. Проверку следует выполнять для каждого компонента защиты / протокола отдельно.

В ЭТОМ РАЗДЕЛЕ

Тестовый «вирус» EICAR и его модификации

Тестовый «вирус» был специально разработан организацией eicar (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.

Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!

Загрузить тестовый «вирус» можно с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Перед загрузкой необходимо отключить антивирусную защиту, поскольку файл *anti_virus_test_file.htm* будет идентифицирован и обработан приложением как зараженный объект, перемещаемый по HTTP-протоколу.

Не забудьте включить антивирусную защиту сразу после загрузки тестового «вируса».

Приложение идентифицирует файл, загруженный с сайта компании **EICAR** как зараженный объект, содержащий **неподверженный лечению** вирус, и выполняет действие, установленное для такого объекта.

Вы также можете использовать модификации стандартного тестового «вируса» для проверки работы приложения. Для этого следует изменить содержание стандартного «вируса», добавив к нему один из префиксов (см. таблицу далее). Для создания модификаций тестового «вируса» может использоваться любой текстовый или гипертекстовый редактор, например, **Microsoft Блокнот**, **UltraEdit32**, и т.д.

Вы можете проверять корректность работы антивирусного приложения с помощью модифицированного «вируса» EICAR только при наличии антивирусных баз, датированных не ранее 24.10.2003 (кумулятивное обновление – Октябрь, 2003).

В первой графе приведены префиксы, которые следует добавить в начало строки стандартного тестового «вируса». Во второй графе перечислены все возможные значения статуса, присваиваемого Антивирусом объекту по результатам проверки. Третья графа содержит информацию об обработке приложением объектов с указанным статусом. Обращаем ваше внимание, что действия над объектами определяются значениями параметров приложения.

После добавления префикса к тестовому «вирусу» сохраните полученный файл, например, под именем: *eicar_dele.com*. Дайте аналогичные названия всем модифицированным «вирусам».

Таблица 6. Модификации тестового «вируса»

Префикс	Статус объекта	Информация об обработке объекта
Префикс отсутствует, стандартный тестовый «вирус».	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Приложение идентифицирует данный объект как вирус, неподверженный лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR–	**Поврежденный**.	Приложение получило доступ к объекту, но не смогло проверить его, поскольку объект поврежден (например, нарушена структура объекта, неверный формат файла). Информацию о том, что объект был обработан, вы можете найти в отчете о работе приложения.
WARN–	**Подозрительный**. Объект содержит код неизвестного вируса. Лечение невозможно.	Объект признан подозрительным с использованием эвристического анализатора. На момент обнаружения базы Антивируса не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
SUSP–	**Подозрительный**. Объект содержит модифицированный код известного вируса. Лечение невозможно.	Приложение обнаружило частичное совпадение участка кода объекта с участком кода известного вируса. На момент обнаружения базы Антивируса не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
ERRO–	**Ошибка проверки**.	При проверке объекта возникла ошибка. Приложение не смогло получить доступ к объекту: нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе). Информацию о том, что объект был обработан, вы можете найти в отчете о работе приложения.
CURE–	**Зараженный**. Объект содержит код известного вируса. Излечим.	Объект содержит вирус, который может быть вылечен. Приложение выполняет лечение объекта, при этом текст тела «вируса» изменяется на CURE. Вы получите уведомление при обнаружении такого объекта.
DELE–	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Приложение идентифицирует данный объект как вирус, неподверженный лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов. Вы получите уведомление при обнаружении такого объекта.

ТЕСТИРОВАНИЕ ЗАЩИТЫ HTTP-ТРАФИКА

- *Чтобы проверить обнаружение вирусов в потоке данных, передаваемых по HTTP-протоколу, выполните следующие действия:*

  попытайтесь загрузить тестовый «вирус» с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

При попытке загрузить тестовый «вирус» приложение обнаружит объект, идентифицирует как зараженный неизлечимый и выполнит действие, установленное в параметрах проверки HTTP-трафика для такого объекта. По

умолчанию, при попытке загрузить тестовый «вирус» соединение с ресурсом будет разорвано, и в окне браузера будет выведено сообщение о том, что данный объект заражен вирусом EICAR-Test-File.

Тестирование защиты SMTP-трафика

Для проверки обнаружения вирусов в потоке данных, передаваемых по SMTP-протоколу, вы можете использовать почтовую систему, передача данных в которой осуществляется по этому протоколу.

Рекомендуется проверить работу Антивируса для исходящей почты, как в теле сообщения, так и во вложении. Для проверки обнаружения вирусов в теле сообщения, поместите текст стандартного тестового или модифицированного «вируса» в тело сообщения.

Для этого:

1. Создайте письмо в формате **Обычный текст** с помощью установленного на компьютере почтового клиента.

   Письмо, содержащее тестовый вирус и сформированное в формате RTF и HTML, проверено не будет!

2. Поместите текст стандартного или модифицированного «вируса» в начало письма или присоедините к письму файл, содержащий тестовый «вирус».

3. Отправьте письмо на адрес администратора.

Приложение обнаружит объект, идентифицирует его как зараженный, заблокирует отправку письма.

Проверка корректности настройки Файлового Антивируса

Чтобы проверить, насколько корректно настроен Файловый Антивирус, выполните следующие действия:

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), а также созданные вами модификации тестового «вируса».

2. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.

3. Запустите файл тестового «вируса» или его модификацию на выполнение.

Файловый Антивирус перехватит обращение к файлу, проверит его и выполнит действие, заданное в параметрах. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результате работы Файлового Антивируса можно посмотреть в отчете о работе компонента.

Проверка корректности настройки задачи поиска вирусов

Чтобы проверить, насколько корректно настроена задача поиска вирусов, выполните следующие действия:

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), а также созданные вами модификации тестового «вируса».

2. Создайте новую задачу поиска вирусов и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов».

3. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.

4. Запустите задачу поиска вирусов на выполнение.

При проверке по мере обнаружения подозрительных или зараженных объектов будут выполняться действия, заданные в параметрах задачи. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результат выполнения задачи поиска вирусов можно посмотреть в отчете по работе компонента.

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ ЗАЩИТЫ ОТ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ

Для проверки защиты от нежелательной почты вы можете использовать тестовое сообщение, которое идентифицируется приложением как спам.

Тестовое сообщение должно содержать в теме письма строку:

```
Spam is bad do not send it
```

После поступления данного сообщения на компьютер приложение проверит его, присвоит сообщению статус спама и выполнит над ним действие, установленное для объекта данного типа.

РАБОТА С ПРИЛОЖЕНИЕМ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Kaspersky Internet Security посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- запуск, остановка, приостановка и возобновление работы компонентов приложения;
- запуск, остановка, приостановка и возобновления выполнения задач проверки на вирусы;
- получение информации о текущем статусе компонентов и задач и их статистики;
- проверка выбранных объектов;
- обновление баз и модулей приложения;
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Обращение к приложению через командную строку должно осуществляться из каталога установки продукта либо с указанием полного пути к avp.com.

В качестве **<команд>** используются:

ACTIVATE	активация Kaspersky Internet Security через интернет с помощью кода активации
ADDKEY	активация приложения с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
START	запуск компонента или задачи
PAUSE	приостановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
RESUME	возобновление работы 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 по работе компонента или задачи
HELP	помощь по синтаксису команды, вывод списка команд
SCAN	проверка объектов на присутствие вирусов
UPDATE	запуск обновления приложения
ROLLBACK	откат последнего произведенного обновления Kaspersky Internet Security (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXIT	завершение работы с приложением (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
IMPORT	импорт параметров защиты Kaspersky Internet Security (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXPORT	экспорт параметров защиты приложения

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента приложения.

В этом разделе

Активация приложения

Активацию Kaspersky Internet Security возможно произвести двумя способами:

- через интернет с помощью кода активации (команда ACTIVATE);
- с помощью файла ключа (команда ADDKEY).

Синтаксис команды:

```
ACTIVATE <код_активации>
ADDKEY <имя_файла> /password=<ваш_пароль>
```

Описание параметров:

<код активации>	код активации приложения, предоставленный при покупке
<имя_файла>	имя файла ключа к приложению с расширением **.key*
<ваш_пароль>	пароль к приложению, заданный в интерфейсе

Обратите внимание, что без ввода пароля команда **ADDKEY** выполняться не будет.

Пример:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<ваш_пароль>
```

УПРАВЛЕНИЕ КОМПОНЕНТАМИ И ЗАДАЧАМИ ПРИЛОЖЕНИЯ

Синтаксис команды:

```
avp.com <команда> <профайл|имя_задачи> [/R[A]:<файл_отчета>]
avp.com STOP|PAUSE <профайл|имя_задачи> /password=<ваш_пароль> [/R[A]:<файл_отчета>]
```

<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. PAUSE – приостановка работы компонента защиты или задачи. RESUME – возобновление 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 команды PAUSE и STOP выполняться не будут.
<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 приложением 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 приложению, 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 следующих значений:

Protection (RTP)	все компоненты защиты. Команда **avp.com START RTP** запускает все компоненты защиты, если защита была полностью отключена либо приостановлена на время. Также данная команда запускает любой из компонентов защиты, работа которого приостановлена из графического интерфейса

	приложения либо командой **PAUSE** командной строки. В случае если компонент был отключен из графического интерфейса приложения либо 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**.
SystemWatch (SW)	Контроль приложений
Firewall (FW)	Сетевой экран
HipsTask (HIPS)	Фильтрация активности
pdm	Проактивная защита
Antivirus (AV)	Антивирус
File_Monitoring (FM)	Файловый Антивирус
Mail_Monitoring (EM)	Почтовый Антивирус
Web_Monitoring (WM)	Веб-Антивирус Значения для подкомпонентов Веб-Антивируса: **httpscan (HTTP)** – проверка http-трафика; **sc** – проверка скриптов.
ContentFilter (CF)	Фильтр содержимого
AdBlocker (AB)	Анти-Баннер
Anti_Spam (AS)	Анти-Спам
ParCtl (PC)	Родительский контроль
OnlineSecurity (OS)	Онлайн-защита
antidial (AD)	Анти-Дозвон
antiphishing (AP)	Анти-Фишинг
ids	Защита от сетевых атак
Updater	Обновление
Rollback	Откат последнего обновления
Scan_Critical_Areas (CRITICAL)	Проверка критических областей
Scan_My_Computer	Проверка компьютера
Scan_Objects	Проверка объектов
Scan_Quarantine	Проверка карантина

Scan_Rootkits	Проверка на наличие руткитов (rootkit)
Scan_Startup (STARTUP)	Проверка объектов автозапуска
Scan_Vulnerabilities (SECURITY)	Анализ безопасности

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе продукта.

Примеры:

- *Для того чтобы включить Файловый Антивирус, в командной строке введите:*

```
avp.com START FM
```

- *Для возобновления работы Родительского контроля в командной строке введите:*

```
avp.com RESUME ParCtl
```

- *Для остановки задачи проверки компьютера в командной строке введите:*

```
avp.com STOP Scan_My_Computer /password=<ваш_пароль>
```

ПРОВЕРКА НА ВИРУСЫ

Командная строка запуска проверки некоторой области на присутствие вирусов и 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 приложении задачами, запустив нужную из командной строки. При этом задача будет выполнена с параметрами, установленными в интерфейсе Kaspersky Internet Security.

Описание параметров:

<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/или каталогам 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 файлы, содержащиеся в нем.
/MEMORY	объекты оперативной памяти
/STARTUP	объекты автозапуска
/MAIL	почтовые ящики

/REMDRIVES	все съемные диски
/FIXDRIVERS	все локальные диски
/NETDRIVERS	все сетевые диски
/QUARANTINE	объекты на карантине
/ALL	полная проверка компьютера
/@:<filelist.lst>	путь к файлу со списком объектов и каталогов, включаемых в проверку. Файл должен иметь текстовый формат; каждый объект проверки необходимо указывать с новой строки. Допускается ввод абсолютного или относительного пути к файлу. Путь указывается без кавычек, даже если в нем содержится символ «пробел».
<действие> - параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i8.**	
/i0	не совершать над объектом никаких действий, только 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 ящики
-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 МБ) превышает значение, заданное параметром **<size>**
<конфигурационный файл> - определяет путь к конфигурационному файлу, содержащему параметры работы приложения 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 приложения.	
/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»
```

- *Приостановить проверку выбранных объектов, запустить полную проверку компьютера, по окончании которой продолжить поиск вирусов среди выбранных объектов:*

```
avp.com PAUSE Scan_Objects /password=<ваш_пароль>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_setting.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 ПРИЛОЖЕНИЯ

Команда для обновления модулей Kaspersky Internet Security и баз приложения имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>] [/R[A]:<файл_отчета>] [/C:<имя_файла>]
[/APP=<on|off>]
```

Описание параметров:

<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 приложения.
/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 приложения. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения параметров, установленные в интерфейсе приложения.
/APP=<on|off>	включить/ отключить обновление модулей приложения

Примеры:

- *Обновить базы приложения, зафиксировав все события в отчете:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Обновить модули приложения, используя параметры конфигурационного файла updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Пример конфигурационного файла:

```
«ftp://my_server/kav updates» /RA:avbases_upd.txt /app=on
```

ОТКАТ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ

Синтаксис команды:

```
ROLLBACK [/R[A]:<файл_отчета>][/password=<ваш_пароль>]
```

Описание параметров:

/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 приложению, заданный в интерфейсе

Обратите внимание, что без ввода пароля данная 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:

<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 приложения и задачами (см. раздел “Управление компонентами и задачами приложения” на стр. 202)».
<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 приложения 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 c:\settings.dat
```

ИМПОРТ ПАРАМЕТРОВ ЗАЩИТЫ

Синтаксис команды:

```
avp.com IMPORT <имя_файла> [/password=<ваш_пароль>]
```

<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 приложения. Импорт параметров защиты возможен только из файла в бинарном формате.

Обратите внимание, что без ввода пароля данная команда выполняться не будет.

Пример:

```
avp.com IMPORT c:\settings.dat /password=<ваш_пароль>
```

ЗАПУСК ПРИЛОЖЕНИЯ

Синтаксис команды:

```
avp.com
```

ОСТАНОВКА ПРИЛОЖЕНИЯ

Синтаксис команды:

```
EXIT /password=<ваш_пароль>
```

<ваш_пароль>	пароль к приложению, заданный в интерфейсе

Обратите внимание, что без ввода пароля данная команда выполняться не будет.

ПОЛУЧЕНИЕ ФАЙЛА ТРАССИРОВКИ

Создание файла трассировки может потребоваться при наличии проблем в работе Kaspersky Internet Security для более точной их диагностики специалистами Службы технической поддержки.

Синтаксис команды:

```
avp.com TRACE [file] [on|off] [<уровень_трассировки>]
```

Описание параметров:

[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 он не был указан, то рекомендуется устанавливать уровень 500.

Рекомендуется включать создание файлов трассировки только для диагностики конкретной проблемы. Постоянное включение трассировки может привести к потере производительности работы компьютера и переполнению жесткого диска.

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 справки по синтаксису командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Для получения справки по синтаксису конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

КОДЫ ВОЗВРАТА КОМАНДНОЙ СТРОКИ

В данном разделе приведено описание кодов возврата командной строки. 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 ПОИСКА ВИРУСОВ	
101	Все опасные объекты обработаны
102	Обнаружены опасные объекты

УСТРАНЕНИЕ ПРОБЛЕМ

Если при использовании Kaspersky Internet Security возникли проблемы, прежде всего убедитесь, не описан ли метод решения вашей проблемы в справочной системе или в Базе знаний «Лаборатории Касперского» (http://support.kaspersky.ru). *База знаний* является отдельным разделом веб-сайта Службы технической поддержки и содержит рекомендации по работе с продуктами «Лаборатории Касперского», ответы на часто задаваемые вопросы. Попробуйте найти ответ на ваш вопрос или решение вашей проблемы на этом ресурсе.

- *Чтобы обратиться к Базе знаний, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В нижней части окна нажмите на ссылку **Поддержка**.
  3. В открывшемся окне **Поддержка** нажмите на ссылку **Служба технической поддержки**.

Еще один ресурс, где вы можете получить информацию по работе с приложением, - это Форум пользователей продуктов «Лаборатории Касперского». Данный ресурс также является отдельным разделом веб-сайта Службы технической поддержки и содержит вопросы, отзывы и пожелания пользователей приложения. Вы можете ознакомиться с основными темами форума, оставить отзыв о приложении или отыскать ответ на свой вопрос.

- *Чтобы открыть форум пользователей, выполните следующие действия:*

  1. Откройте главное окно приложения.
  2. В нижней части окна нажмите на ссылку **Поддержка**.
  3. В открывшемся окне **Поддержка** нажмите на ссылку **Форум пользователей**.

Если вы не нашли решения вашей проблемы в справке, Базе знаний или на Форуме пользователей, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 10).

В ЭТОМ РАЗДЕЛЕ

Создание отчета о состоянии системы

При решении ваших проблем специалистам Службы поддержки «Лаборатории Касперского» может понадобиться отчет о состоянии системы. Этот отчет содержит подробную информацию о запущенных процессах, загружаемых модулях и драйверах, модулях расширения Microsoft Internet Explorer и Проводника Microsoft Windows, открытых портах, обнаруженных подозрительных объектах и проч.

В процессе создания отчета о состоянии системы не производится сбор персональных данных пользователя.

Чтобы создать отчет о состоянии системы, выполните следующие действия:

1. Откройте главное окно приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** нажмите на ссылку **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 приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** нажмите на кнопку **Открыть папку**.
5. Откройте архив *sysinfo.zip*, содержащий файлы отчета.

См. также

Создание файла трассировки 212

Отправка файлов данных 213

Создание файла трассировки

После установки Kaspersky Internet Security могут возникнуть сбои в работе операционной системы или отдельных программ. В этом случае, скорее всего, имеет место конфликт приложения с программным обеспечением, установленным на вашем компьютере, или с драйверами комплектующих вашего компьютера. Для успешного решения вашей проблемы специалисты Службы поддержки «Лаборатории Касперского» могут попросить вас создать файл трассировки.

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** воспользуйтесь раскрывающимся списком в блоке **Трассировка**, чтобы выбрать уровень трассировки. Уровень трассировки задается специалистом Службы поддержки. При отсутствии указаний Службы поддержки рекомендуется устанавливать уровень трассировки **500**.
5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.
6. Воспроизведите ситуацию, в которой возникает ваша проблема.
7. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

Вы можете перейти к загрузке результатов трассировки (см. раздел «Отправка файлов данных» на стр. 213) на сервер «Лаборатории Касперского».

См. также

Отправка файлов данных

После создания файлов трассировки и отчета о состоянии системы их необходимо отправить специалистам Службы поддержки «Лаборатории Касперского».

Для того чтобы загрузить файлы данных на сервер Службы поддержки, вам понадобится номер запроса. Этот номер доступен в вашем Персональном кабинете на сайте Службы поддержки при наличии активного запроса.

Чтобы загрузить файлы данных на сервер Службы поддержки, выполните следующие действия:

1. Откройте главное окно приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** в блоке **Действия** нажмите на ссылку **Загрузить информацию для поддержки на сервер**.
5. В открывшемся окне установите флажки рядом с теми файлами, которые вы хотите отправить в Службу поддержки, и нажмите на кнопку **Загрузить**.
6. В открывшемся окне **Ввод номера запроса** укажите номер, присвоенный вашему запросу при заполнении электронной формы на сайте Службы поддержки.

Выбранные файлы данных будут упакованы и отправлены на сервер Службы поддержки.

При отсутствии возможности связаться со Службой поддержки вы можете сохранить файлы данных на вашем компьютере.

Чтобы сохранить файлы данных на диск, выполните следующие действия:

1. Откройте главное окно приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки**.
4. В открывшемся окне **Информация для поддержки** в блоке **Действия** нажмите на ссылку **Загрузить информацию для поддержки на сервер**.
5. В открывшемся окне установите флажки рядом с теми файлами, которые вы хотите отправить в Службу поддержки, и нажмите на кнопку **Загрузить**.
6. В открывшемся окне **Ввод номера запроса** нажмите на кнопку **Нет** и в открывшемся окне подтвердите сохранение файлов на диск.
7. В открывшемся окне задайте имя архива.

Впоследствии вы можете отправить сохраненные файлы в Службу поддержки с помощью Персонального кабинета (https://support.kaspersky.com/ru/PersonalCabinet).

См. также

Создание файла трассировки 212

Создание отчета о состоянии системы 211

Выполнение скрипта AVZ

Специалисты «Лаборатории Касперского» анализируют вашу проблему на основе файлов трассировки и отчета о состоянии системы. Результатом анализа является последовательность действий, направленных на устранение обнаруженных проблем. Зачастую этих действий может оказаться очень много.

Для упрощения процедуры устранения проблем используются скрипты AVZ. Скрипт AVZ представляет собой набор инструкций, позволяющих: редактировать ключи реестра, помещать на карантин файлы, производить поиск классов с возможностью карантина связанных с ними файлов, выполнять блокирование перехватчиков UserMode и KernelMode и проч.

Для запуска скриптов в состав приложения включен мастер *Выполнения скриптов AVZ*. Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопки **Назад** и ссылки **Далее**, а завершение работы мастера при помощи ссылки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Не рекомендуется вносить изменения в текст скрипта, присланного вам специалистами «Лаборатории Касперского». В случае возникновения проблем в ходе выполнения скрипта обращайтесь в Службу поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 10).

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно приложения.
2. В нижней части окна приложения нажмите на ссылку **Поддержка**.
3. В открывшемся окне **Поддержка** нажмите на ссылку **Трассировки** в нижней части окна.
4. В открывшемся окне **Информация для поддержки** нажмите на ссылку **Выполнить скрипт AVZ**.

В случае успешного выполнения скрипта работа мастера завершается. Если во время выполнения скрипта возникает сбой, мастер выводит соответствующее сообщение.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ KASPERSKY SECURITY NETWORK

В настоящем Положении изложен порядок сбора и использования информации, указанной в приведенном ниже перечне.

Настоящее Положение относится к продуктам Антивирус Касперского, Kaspersky Internet Security, правообладателем которых является ЗАО «Лаборатория Касперского».

В целях выявления новых угроз информационной безопасности и их источников, а также повышения уровня защиты информации пользователей, обрабатываемой с помощью ЭВМ, совершенствования функционала продуктов, разрабатываемых ЗАО «Лаборатория Касперского», после включения Пользователем функции сбора информации в разделе **Обратная связь** окна настройки (см. раздел «Обратная связь» на стр. 182) соответствующего продукта Kaspersky Security Network будет осуществлять сбор основной и расширенной информации в соответствии с указанным далее перечнем.

Перечень основной информации:

- Информация об установленном на компьютере аппаратном и программном обеспечении, в том числе версия операционной системы и установленные пакеты обновлений, объекты ядра, драйверы, сервисы, расширения Microsoft Internet Explorer, расширения системы печати, расширения Windows Explorer, загруженные объекты, элементы Active Setup, апплеты, панели управления, записи файла hosts и системного реестра, IP-адреса, версии браузеров и почтовых клиентов, а также номер версии продукта «Лаборатории Касперского».

- Уникальный идентификатор, присваиваемый продуктом «Лаборатории Касперского» компьютеру пользователя.

- Информация о состоянии антивирусной защиты компьютера, а также данные обо всех потенциально вредоносных файлах и действиях (в том числе название вируса, дата и время обнаружения, названия и размер зараженных файлов и пути к ним, IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, название потенциально вредоносного приложения).

Перечень расширенной информации:

- Информация о загружаемых пользователем подписанных приложений (URL-адрес, размер файла, имя подписи).

- Информация о запускаемых приложениях (размер, атрибуты, дата создания, информация заголовка PE, регион, имя, местоположение, упаковщик).

Сбор, обработка и хранение персональных данных пользователя не производится.

Предоставление вышеуказанной информации является добровольным. Функцию сбора информации можно в любой момент включить или выключить в разделе **Обратная связь** окна настройки (см. раздел «Обратная связь» на стр. 182) соответствующего продукта «Лаборатории Касперского».

ООО «КРИПТОЭКС»

Для формирования и проверки электронной цифровой подписи в Антивирусе Касперского используется программная библиотека защиты информации (ПБЗИ) «Крипто-Си», разработанная ООО «КриптоЭкс».

ООО «КриптоЭкс» имеет лицензии ФАПСИ (ФСБ) на разработку, производство и распространение шифровальных средств комплексов, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну.

ПБЗИ «Крипто-Си» предназначена для использования в системах комплексной защиты конфиденциальной информации по классу КС1 и имеет сертификат соответствия ФСБ № СФ/114-0901 от 01 июля 2006 года.

Модули библиотеки реализуют шифрование и расшифровку блока данных фиксированной размерности и (или) потока данных в соответствии с криптографическим алгоритмом (ГОСТ 28147-89), генерацию и проверку электронной цифровой подписи в соответствии с алгоритмами (ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001), хэш-функцию (ГОСТ Р 34.11-94), генерацию ключевой информации с использованием программного датчика псевдослучайных чисел. Реализована также схема распределения ключевой информации и выработка имитовекторов (ГОСТ 28147-89).

Модули библиотеки реализованы на языке программирования «Си» (в соответствии со стандартом ANSI «C») и могут быть интегрированы в приложения в виде статически и динамически подгружаемого кода и поддерживают возможность исполнения на платформах x86, x86-64, Ultra SPARC II и совместимых с ними.

Модули библиотеки переносимы под операционные среды: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris для Ultra SPARC II).

Веб-сайт ООО «КриптоЭкс»: http://www.cryptoex.ru

Адрес электронной почты: info@cryptoex.ru

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ЗАО «Лаборатория Касперского» была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более четырехсот пятидесяти высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Телефон, факс:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 18:30 часов по московскому времени) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	Контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com
Антивирусная	newvirus@kaspersky.com

лаборатория:	(только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Общая информация:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

К

А

В

Г

Д

З

И

Л

М

Н

О

П

Р

С

Т

У

Ф

Э