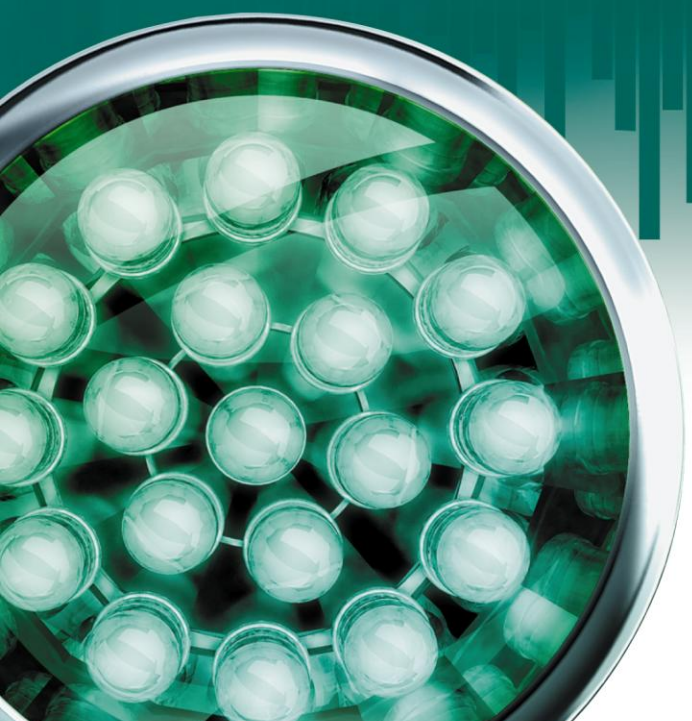
Антивирус Касперского 6.0 для Windows Workstations MP4

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВЕРСИЯ ПРОГРАММЫ: 6.0 ПЛАНОВОЕ ОБНОВЛЕНИЕ 4, КРИТИЧЕСКОЕ ИСПРАВЛЕНИЕ 1



KASPERSKY lab

Уважаемый пользователь!

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

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 24.02.2010

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В ЭТОМ РАЗДЕЛЕ

Комплект поставки

Антивирус Касперского вы можете приобрести у наших партнеров (коробочный вариант), а также в одном из интернет-магазинов (например, http://www.kaspersky.ru, раздел **Интернет-магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта и документация в формате pdf.
- Руководство пользователя в печатном виде (если данная позиция была включена в заказ) или Руководство по продуктам.
- Файл ключа приложения, записанный на специальную дискету.
- Регистрационная карточка (с указанием серийного номера продукта).
- Лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском (или с дискетами), внимательно ознакомьтесь с лицензионным соглашением.

При покупке Антивируса Касперского в интернет-магазине вы копируете продукт с веб-сайта «Лаборатории Касперского», в дистрибутив которого помимо самого продукта включено также данное Руководство. Файл ключа будет вам отправлен по электронной почте по факту оплаты.

Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с продуктом партнеру, у которого она была приобретена, и получить назад сумму, уплаченную за продукт. При этом конверт с установочным компакт-диском (или с дискетами) должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском (или с дискетами), вы тем самым принимаете все условия лицензионного соглашения.

Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели программный продукт.

Если впоследствии у вас изменится почтовый / электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен отрывной корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока действия лицензии. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского», высылается информация о выходе новых программных продуктов.

Сервис для зарегистрированных пользователей

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования приложения.

Приобретая лицензию, вы становитесь зарегистрированным пользователем и в течение срока действия лицензии можете получать следующие услуги:

- ежечасное обновление баз приложения и предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире. Данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/subscribe/).

Консультации по вопросам функционирования и использования операционных систем, стороннего программного обеспечения, а также работы различных технологий не проводятся.

Аппаратные и программные требования к системе

Для нормального функционирования Антивируса Касперского 6.0, компьютер должен удовлетворять следующим минимальным требованиям:

Общие требования:

- 300 МБ свободного места на жестком диске.
- Microsoft Internet Explorer 6.0 или выше (для обновления баз и модулей программы через интернет).
- Microsoft Windows Installer 2.0 или выше.

Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2 или выше), Microsoft Windows XP Professional x64 (Service Pack 2 или выше):

- Процессор Intel Pentium 300 МГц 32-bit (x86) / 64-bit (x64) или выше (или совместимый аналог).
- 256 МБ свободной оперативной памяти.

Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1 или выше), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1 или выше), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:

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

АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS WORKSTATIONS MP4

Антивирус Касперского 6.0 для Windows Workstations MP4 – это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 6.0 для Windows Workstations MP4 от существующих продуктов, в том числе и от продуктов компании ЗАО «Лаборатория Касперского», – это комплексный подход к защите информации на компьютере пользователя.

В ЭТОМ РАЗДЕЛЕ

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ПРОГРАММЕ

Если у вас возникли вопросы, связанные с выбором, приобретением, установкой или использованием Антивируса Касперского, вы можете быстро получить ответы на них.

«Лаборатория Касперского» предоставляет различные источники информации о программе. Среди них вы можете выбрать наиболее удобный для себя в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

ИСТОЧНИКИ ИНФОРМАЦИИ ДЛЯ САМОСТОЯТЕЛЬНОГО ПОИСКА

Вы можете обратиться к следующим источникам информации о программе:

- странице программы на веб-сайте «Лаборатории Касперского»;
- странице программы на веб-сайте Службы технической поддержки (в Базе знаний);
- электронной справочной системе;
- документации.

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/anti-virus_windows_workstation http://www.kaspersky.ru/anti-virus_windows_workstation

На этой странице вы получите общую информацию о программе, ее возможностях и особенностях.

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

http://support.kaspersky.ru/wks http://support.kaspersky.ru/wks

На этой странице вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы по приобретению, установке и использованию программы. Они сгруппированы по темам, таким как «Работа с файлами ключей», «Настройка обновлений баз» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, которые относятся не только к этой программе, но и к другим продуктам «Лаборатории Касперского»; они могут содержать новости Службы технической поддержки в целом.

Электронная справочная система

В комплект поставки программы входит файл полной и контекстной справки, который содержит информацию о том, как управлять защитой компьютера: просматривать состояние защиты, проверять различные области компьютера на вирусы, выполнять другие задачи, а также информацию по каждому окну программы: перечень и описание представленных в нем параметров и список решаемых задач.

Чтобы открыть файл справки, нажмите на кнопку **Справка** в интересующем вас окне или на клавишу **<F1>**.

Документация

В комплект поставки Антивируса Касперского входит документ **Руководство пользователя** (в формате .pdf). Данный документ содержит описание функций и возможностей программы и основные алгоритмы работы.

Обращение в Департамент продаж

Если у вас возникли вопросы по выбору, приобретению Антивируса Касперского 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 осуществляется 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 Антивирус Касперского, вы можете получить информацию об этом приложении от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваши вопросы об установке и использовании приложения, а если ваш компьютер был заражен, они помогут устранить 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

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 как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Выберите тему, наиболее точно соответствующую возникшей проблеме, 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**. Как можно подробнее опишите 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 можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к специалистам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, соберите информацию (http://support.kaspersky.ru/support/details) о своем компьютере и установленном на нем антивирусном приложении. Это позволит нашим специалистам быстрее помочь вам.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

Если ваш вопрос не требует срочного ответа, его можно обсудить 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 Антивирусе Касперского 6.0 для Windows Workstations MP4

Антивирус Касперского 6.0 – это универсальное средство защиты информации. Программа обеспечивает не только антивирусную защиту, но и защиту от спама и сетевых атак. Также компоненты программы позволяют защищать компьютер от неизвестных угроз и интернет-мошенничества, контролировать доступ пользователей компьютера к интернету.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента позволяет максимально адаптировать Антивирус Касперского под нужды конкретного пользователя.

Рассмотрим детально нововведения Антивируса Касперского 6.0.

Новое в защите:

- Новое антивирусное ядро, на базе которого построен Антивирус Касперского, обладает более высокой эффективностью обнаружения вредоносных программ. Также новое антивирусное ядро обеспечивает существенное увеличение скорости проверки системы на присутствие вирусов. Это достигается за счет улучшенной обработки объектов и оптимизированного использования ресурсов компьютера (в особенности платформ на базе двух- и четырехъядерных процессоров).

- Реализован новый эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы. В случае если сигнатура программы не содержится в базах антивируса, эвристический анализатор имитирует ее запуск в изолированной виртуальной среде. Такой метод безопасен и позволяет проанализировать все действия программы еще до ее запуска в реальных условиях.

- Новый компонент Контроль доступа осуществляет контроль работы пользователя с внешними устройствами ввода / вывода, позволяя администраторам ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных.

- Значительно улучшены компоненты Сетевой экран (повышена общая эффективность компонента и добавлена поддержка протокола IPv6) и Проактивная защита (расширен список событий, обрабатываемых компонентом).

- Усовершенствована процедура обновления программы: теперь перезагрузка компьютера требуется в редких случаях.

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

Новое в интерфейсе программы:

- В интерфейсе реализован простой и удобный доступ к любому компоненту программы.

- Интерфейс разработан с учетом потребностей администраторов как небольших сетей, так и сетей крупных корпораций.

Новое в работе через Kaspersky Administration Kit:

- Kaspersky Administration Kit обеспечивает удобное и легкое управление системой антивирусной защиты организации. Программа способна осуществлять централизованное управление защитой корпоративной сети любого размера, насчитывающей десятки тысяч узлов, включая удаленных и мобильных пользователей.

- Реализована возможность удаленной установки программы с последней версией баз программы.

- Усовершенствован механизм работы с программой, установленном на удаленном компьютере (переработана структура политик).

- Добавлена возможность удаленного управления компонентами Анти-Спам и Анти-Шпион.

- Реализована возможность использования конфигурационного файла программы при создании политики.

- При настройке параметров групповых задач обновления добавлена возможность устанавливать специфические параметры для мобильных пользователей.

- Реализована возможность временно выводить клиентские компьютеры с установленной программой из области действия политик и групповых задач (после ввода установленного пароля).

На чем строится защита Антивируса Касперского

Защита Антивируса Касперского строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент программы, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать программу под нужды конкретного пользователя или предприятия в целом.

Антивирус Касперского включает:

- Компоненты защиты (на стр. 19), обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации в режиме реального времени.
- Задачи проверки на вирусы (на стр. 20), посредством которых выполняется проверка компьютера или отдельных файлов, папок, дисков или областей, на присутствие вирусов.
- Обновление (на стр. 20), обеспечивающее актуальность внутренних модулей программы, а также баз, использующихся для поиска вредоносных программ, обнаружения хакерских атак и спам-сообщений.
- Сервисные функции (см. раздел «Сервисные функции программы» на стр. 21), обеспечивающие информационную поддержку в работе с программой и позволяющие расширить ее функциональность.

Компоненты защиты

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

Файловый Антивирус (см. стр. 47)

Файловый Антивирус контролирует файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается Антивирусом Касперского, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

Почтовый Антивирус (см. стр. 58)

Почтовый Антивирус проверяет все входящие и исходящие почтовые сообщения вашего компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов. Также компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

Веб-Антивирус (см. стр. 68)

Веб-Антивирус перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик. Также компонент анализирует веб-страницы на предмет фишинг-мошенничества.

Проактивная защита (см. стр. 75)

Проактивная защита позволяет обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. Компонент основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Антивирус Касперского принимает решение: является программа потенциально опасной или нет. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

Анти-Шпион (см. стр. 85)

Анти-Шпион отслеживает несанкционированный показ материалов рекламного характера (баннеры, всплывающие окна), перехватывает программы несанкционированного дозвона на платные интернет-ресурсы и блокирует их.

Анти-Хакер (см. стр. 89)

Анти-Хакер защищает ваш компьютер при работе в интернете и других сетях. Он контролирует исходящие и входящие соединения, проверяет порты и пакеты данных.

Анти-Спам (см. стр. 106)

Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.). Также компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

Контроль устройств (см. стр. 124)

Компонент предназначен для контроля за доступом пользователей к внешним устройствам, установленным на компьютере. Он ограничивает доступ программ к внешним устройствам (USB-, Firewire-, Bluetooth-устройства и т.д.).

Задачи проверки на вирусы

Крайне важно периодически проводить проверку вашего компьютера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты из-за, например, установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов в состав Антивируса Касперского включены следующие задачи:

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.

Обновление

Чтобы всегда быть готовым отразить любую сетевую атаку, уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского в актуальном состоянии. Для этого предназначен компонент **Обновление**. Он отвечает за обновление баз и модулей, используемых в работе программы.

Сервис копирования обновлений позволяет сохранять обновления баз, а также модулей программы, полученных с серверов «Лаборатории Касперского», в локальном каталоге, а затем предоставлять доступ к ним другим компьютерам сети в целях экономии интернет-трафика.

Сервисные функции программы

Антивирус Касперского включает ряд сервисных функций. Они предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

Файлы данных и отчеты

В процессе работы программы по каждому компоненту защиты, задаче проверки или обновлению программы формируется отчет. Он содержит информацию о выполненных операциях и результаты работы, благодаря чему вы всегда сможете узнать подробности о работе любого компонента Антивируса Касперского. В случае возникновения проблем отчеты можно отправлять в «Лабораторию Касперского», чтобы наши специалисты смогли подробнее изучить ситуацию и помочь вам как можно быстрее.

Все подозрительные, с точки зрения безопасности, объекты Антивирус Касперского переносит в специальное хранилище – *Карантин*. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Вы можете проверять эти объекты на присутствие вирусов, восстанавливать в исходном местоположении, удалять, самостоятельно добавлять объекты на карантин. Все объекты, которые по результатам проверки на вирусы окажутся незараженными, автоматически восстанавливаются в исходном местоположении.

В *Резервное хранилище* помещаются копии вылеченных и удаленных Антивирусом Касперского объектов. Данные копии создаются на случай необходимости восстановить объекты или картину их заражения. Резервные копии объектов также хранятся в зашифрованном виде, чтобы избежать заражения компьютера.

Вы можете восстановить объект из резервного хранилища в исходном местоположении или удалить копию.

Диск аварийного восстановления

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения.

Лицензия

При покупке Антивируса Касперского между вами и «Лабораторией Касперского» заключается лицензионное соглашение, на основе которого вы можете использовать программу и получать доступ к обновлению баз программы и Службе технической поддержки в течение определенного временного периода. Срок использования, а также другая информация, необходимая для полнофункциональной работы программы, 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 Антивируса Касперского 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 программы, 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 Антивирусом Касперского по телефону.

УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 6.0

Антивирус Касперского 6.0 для Windows Workstations MP4 может быть установлен на компьютер несколькими способами:

- локальная установка – установка программы на отдельном компьютере. Для запуска и проведения установки требуется непосредственный доступ к данному компьютеру. Локальная установка может быть проведена в одном из двух режимов:
  - интерактивном, с помощью мастера установки программы (см. раздел «Процедура установки с помощью мастера установки» на стр. 22), данный режим требует участия пользователя в процессе установки;
  - неинтерактивном, запуск установки программы в данном режиме выполняется из командной строки и не требует участия пользователя в процессе установки (см. раздел «Процедура установки программы из командной строки» на стр. 26).
- удаленная установка – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:
  - программного комплекса Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
  - групповых доменных политик Microsoft Windows Server 2000/2003 (см. раздел «Процедура установки через Редактор объектов групповой политики (Group Policy Object)» на стр. 26).

Перед началом установки Антивируса Касперского (в том числе и удаленной) рекомендуется закрыть все работающие программы.

В ЭТОМ РАЗДЕЛЕ

ПРОЦЕДУРА УСТАНОВКИ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Чтобы установить Антивирус Касперского на ваш компьютер, на CD-диске с продуктом запустите файл дистрибутива.

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

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 программы на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

Шаг 1. Проверка соответствия системы необходимым условиям установки Антивируса Касперского

Перед установкой программына компьютере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского. Также проверяется наличие на 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 Антивируса Касперского.

Шаг 2. Стартовое окно процедуры установки

Если ваша система полностью соответствует предъявляемым требованиям, сразу после запуска файла дистрибутива на экране будет открыто стартовое окно, содержащее информацию о начале установки Антивируса Касперского на компьютер.

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

Шаг 3. Просмотр Лицензионного соглашения

Следующее окно программы 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 4. Выбор каталога установки

Следующий этап установки Антивируса Касперского определяет каталог на компьютере, в который будет установлена программа. По умолчанию задан путь:

- **<Диск> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Workstations MP4** – для 32-разрядных систем.
- **<Диск> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Workstations MP4** – для 64-разрядных систем.

Вы можете указать другой каталог, нажав на кнопку **Обзор** и выбрав его в стандартном окне выбора каталога или введя путь к каталогу в соответствующем поле ввода.

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

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

Шаг 5. Использование параметров программы, сохраненных с предыдущей установки

На данном этапе вам будет предложено определить, хотите ли вы использовать в работе программой параметры защиты, базы программы и базу Анти-Спама, если таковые были сохранены на вашем компьютере при удалении предыдущей версии Антивируса Касперского 6.0.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на компьютере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере базы программы, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок ☑ **Базы программы**. Базы программы, включенные в поставку программы, не будут копироваться на компьютер.

Для того чтобы использовать параметры защиты, которые вы настроили в предыдущей версии и сохранили на компьютере, установите флажок ☑ **Параметры работы программы**.

Также рекомендуется воспользоваться базой Анти-Спама, если таковая была сохранена при удалении предыдущей версии программы. Это позволит вам избежать процедуры обучения Анти-Спама. Чтобы учесть уже сформированную вами базу, установите флажок ☑ **Базу Анти-Спама**.

Шаг 6. Выбор типа установки

На данном этапе вам нужно определить полноту установки программы на ваш компьютер. Предусмотрено два варианта установки:

Полная. В этом случае все компоненты Антивируса Касперского будут установлены на ваш компьютер. Для ознакомления с дальнейшей последовательностью установки см. Шаг 8.

Выборочная. В данном случае вам будет предложено выбрать, какие компоненты программы вы хотите установить на ваш компьютер. Подробнее см. Шаг.7.

Для выбора типа установки нажмите на соответствующую кнопку.

Шаг 7. Выбор компонентов программы для установки

Данный шаг выполняется только в случае **Выборочной** установки программы.

При выборочной установке вам нужно определить список компонентов Антивируса Касперского, которые вы хотите установить. По умолчанию для установки выбраны все компоненты защиты, компонент проверки на вирусы, а также коннектор к Агенту администрирования для удаленного управления программой через Kaspersky Administration Kit.

Для того чтобы выбрать компонент для последующей установки, нужно открыть меню по левой клавише мыши на значке рядом с именем компонента и выбрать пункт **Компонент будет установлен на локальный жесткий диск**. Подробнее о том, какую защиту обеспечивает выбранный компонент и сколько места на диске требуется для его установки, вы можете прочесть в нижней части данного окна программы установки.

Чтобы узнать подробную информацию о свободном месте на жестких дисках вашего компьютера, нажмите на кнопку **Диск**. Информация будет предоставлена в открывшемся окне.

Для отказа от установки компонента в контекстном меню выберите вариант **Компонент будет недоступен**. Помните, что, отменяя установку какого-либо компонента, вы лишаетесь защиты от целого ряда опасных программ.

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. Отключение сетевого экрана Microsoft Windows

Данный шаг выполняется только в том случае, если Антивирус Касперского устанавливается на компьютер с включенным сетевым экраном, и в числе устанавливаемых компонентов присутствует Анти-Хакер.

На данном этапе установки Антивируса Касперского вам предлагается отключить сетевой экран операционной системы Microsoft Windows, поскольку входящий в состав Антивируса Касперского компонент Анти-Хакер обеспечивает полную защиту вашей работы в сети, и нет необходимости в дополнительной защите средствами операционной системы.

Если вы хотите использовать Анти-Хакер в качестве основного средства защиты при работе в сети, нажмите на кнопку **Далее**. Сетевой экран Microsoft Windows будет автоматически отключен.

Если вы хотите защищать свой компьютер с помощью сетевого экрана Microsoft Windows, выберите вариант **Использовать сетевой экран Microsoft Windows**. В этом случае компонент Анти-Хакер будет установлен, но отключен во избежание конфликтов в работе программ.

Шаг 9. 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 Антивируса Касперского 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 программ вы можете выбрать, автоматически удалить их или вручную.

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

Шаг 10. Завершающая подготовка к установке программы

На данном этапе вам будет предложено произвести завершающую подготовку к установке программы на ваш компьютер.

При первоначальной установке Антивируса Касперского 6.0 не рекомендуется снимать флажок **Защитить процесс установки**. Включенная защита позволит, в случае возникновения ошибок в ходе установки программы, провести корректную процедуру отката установки. При повторной попытке установки программы рекомендуется снять данный флажок.

При удаленной установке программы на компьютер через **Windows Remote Desktop** рекомендуется снимать флажок **Защитить процесс установки**. В противном случае процедура установки может быть не проведена или проведена некорректно.

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

В процессе установки в составе Антивируса Касперского компонентов, перехватывающих сетевой трафик, происходит разрыв текущих сетевых соединений. Большинство прерванных соединений восстанавливается через некоторое время.

Шаг 11. Завершение процедуры установки

Окно **Завершение установки** содержит информацию об окончании процесса установки Антивируса Касперского на ваш компьютер.

Для запуска мастера первоначальной настройки программы нажмите на кнопку **Далее**.

Если для корректного завершения установки необходимо перезагрузить компьютер, на экран будет выведено соответствующее уведомление.

Процедура установки программы из командной строки

- *Чтобы установить Антивируса Касперского 6.0 для Windows Workstations MP4, наберите в командной строке:*

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. раздел «Процедура установки с помощью мастера установки» на стр. 22). По завершении установки программы, необходимо перезагрузить компьютер.

- *Чтобы установить программу в неинтерактивном режиме (без запуска мастера установки), наберите:*

```
msiexec /i <имя_пакета> /qn
```

В данном случае по завершении установки программы потребуется вручную произвести перезагрузку компьютера. Для выполнения автоматической перезагрузки в командной строке наберите:

```
msiexec /i <имя_пакета> ALLOWREBOOT=1 /qn
```

Обратите внимание, что автоматическая перезагрузка компьютера может быть выполнена только в режиме неинтерактивной установки (с ключом /qn).

- *Чтобы установить программу с указанием пароля, подтверждающего право на удаление программы, наберите:*

  `msiexec /i <имя_пакета> KLUNINSTPASSWD=******` – при установке программы в интерактивном режиме;

  `msiexec /i <имя_пакета> KLUNINSTPASSWD=****** /qn` – при установке программы в неинтерактивном режиме без перезагрузки компьютера;

  `msiexec /i <имя_пакета> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn` – при установке программы в неинтерактивном режиме с последующей перезагрузкой компьютера.

При установке Антивируса Касперского в неинтерактивном режиме поддерживается чтение файла setup.ini (см. стр. 27), содержащего общие параметры установки программы, конфигурационного файла *install.cfg* (см. раздел «Импорт параметров защиты» на стр. 208), а также файла ключа. Обратите внимание, что данные файлы должны быть расположены в одном каталоге с дистрибутивом Антивируса Касперского.

Процедура установки через Редактор объектов групповой политики (Group Policy Object)

С помощью **Редактора объектов групповой политики** вы можете устанавливать, обновлять и удалять Антивирус Касперского на рабочих станциях предприятия, входящих в состав домена, без использования Kaspersky Administration Kit.

Установка программы

Чтобы установить Антивирус Касперского, выполните следующие действия:

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена, и поместите в нее дистрибутив Антивируса Касперского в формате *.msi*.

   Дополнительно в данную директорию можно поместить файл *setup.ini* (см. стр. 27), содержащий перечень параметров установки Антивируса Касперского, конфигурационный файл *install.cfg* (см. раздел «Импорт параметров защиты» на стр. 208), а также файл ключа.

2. Откройте **Редактор объектов групповой политики** через стандартную консоль MMC (подробную информацию о работе с Редактором см. в справочной системе к Microsoft Windows Server).

3. Создайте новый пакет. Для этого в дереве консоли выберите **Объект групповой политики / Конфигурация компьютера/ Конфигурация программ / Установка программного обеспечения** и воспользуйтесь командой **Создать / Пакет** контекстного меню.

   В открывшемся окне укажите путь к сетевой папке общего доступа, содержащей дистрибутив Антивируса Касперского. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный** и нажмите на кнопку **ОК**.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате Антивирус Касперского будет установлен на все компьютеры.

Описание параметров файла setup.ini

Файл *setup.ini*, расположенный в каталоге дистрибутива Антивируса Касперского, используется при установке программы в неинтерактивном режиме через командную строку или Редактор объектов групповой политики. Данный файл содержит следующие параметры:

[Setup] – общие параметры установки программы.

- **InstallDir=**<путь к каталогу установки программы>.
- **Reboot=yes|no** – следует ли выполнять перезагрузку компьютера по завершении установки программы (по умолчанию перезагрузка не выполняется).
- **SelfProtection=yes|no** – следует ли включать самозащиту Антивируса Касперского при установке (по умолчанию самозащита включена).
- **NoKLIM5=yes|no** – следует ли отменить установку сетевых драйверов Антивируса Касперского при установке (по умолчанию драйверы устанавливаются). Сетевые драйверы Антивируса Касперского, относящиеся к группе драйверов NDIS и отвечающие за перехват сетевого трафика для таких компонентов программы, как Анти-Хакер, Почтовый Антивирус, Веб-Антивирус и Анти-Спам, могут привести к конфликтам с другими программами или оборудованием, установленным на компьютере пользователя. На компьютерах под управлением Microsoft Windows XP или Microsoft Windows 2000 для решения возможных конфликтов можно отказаться от установки сетевых драйверов.

  На компьютерах под управлением Microsoft Windows XP x64 Edition и Microsoft Vista данная возможность недоступна.

[Components] – выбор компонентов программы для установки. В случае если не указан ни один компонент, программа устанавливается полностью. Если указан хотя бы один из компонентов, неперечисленные компоненты не устанавливаются.

- **FileMonitor=yes|no** – установка компонента Файловый Антивирус.
- **MailMonitor=yes|no** – установка компонента Почтовый Антивирус.

- **WebMonitor=yes|no** – установка компонента Веб-Антивирус.
- **ProactiveDefence=yes|no** – установка компонента Проактивная защита.
- **AntiSpy=yes|no** – установка компонента Анти-Шпион.
- **AntiHacker=yes|no** – установка компонента Анти-Хакер.
- **AntiSpam=yes|no** – установка компонента Анти-Спам.
- **LockControl=yes|no** – установка компонента Контроль устройств.

[Tasks] – включение задач Антивируса Касперского. В случае если не указана ни одна задача, после установки все задачи будут работать. Если указана хотя бы одна задача, все неперечисленные задачи будут выключены.

- **ScanMyComputer=yes|no** – задача полной проверки.
- **ScanStartup=yes|no** – задача быстрой проверки.
- **Scan=yes|no** – задача проверки.
- **Updater=yes|no** – задача обновления баз и модулей программы.

Вместо значения **yes** могут использоваться значения 1, on, enable, enabled, а вместо значения **no** – 0, off, disable, disabled.

Обновление версии программы

Для обновления версии Антивируса Касперского, выполните следующие действия:

1. Поместите дистрибутив, содержащий обновления Антивируса Касперского, в формате .msi в сетевую папку общего доступа.
2. Откройте **Редактор объектов групповой политики** и создайте новый пакет описанным выше способом.
3. Выберите новый пакет в списке и воспользуйтесь командой **Свойства** контекстного меню. В окне свойств пакета перейдите на закладку **Обновления** и укажите пакет, который содержит дистрибутив предыдущей версии Антивируса Касперского. Чтобы установить обновленную версию Антивируса Касперского с сохранением параметров защиты, выберите вариант установки поверх существующего пакета.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене.

Удаление программы

Чтобы удалить Антивирус Касперского, выполните следующие действия:

1. Откройте **Редактор объектов групповой политики**.
2. В дереве консоли выберите **Объект_групповой_политики / Конфигурация компьютера/ Конфигурация программ/ Установка программного обеспечения**.

   В списке пакетов выберите пакет Антивируса Касперского, откройте контекстное меню и выполните команду **Все задачи/ Удалить**.

В диалоговом окне **Удаление программ** выберите **Немедленное удаление этой программы с компьютеров всех пользователей**, чтобы Антивирус Касперского был удален при следующей перезагрузке компьютера.

НАЧАЛО РАБОТЫ

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

Однако особенности конфигурации вашего компьютера или задач, решаемых на нем, могут иметь некоторую специфику. Поэтому мы рекомендуем вам провести предварительную настройку программы, чтобы максимально гибко подойти к защите именно вашего компьютера.

Для удобства пользователей мы постарались объединить этапы предварительной настройки в едином интерфейсе мастера первоначальной настройки, который запускается в конце процедуры установки программы. Следуя указаниям мастера, вы сможете провести активацию программы, настроить параметры обновления, ограничить доступ к программе с помощью пароля и произвести другие настройки.

Ваш компьютер может быть заражен вредоносными программами до установки Антивируса Касперского. Чтобы обнаружить имеющиеся вредоносные программы, запустите проверку компьютера (см. раздел «Проверка компьютера на вирусы» на стр. 126).

На момент установки программы входящие в поставку базы могут устареть. Запустите обновление программы (на стр. 138) (если это не было сделано с помощью мастера настройки либо автоматически сразу после установки программы).

Входящий в состав Антивируса Касперского компонент Анти-Спам использует самообучающийся алгоритм для распознавания нежелательных сообщений. Запустите мастер обучения Анти-Спама (см. раздел «Обучение с помощью Мастера обучения» на стр. 109), чтобы настроить компонент для работы с вашей корреспонденцией.

После выполнения вышеописанных действий программа готово к работе. Чтобы оценить уровень защиты вашего компьютера, воспользуйтесь мастером управления безопасностью (см. раздел «Управление безопасностью» на стр. 38).

В ЭТОМ РАЗДЕЛЕ

Мастер первоначальной настройки

Мастер настройки Антивируса Касперского запускается в конце процедуры установки программы. Его задача – помочь вам провести первичную настройку параметров программы, исходя из особенностей и задач вашего компьютера.

Интерфейс мастера настройки выполнен в стиле программы-мастера для Microsoft Windows (Windows Wizard) и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Для полной установки программы на компьютер, необходимо выполнить все шаги мастера. Если по каким-либо причинам работа мастера была прервана, то уже заданные значения параметров не сохраняются. Далее, при попытке начать работу с программой, мастер первоначальной настройки запускается вновь, что влечет за собой необходимость заново производить настройку параметров.

Использование объектов, сохраненных с предыдущей версии

Данное окно мастера появляется при установке программы поверх предыдущей версии Антивируса Касперского. Вам предлагается выбрать, какие данные, используемые предыдущей версией, требуется перенести в новую версию. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в новой версии программы, установите необходимые флажки.

Активация программы

Процедура активации программы заключается в регистрации лицензии при помощи установки файла ключа. На основании лицензии программа будет определять наличие прав и срок на его использование.

Файл ключа содержит служебную информацию, необходимую для полнофункциональной работы Антивируса Касперского, а также дополнительные сведения:

- информацию о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также дату окончания срока действия лицензии.

В зависимости от того, имеется ли у вас файл ключа или вам необходимо получить его с сервера «Лаборатории Каперского», вам предлагаются следующие варианты активации Антивируса Касперского:

- онлайн-активация (на стр. 31). Выберите этот вариант активации, если вы приобрели коммерческую версию программы и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к полной функциональности программы на весь период действия лицензии.
- активация пробной версии (на стр. 32). Выберите данный вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный файл ключа со сроком действия, ограниченным лицензией для пробной версии программы.
- активация с помощью полученного ранее файла ключа (см. раздел «Активация с помощью файла ключа» на стр. 32). Активируйте программу с помощью полученного ранее файла ключа для Антивируса Касперского 6.0.
- активировать программу позже. При выборе этого варианта этап активации Антивируса Касперского будет пропущен. Программа будет установлена на ваш компьютер, вам будут доступны все функции программы, за исключением обновления (обновить программу вы сможете только один раз после установки). Вариант **Активировать программу позже** доступен только при первом запуске мастера

активации. При последующих запусках мастера, в случае если программа уже активирована, вариант **Удалить файл ключа** для выполнения соответствующей операции.

При выборе первых двух вариантов активация программы осуществляется через веб-сервер «Лаборатории Касперского», для соединения с которым требуется подключение к интернету. Перед началом активации проверьте и, при необходимости, измените параметры сетевого соединения в окне, открывающемся по кнопке **Параметры LAN**. Для получения более подробной информации о настройке сетевых параметров обратитесь к вашему системному администратору или интернет-провайдеру.

Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже из интерфейса программы либо, выйдя в интернет с другого компьютера, получить файл ключа по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

Вы также можете активировать программу через Kaspersky Administration Kit. Для этого необходимо создать задачу установки файла ключа (см. стр. 224) (подробнее смотрите Справочное руководство «Kaspersky Administration Kit»).

См. также

Онлайн-активация

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

Ввод кода активации

На данном этапе требуется указать код активации. 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.

В нижней части окна укажите вашу контактную информацию: фамилию, имя, отчество, адрес электронной почты, страну и город проживания. Данная информация может потребоваться для идентификации зарегистрированного пользователя, если, например, данные о лицензии были утрачены или похищены. В данном случае на основании контактных данных вы сможете получить другой код активации.

Получение файла ключа

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете и отправляет на них ваши регистрационные данные (код активации, контактную информацию). После установления соединения на сервере проверяются код активации и полнота заполнения контактной информации. Если код активации прошел проверку, мастер получает файл ключа, который автоматически устанавливается. Процесс активации завершается, что сопровождается окном с подробной информацией о приобретенной лицензии.

Если код активации не прошел проверку, на экране появляется соответствующее уведомление. В данном случае вам следует обратиться за информацией в компанию, где вы приобрели Антивирус Касперского.

Если число активаций с помощью кода активации превышено, на экране также появляется соответствующее уведомление. Процесс активации будет прерван, и программа предложит вам обратиться в Службу поддержки «Лаборатории Касперского».

Активация пробной версии

Данный вариант активации следует использовать, если вы хотите установить пробную версию Антивируса Касперского перед принятием решения о покупке коммерческой версии. Вам будет предоставлена бесплатная лицензия со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

Активация с помощью файла ключа

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

После успешной установки ключа в нижней части окна будет представлена информация о лицензии: номер лицензии, ее тип (коммерческая, пробная и т. д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

Завершение активации

Мастер настройки информирует вас об успешном завершении активации Антивируса Касперского. Кроме того, приводится информация о лицензии: номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная и т.д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

Выбор режима защиты

В данном окне мастера настройки вам предлагается выбрать режим защиты, в котором будет работать программа:

- **Базовый**. Этот режим установлен по умолчанию и предназначен для большинства пользователей, не имеющих достаточного опыта работы с компьютером и антивирусными продуктами. Он подразумевает работу компонентов программы на рекомендуемом уровне безопасности и информирование пользователя о возникновении только опасных событий (например, обнаружение вредоносного объекта, выполнение опасных действий).

- **Интерактивный**. Этот режим предполагает расширенную защиту данных компьютера по сравнению с базовой защитой. Он позволяет отслеживать попытки изменения системных настроек, подозрительную активность в системе, а также несанкционированные действия в сети.

  Все перечисленные выше действия могут являться как результатом деятельности вредоносных программ, так и быть стандартными в рамках работы программ, используемых на вашем компьютере. В каждом отдельном случае вам понадобится принять решение о допустимости или недопустимости тех или иных действий.

  При выборе этого режима укажите, в каких случаях он должен использоваться:

  - **Включить режим обучения Анти-Хакера** – запрашивать подтверждение действий пользователя при попытках программ, установленных на вашем компьютере, установить соединение с некоторым сетевым ресурсом. Вы можете разрешить либо запретить данное соединение, настроить правила работы Анти-Хакера для данной программы. При отключении режима обучения Антивирус Касперского работает в режиме минимальной защиты, то есть всем программам разрешен доступ к сетевым ресурсам.

  - **Включить мониторинг системного реестра** – выводить запрос действий пользователя при обнаружении попыток изменения объектов системного реестра.

НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ

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

- **Автоматически**. Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.

- **Каждые 2 часа** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открывающемся по кнопке **Изменить**.

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

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

Если вы хотите перейти к настройке параметров обновления (установить сетевые параметры, выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления от имени определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на кнопку **Настройка**.

НАСТРОЙКА РАСПИСАНИЯ ПРОВЕРКИ НА ВИРУСЫ

Поиск вредоносных объектов в заданных областях проверки – одна из важных задач, обеспечивающих защиту компьютера.

При установке Антивируса Касперского по умолчанию создаются три задачи проверки на вирусы. В данном окне мастера настройки вам предлагается выбрать режим запуска задач проверки:

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. Параметры расписания можно изменить в окне, открывающемся по кнопке **Изменить**.

Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы. Параметры расписания можно изменить в окне, открывающемся по кнопке **Изменить**.

ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

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

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 программой, за исключением работы с уведомлениями об обнаружении опасных объектов.

- **Отдельные операции**:

  - **Настройка параметров программы** – запрашивать пароль при попытке пользователя изменить параметры работы Антивируса Касперского.

  - **Завершение работы программы** – запрашивать пароль при попытке пользователя завершить работу программы.

  - **Отключение компонентов защиты и остановка задач проверки** – запрашивать пароль при попытке пользователя выключить работу какого-либо компонента защиты либо остановить задачу проверки.

  - **Отключение политики Kaspersky Administration Kit** – запрашивать пароль при попытке пользователя вывести компьютер из области действия политик и групповых задач (при работе через Kaspersky Administration Kit).

  - **При удалении программы** – запрашивать пароль при попытке пользователя удалить программу с компьютера.

Настройка параметров работы Анти-Хакера

Анти-Хакер является компонентом Антивируса Касперского, обеспечивающим безопасность работы вашего компьютера в локальных сетях и интернете. На данном этапе мастер настройки предлагает вам сформировать ряд правил, которыми Анти-Хакер будет руководствоваться при анализе сетевой активности вашего компьютера.

См. также

Определение статуса зоны безопасности

На данном этапе мастер настройки проводит анализ сетевого окружения вашего компьютера. По результатам анализа все сетевое пространство делится на условные зоны:

- *Интернет* – глобальная сеть Интернет. В данной зоне Антивирус Касперского работает как персональный сетевой экран. При этом вся сетевая активность регламентируется правилами для пакетов и программ, созданными по умолчанию для обеспечения максимальной безопасности. Вы не можете изменять условия защиты при работе в данной зоне, кроме как включить режим невидимости компьютера для дополнительной безопасности.

- *Зоны безопасности* – некоторые условные зоны, зачастую совпадающие с подсетями, в которые включен ваш компьютер (это могут быть локальные подсети дома или на работе). По умолчанию данные зоны считаются зонами средней степени риска при работе в них. Вы можете изменять статус данных зон исходя из степени доверия той или иной подсети, а также настраивать правила для пакетов и программ.

Все обнаруженные зоны представлены в списке. Для каждой из них дано описание, указаны адрес и маска подсети, а также статус, на основании которого будет разрешена либо запрещена та или иная сетевая активность в рамках работы компонента Анти-Хакер:

- **Интернет**. Этот статус по умолчанию присваивается сети Интернет, поскольку при работе в ней компьютер подвержен любым возможным типам угроз. Также данный статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами и

т.д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне, а именно:

- блокируется любая сетевая NetBios-активность в рамках подсети;
- запрещается выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям подсети с таким статусом. Кроме того, при выборе данного статуса вы не сможете получить доступ к файлам и принтерам на других компьютерах сети.

- **Локальная сеть**. Этот статус присваивается по умолчанию большинству зон безопасности, обнаруженных при анализе сетевого окружения компьютера, за исключением сети Интернет. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети). При выборе данного статуса разрешается:
  - любая сетевая NetBios-активность в рамках подсети;
  - выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Выбирайте этот статус, если вы хотите предоставить доступ к некоторым каталогам или принтерам на вашем компьютере, но запретить любую другую внешнюю активность.

- **Доверенная**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность. Даже если установлен уровень Максимальной защиты и созданы запрещающие правила, они не будут действовать для удаленных компьютеров доверенной зоны.

Для сети со статусом **Интернет** вы можете для дополнительной безопасности использовать *режим невидимости*. В этом режиме разрешена только сетевая активность, инициируемая с вашего компьютера. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на вашу работу в интернете режим не оказывает никакого влияния.

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, http-сервера). Иначе, компьютеры, обращающиеся к данному серверу, не будут видеть его в сети.

Чтобы изменить статус зоны либо включить/ отключить режим невидимости, выберите ее в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующими ссылками. Аналогичные действия, а также редактирование адреса и маски подсети можно выполнить в окне **Параметры зоны**, открывающемся по кнопке **Изменить**.

При просмотре списка зон вы можете добавить в него новую, для этого воспользуйтесь кнопкой **Найти**. Анти-Хакер произведет поиск доступных зон и, если таковые будут обнаружены, предложит вам определить их статус. Кроме того, вы можете добавить новую зону в список вручную (например, в случае, когда вы включаете мобильный компьютер в новую сеть). Для этого воспользуйтесь кнопкой **Добавить** и укажите требующуюся информацию в окне **Параметры зоны**.

Чтобы удалить сеть из списка, воспользуйтесь кнопкой **Удалить**.

Формирование списка сетевых программ

Мастер настройки анализирует установленное на вашем компьютере программное обеспечение и формирует список программ, использующих для своей работы сеть.

Для каждого из таких программ Анти-Хакер создает правило, регламентирующее сетевую активность. Правила применяются на основе сформированных в «Лаборатории Касперского» и включенных в поставку продукта шаблонов наиболее распространенных программ, использующих сеть.

Список сетевых программ и правила для них вы можете посмотреть в окне настройки Анти-Хакера, которое открывается по кнопке **Список**.

В качестве дополнительной защиты рекомендуется отключить кеширование доменных имен при работе с интернет-ресурсами. Этот сервис значительно сокращает время соединения вашего компьютера с нужным интернет-ресурсом, однако в то же время является опасной уязвимостью, используя которую злоумышленники могут организовать канал утечки данных, который невозможно будет отследить с помощью сетевого экрана. Поэтому для повышения уровня безопасности вашего компьютера мы рекомендуем отключать сохранение информации о доменных именах в кеше.

Завершение работы мастера настройки

В последнем окне мастера вам предлагается перезагрузить компьютер для завершения установки программы. Перезагрузка необходима для регистрации драйверов Антивируса Касперского.

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

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 Антивируса Касперского 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 программы.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Нажмите на кнопку **Выполнить проверку**, чтобы начать проверку. Нажмите на кнопку **Остановить проверку** во время работы задачи, если возникла необходимость остановить ее выполнение.

Обновление программы

Для обновления Антивируса Касперского требуется наличие соединения с интернетом.

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

Во время работы мастера настройки программы вы можете выбрать режим запуска обновления. По умолчанию Антивирус Касперского автоматически проверяет наличие обновлений на серверах «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Антивирус Касперского в фоновом режиме скачивает и устанавливает их.

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

Для поддержания защиты вашего компьютера в актуальном состоянии рекомендуется обновить Антивирус Касперского непосредственно после установки.

Чтобы самостоятельно обновить Антивирус Касперского, выполните следующие действия:

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

Управление лицензиями

Возможность использования Антивируса Касперского определяется наличием лицензии. Лицензия предоставляется вам на основании покупки продукта и дает право использовать программу со дня активации.

Без лицензии в случае, если не было активации пробной версии программы, Антивирус Касперского будет работать в режиме – одно обновление. В дальнейшем новые обновления производиться не будут.

Если была активирована пробная версия программы, то после завершения срока действия пробной лицензии, Антивирус Касперского работать не будет.

По окончании срока действия коммерческой лицензии функциональность программы сохраняется за исключением возможности обновления баз программы. Вы по-прежнему можете проверять ваш компьютер посредством задач проверки и использовать компоненты защиты, но только на основе баз, актуальных на дату окончания срока действия лицензии. 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 лицензию на использование Антивируса Касперского. За две недели до истечения срока действия лицензии программа уведомляет вас об этом. В течение некоторого периода времени при каждом запуске программы на экран выводится соответствующее сообщение.

Основная информация об используемой лицензии (активной и дополнительной, если последняя была установлена) представлена в разделе **Лицензия** главного окна Антивируса Касперского: тип лицензии (коммерческая, пробная, для бета-тестирования), ограничение количества компьютеров, дата окончания срока действия лицензии и количество дней до этой даты. Чтобы получить более подробную информацию и лицензии, воспользуйтесь ссылкой с используемым типом лицензии.

Чтобы ознакомиться с условиями лицензионного соглашения на использование программы воспользуйтесь кнопкой **Прочесть лицензионное соглашение**.

Чтобы удалить лицензию нажмите на кнопку **Добавить / Удалить** и следуйте указаниям открывшегося мастера.

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**.

Чтобы приобрести лицензию или продлить срок ее действия, выполните следующие действия:

1. Приобретите новый файл ключа или код активации. Для этого воспользуйтесь кнопкой **Купить лицензию** (в случае если программа 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 программы.
2. Активируйте программу. Для этого воспользуйтесь кнопкой **Добавить / Удалить** в разделе **Лицензия** главного окна программы либо командой **Активация** контекстного меню программы. В результате будет запущен мастер активации.

Управление безопасностью

О появлении проблем в защите компьютера сигнализирует статус защиты компьютера (см. раздел «Главное окно программы» на стр. 43) посредством изменения цвета значка статуса защиты и панели, на которой он расположен. При возникновении проблем в защите рекомендуется немедленно устранить их.

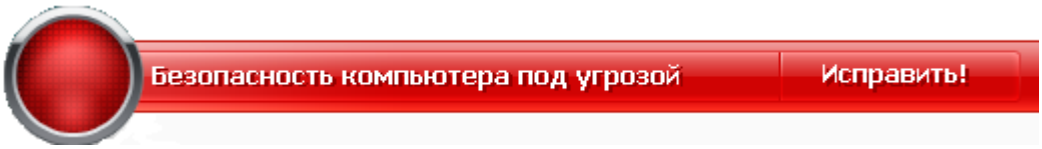


Рисунок 1. Текущее состояние защиты компьютера

Просмотреть список возникших проблем, их описание и возможные пути решения вы можете с помощью Мастера безопасности (см. рис. ниже), переход к которому осуществляется по ссылке **Исправить** (см. рис. выше).

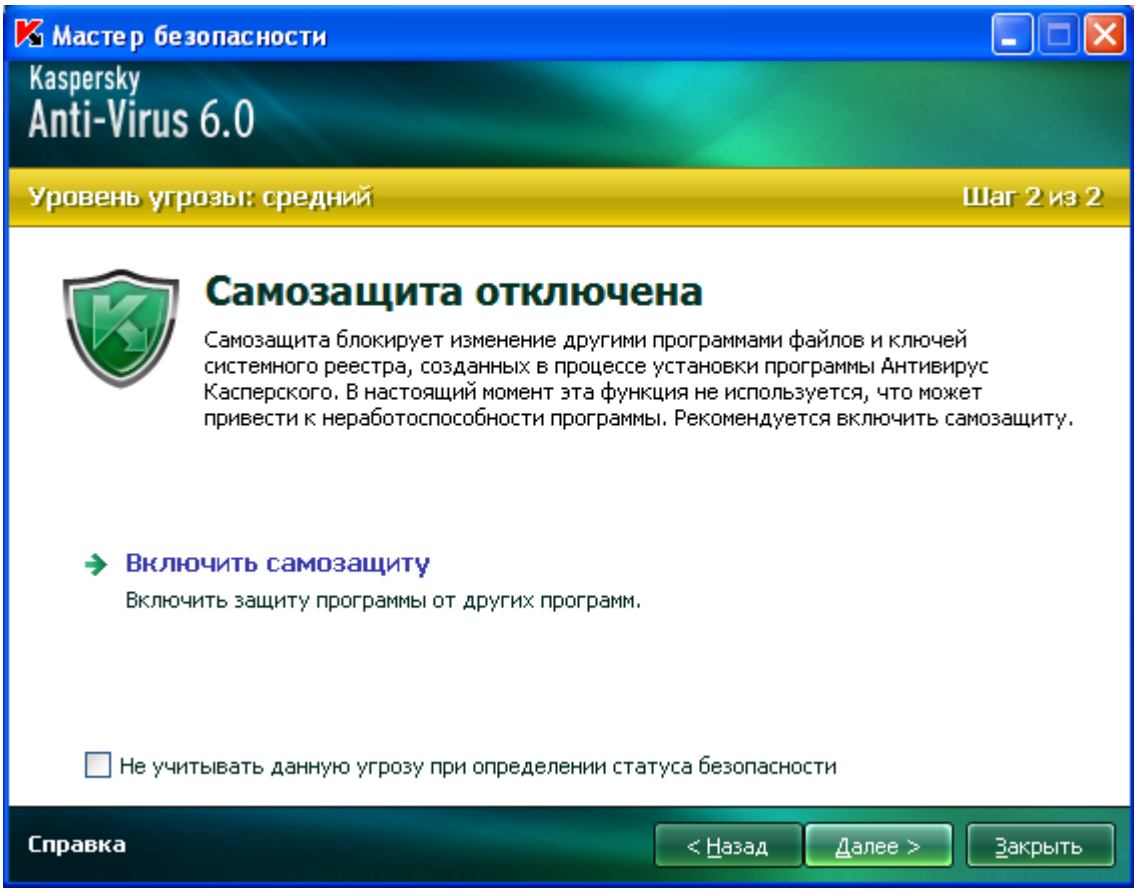


Рисунок 2. Решение проблем безопасности

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 ссылки, 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. Установите флажок ☑ **Не учитывать**

данную угрозу при определении статуса безопасности, чтобы угроза не влияла на текущий статус защиты.

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 программы. Такого рода проблемы необходимо устранять как можно быстрее.

ПРИОСТАНОВКА ЗАЩИТЫ

Приостановка защиты означает отключение на некоторый промежуток времени всех компонентов защиты, контролирующих файлы на вашем компьютере, входящую и исходящую почту, интернет-трафик, поведение программ, а также Анти-Хакер и Анти-Спам.

Чтобы приостановить работу Антивируса Касперского, выполните следующие действия:

1. В контекстном меню программы выберите пункт **Приостановка защиты**.

2. В открывшемся окне **Приостановка защиты** из предложенных вариантов выберите период времени, спустя который защита будет включена.

УСТРАНЕНИЕ ПРОБЛЕМ. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПОЛЬЗОВАТЕЛЕЙ

Если при использовании Антивируса Касперского 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 программы.

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 программой, – это Форум пользователей продуктов «Лаборатории Касперского». Данный ресурс также является отдельным разделом веб-сайта Службы технической поддержки и содержит вопросы, отзывы и пожелания пользователей программы. Вы можете ознакомиться с основными темами форума, оставить отзыв о программе или отыскать ответ на свой вопрос.

Чтобы открыть форум пользователей, выполните следующие действия:

1. Откройте главное окно программы.

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».

Создание файла трассировки

После установки Антивируса Касперского могут возникнуть сбои в работе операционной системы или отдельных программ. В этом случае, скорее всего, имеет место конфликт программы 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 программы.
2. В нижней части окна программы 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**.

Настройка параметров программы

Для быстрого доступа к параметрам Антивируса Касперского 6.0 предназначено окно настройки параметров программы (см. стр. 150), которое вызывается из главного окна с помощью кнопки **Настройка**.

Отчеты о работе программы. Файлы данных

Работа каждого компонента Антивируса Касперского и выполнение каждой задачи проверки и обновления фиксируется в отчете (см. стр. 172). Чтобы перейти к просмотру отчетов, воспользуйтесь кнопкой **Отчеты**, расположенной в правом нижнем углу главного окна.

Объекты, помещенные в процессе работы Антивируса Касперского на карантин (см. стр. 173) или в резервное хранилище (см. стр. 174), называются *файлами данных программы*. С помощью кнопки **Обнаружено**, вы можете открыть окно **Хранилище данных**, где с этими объектами вы можете выполнять нужные действия.

ИНТЕРФЕЙС ПРОГРАММЫ

Антивирус Касперского обладает достаточно простым и удобным в работе интерфейсом. В данной главе мы подробнее рассмотрим основные его элементы.

Кроме основного интерфейса программа имеет компоненты расширения (плагины), встраиваемые в программы Microsoft Office Outlook (проверка на вирусы и проверка на спам), Microsoft Outlook Express (Windows Mail), The Bat! (проверка на вирусы и проверка на спам), Microsoft Internet Explorer, Microsoft Windows Explorer. Плагины расширяют возможности перечисленных программ, позволяя из их интерфейса осуществлять управление и настройку соответствующих компонентов Антивируса Касперского.

В ЭТОМ РАЗДЕЛЕ

См. также

Значок в области уведомлений панели задач

Сразу после установки Антивируса Касперского его значок появляется в области уведомлений панели задач Microsoft Windows.

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

Если значок активный (цветной), это означает, что защита вашего компьютера включена. Если значок неактивный (серый), значит все компоненты защиты (на стр. 19) выключены.

В зависимости от выполняемой операции значок Антивируса Касперского меняется:

- – выполняется проверка почтового сообщения.
- –выполняется проверка HTTP-трафика.
- – выполняется проверка файла, который открываете, сохраняете или запускаете вы или некоторая программа.
- – выполняется обновление баз и модулей Антивируса Касперского.
- – требуется перезагрузка компьютера для применения обновлений.
- – произошел сбой в работе какого-либо из компонентов Антивируса Касперского.

Также значок обеспечивает доступ к основным элементам интерфейса программы: контекстному меню и главному окну.

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

Чтобы открыть главное окно Антивируса Касперского, щелкните левой клавишей мыши по значку программы.

Контекстное меню

Контекстное меню позволяет перейти к выполнению основных задач защиты.

Меню Антивируса Касперского содержит следующие пункты:

- **Полная проверка –** запуск полной проверки (см. стр. 126) вашего компьютера на присутствие вредоносных объектов. В результате будут проверены объекты на всех дисках, в том числе и сменных носителях.

- **Проверка –** переход к выбору объектов и запуску проверки на вирусы. По умолчанию список содержит ряд объектов, таких как каталог **Мои Документы**, объекты автозапуска, почтовые базы, все диски вашего компьютера и т.д. Вы можете пополнить список, выбрать объекты для проверки и запустить поиск вирусов.

- **Обновление** – запуск обновления (см. стр. 138) модулей и баз программы для Антивируса Касперского и их установка на вашем компьютере.

- **Мониторинг сети** – просмотр списка (см. стр. 102) установленных сетевых соединений, открытых портов и трафика.

- **Активация** – переход к активации программы (см. стр. 30). Для получения статуса зарегистрированного пользователя, на основании которого вам будут доступны полная функциональность программы и сервисы Службы технической поддержки, необходимо активировать вашу версию Антивируса Касперского. Данный пункт меню присутствует только в том случае, если программа не активирована.

- **Настройка** – переход к просмотру и настройке параметров работы (см. стр. 150) Антивируса Касперского.

- **Антивирус Касперского** – открытие главного окна (см. стр. 43) программы.

- **Приостановка защиты / Включение защиты** – выключение на время/ включение работы компонентов защиты (см. стр. 19). Данный пункт меню не влияет на обновление программы и на выполнение задач поиска вирусов.

- **Отключение политики / Включение политики –** выключение на время/ включение политики при работе программы через Kaspersky Administration Kit. Пункт меню позволяет вывести компьютер из зоны действия политик и групповых задач. Данная возможность управляется паролем. Пункт меню появляется в том случае, если задан пароль.

- **О программе** – вызов информационного окна о программе.

- **Выход** – завершить работу Антивируса Касперского (при выборе данного пункта меню программа будет выгружена из оперативной памяти компьютера).

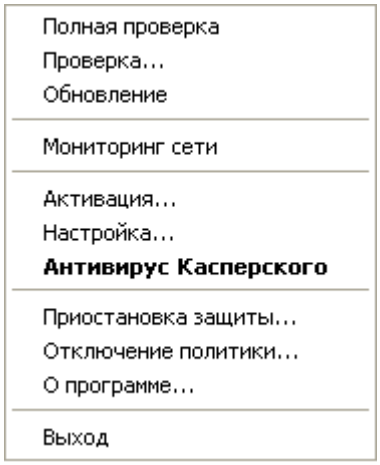


Рисунок 3. Контекстное меню

Если в данный момент запущена какая-либо задача поиска вирусов, ее имя будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав задачу, вы можете перейти к окну отчета с текущими результатами ее выполнения.

Главное окно программы

Главное окно программы условно можно разделить на три части:

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

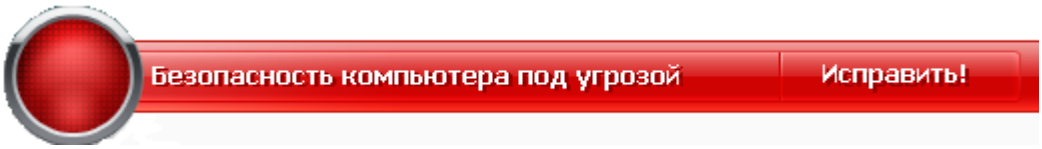


Рисунок 4. Текущее состояние защиты компьютера

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 Антивируса Касперского. К угрозам относятся не только вредоносные программы, но и устаревшие базы программы, некоторые выключенные компоненты защиты, минимальные параметры работы программы 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 программы, к выполнению задач проверки на вирусы или обновления и др.

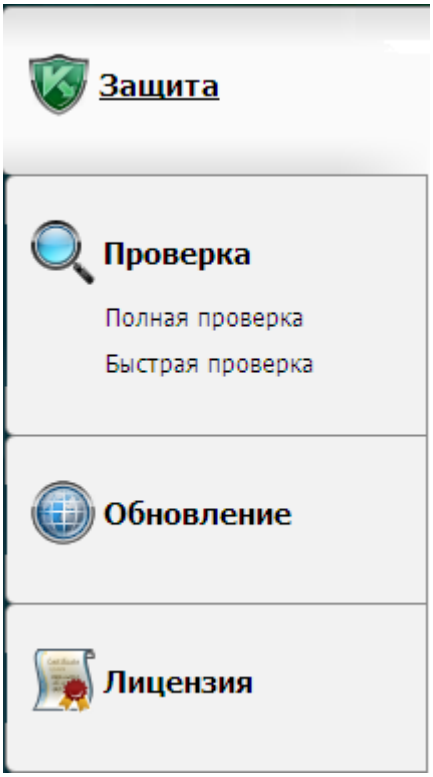


Рисунок 5. Левая часть главного окна

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

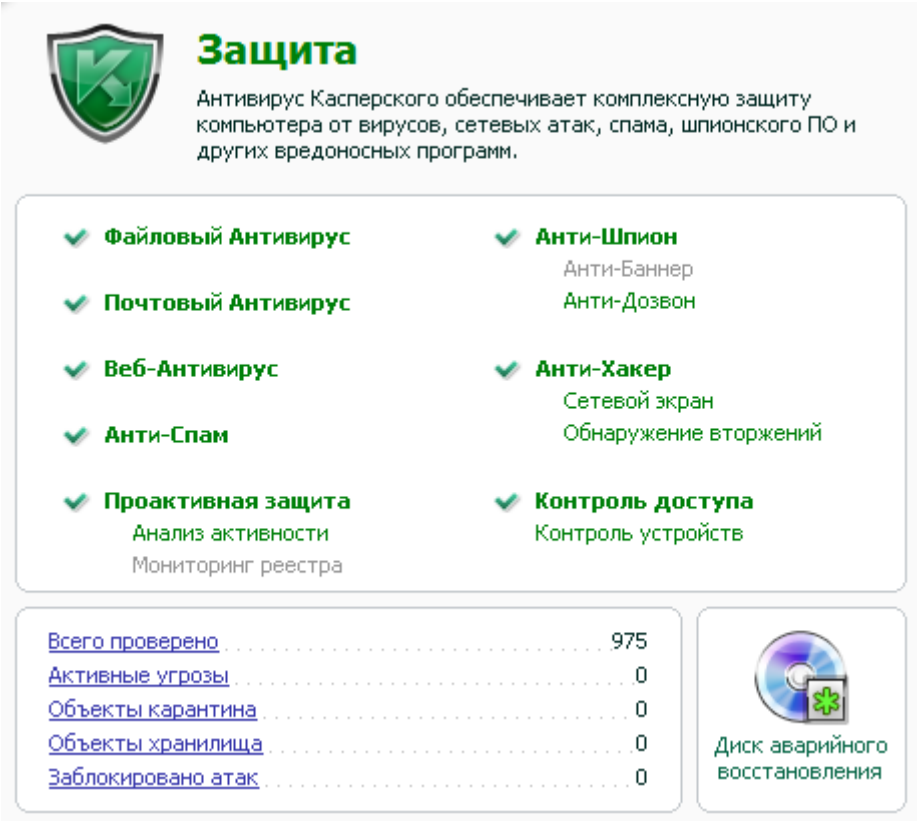


Рисунок 6. Правая часть главного окна

Также вы можете воспользоваться:

- кнопкой **Настройка** для перехода к окну настройки параметров (см. стр. 150) программы;
- ссылкой **Справка** для перехода к справочной системе Антивируса Касперского;
- кнопкой **Обнаружено** для перехода к работе с файлами данных (см. стр. 171) программы;
- кнопкой **Отчеты** для перехода к отчетам о работе компонентов (см. стр. 172) программы;
- ссылкой **Поддержка** для перехода к окнам с информацией о системе и ссылкам на информационные ресурсы «Лаборатории Касперского» (см. стр. 39) (сайт Службы технической поддержки, форум).

Уведомления

При возникновении событий в процессе работы Антивируса Касперского на экран выводятся специальные уведомления – всплывающие сообщения над значком программы 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 Анти-Хакера. Информационные уведомления имеют зеленый цвет.

См. также

Виды уведомлений 192

Окно настройки параметров программы

Окно настройки параметров Антивируса Касперского можно открыть из главного окна или контекстного меню. Для этого нажмите на кнопку **Настройка** в верхней части главного окна либо выберите одноименный пункт в контекстном меню программы.

Окно настройки состоит из двух частей:

- левая часть окна обеспечивает доступ к компонентам Антивируса Касперского, 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 программы 150

АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА

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 следующими 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 программ).

Чтобы изменить параметры работы Файлового Антивируса, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В этом разделе

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 были добавлены или изменены 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:

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

- В результате анализа возможны следующие варианты поведения Антивируса Касперского:

  a. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл, помещает его копию в *резервное хранилище* и пытается провести лечение. В результате успешного лечения файл становится доступным для работы. Если же лечение провести не удалось, файл удаляется.

b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной уверенности в этом 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 программа 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

Антивирусная защита файловой системы компьютера.....47

Изменение уровня безопасности

Под уровнем безопасности подразумевается предустановленный набор параметров Файлового Антивируса. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, вы принимаете самостоятельно, в зависимости от условий работы и сложившейся ситуации.

- Если вероятность заражения компьютера очень высока, необходимо выбрать высокий уровень безопасности.
- Рекомендуемый уровень обеспечивает баланс между производительностью и безопасностью и подходит для большинства случаев.
- При работе в защищенной среде (например, в корпоративной сети с централизованным обеспечением безопасности), а также в случае работы с ресурсоемкими программами следует установить низкий уровень безопасности.

Перед включением низкого уровня безопасности рекомендуется провести полную проверку компьютера с высоким уровнем.

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы 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 Файлового Антивируса, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне 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 файла на вирусы Антивирус Касперского находит зараженные или возможно зараженные объекты, дальнейшие операции Файлового Антивируса зависят от статуса объекта и выбранного действия.

По умолчанию все зараженные файлы подвергаются лечению, а все возможно зараженные – помещаются на карантин.

Все возможные действия приведены в таблице ниже.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
Запросить действие	Файловый Антивирус выдает на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным объектом заражен/возможно заражен файл, и предлагает на выбор одно из дальнейших действий. В зависимости от статуса объекта действия могут быть разными.
Заблокировать доступ	Файловый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Заблокировать доступ ☑ **Лечить**	Файловый Антивирус блокирует доступ к объекту и пытается его лечить. Если объект удалось вылечить, он предоставляется для работы. Если вылечить объект не удалось, он либо блокируется (если вылечить объект невозможно), либо ему присваивается статус *возможно зараженный* (если объект считается подозрительным), и он помещается на карантин. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Заблокировать доступ ☑ **Лечить** ☑ **Удалить, если лечение невозможно**	Файловый Антивирус блокирует доступ к объекту и пытается его лечить. Если объект удалось вылечить, он предоставляется для работы. Если вылечить объект не удалось, он удаляется. При этом копия объекта сохраняется в резервном хранилище.
Заблокировать доступ ☐ **Лечить** ☑ **Удалить**	Файловый Антивирус блокирует доступ к объекту и удаляет его.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне выберите нужное действие.

Формирование области защиты

Под областью защиты подразумевается не только местоположение проверяемых объектов, но и тип файлов, которые следует проверять. По умолчанию Антивирус Касперского 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 свой компьютер риску быть зараженным.

При выборе типа файлов следует помнить следующее:

- Существует ряд форматов файлов, для которых вероятность внедрения в них вредоносного кода и его последующей активации достаточно низка (например, *txt*). Существуют также 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*, тогда как на самом деле это будет исполняемый файл, переименованный в *txt*-файл. Если выбран параметр **Файлы, проверяемые по расширению**, такой файл в процессе проверки будет пропущен. 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.

Указывая тип проверяемых файлов, вы определяете, файлы какого формата, размера и на каких дисках будут проверяться на присутствие вирусов при открытии, исполнении и сохранении.

Для простоты настройки все файлы разделены на две группы: *простые* и *составные*. Простые файлы не содержат в себе каких-либо объектов (например, txt-файл). Составные объекты могут включать несколько объектов, каждый из которых также может иметь несколько вложений. Примерами таких объектов могут служить архивы, файлы, содержащие в себе макросы, таблицы, письма с вложениями и т. д.

Помните, что Файловый Антивирус будет проверять на присутствие вирусов только те файлы, которые включены в сформированную область защиты. Файлы, не входящие в данную область, будут доступны для работы без проверки. Это повышает риск заражения компьютера!

Чтобы изменить список проверяемых объектов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** в разделе **Область защиты** нажмите на кнопку **Добавить**.

6. В окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**.

7. Чтобы исключить какой-либо объект из списка проверки, снимите флажок рядом с ним.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.

4. В открывшемся окне нажмите на кнопку **Настройка**.

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. Антивирус Касперского сравнивает найденный объект с записями в базах, в результате чего делается однозначный вывод о том, 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 заключается 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 еще до того, как их активность станет известна вирусным аналитикам.

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 установленный 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 программы.

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

3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.

4. В открывшемся окне нажмите на кнопку **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 Антивируса Касперского, 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 программы.

2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Производительность** установите флажок **Проверять только новые и измененные файлы**.

Проверка составных файлов

Распространенная практика сокрытия вирусов предусматривает 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. Чтобы обезопасить свой компьютер от исполнения вредоносного кода и в то же время увеличить скорость проверки, отключите проверку архивов и включите проверку файлов данных типов.

Если файл, содержащий OLE-объект, представляет собой архив, он будет проверен при распаковке. Вы можете включить проверку архивов, чтобы проверять файлы, содержащие OLE-объекты, которые находятся в архиве, до его распаковки. Однако, это приведет к снижению скорости проверки.

По умолчанию Антивирус Касперского проверяет только вложенные OLE-объекты.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** установите флажки рядом с теми типами составных файлов, которые будут проверяться программой.

Проверка составных файлов большого размера

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

Вы можете снизить время доступа к составным файлам, отключив распаковку файлов, размер которых больше заданного. Проверка файлов при извлечении из архивов будет производится всегда.

- *Чтобы программа распаковывала файлы больших размеров в фоновом режиме, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **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 программа не распаковывала составные файлы большого размера, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.

4. В открывшемся окне нажмите на кнопку **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.

Изменение режима проверки

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

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

3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.

4. В открывшемся окне нажмите на кнопку **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 программы, дату предыдущей проверки объекта, а также изменение параметров проверки.

  Например, у вас есть файл архива, которому по результатам проверки программой был присвоен статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен, и если не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили базы программы, архив будет проверен повторно.

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

- **iSwift**. Технология представляет собой развитие технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

Чтобы изменить технологию проверки объектов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **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. Чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, можно настроить отключение компонента в определенное время.

Чтобы настроить расписание приостановки работы компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **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**).

Приостановка работы компонента: формирование списка программ

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

Настройка отключения Файлового Антивируса при конфликте с определенными программами – 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 Антивируса Касперского с программами, установленными на вашем компьютере.

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

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

Восстановление параметров защиты по умолчанию

Настраивая работу Файлового Антивируса, вы всегда можете вернуться к рекомендуемым параметрам его работы. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Если при настройке параметров Файлового Антивируса вы изменяли список объектов, включенных в область защиты, то при восстановлении первоначальных настроек вам будет предложено сохранить данный список для дальнейшего использования.

Чтобы восстановить параметры защиты по умолчанию, а также сохранить измененный список объектов, включенных в область защиты, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **По умолчанию**.
5. В открывшемся окне **Восстановление параметров** установите флажок **Область защиты**.

Статистика защиты файлов

Все операции, производимые Файловым Антивирусом, фиксируются в специальном отчете, где вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на закладках:

- Все опасные объекты, обнаруженные в процессе защиты файловой системы, перечислены на закладке *Обнаружено*. Здесь приводится полный путь к местоположению каждого объекта и статус, присвоенный объекту Файловым Антивирусом. Если удалось точно установить, какой вредоносной программой поражен объект, ему присваивается соответствующий статус: например, *вирус*, *троянская программа* и т. д. Если тип вредоносного воздействия точно установить невозможно, объекту присваивается статус *подозрительный*. Рядом со статусом также указывается выполненное над объектом действие (обнаружен, не найден, вылечен).
- Полный список событий, возникших в работе Файлового Антивируса, ведется на закладке *События*. События могут иметь следующие статусы:
  - *информационное событие* (например: объект не обработан: пропущен по типу);

- *внимание* (например: обнаружен вирус);
- *примечание* (например: архив защищен паролем).

Как правило, информационные сообщения носят справочный характер и не представляют особого интереса. Вы можете отключить просмотр информационных сообщений. Для этого снимите флажок **Показывать все события**.

- *Статистика* проверки приводится на соответствующей закладке. Здесь указывается общее количество проверенных объектов, а затем в специальных графах отдельно отражено, сколько объектов из общего числа проверенных являются архивами, сколько из них опасных объектов, сколько вылеченных, сколько помещенных на карантин и т. д.
- *Параметры*, в соответствии с которыми работает Файловый Антивирус, приводятся на одноименной закладке. Чтобы быстро перейти к настройке компонента, воспользуйтесь ссылкой **Изменить параметры**.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Файловый Антивирус** выберите пункт **Отчет**.

Отложенное лечение объектов

Если в качестве действия над вредоносными объектами вы выбрали **Заблокировать доступ**, объекты не будут подвергаться лечению, и доступ к ним будет закрыт.

Если в качестве действия выбрано

Заблокировать доступ

Лечить

то все не вылеченные объекты также будут заблокированы.

Чтобы вновь получить доступ к заблокированным объектам, необходимо предварительно попытаться вылечить их. Если объект удастся вылечить, он будет доступен для работы. Если вылечить объект нельзя, вам на выбор будет предложено *удалить* его или *пропустить*. В последнем случае доступ к файлу будет предоставлен. Однако это значительно повышает риск заражения компьютера. Настоятельно не рекомендуется пропускать вредоносные объекты.

Чтобы получить доступ к заблокированным объектам с целью их лечения, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Активные угрозы** выберите интересующие вас объекты и нажмите на ссылку **Лечить все**.

АНТИВИРУСНАЯ 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 и NNTP. Также компонент проверяет трафик интернет-пейджеров ICQ и MSN.

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 самостоятельно настраивать параметры работы Почтового Антивируса. В большинстве случаев достаточно выбрать другой уровень безопасности.

Если Почтовый Антивирус был по каким-либо причинам отключен, то соединения, установленные с почтовым сервером до его включения, не будут контролироваться. Также не будет контролироваться трафик программ для быстрого обмена сообщениями (см. стр. 62), если его проверка была отключена. Следует перезапустить программу сразу после включения проверки трафика или запуска Почтового Антивируса.

Чтобы изменить параметры работы Почтового Антивируса, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В этом разделе

Алгоритм работы компонента

Почтовый Антивирус запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения, пересылаемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP, а также через защищенные соединения (SSL) по протоколам POP3 и IMAP.

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

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 них опасных объектов. Распознавание вредоносных объектов происходит на основании баз, используемых в работе программы, 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, помещает копию зараженного объекта в *резервное хранилище* 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 программой.

- Если тело или вложение письма содержит код, похожий на вредоносный, но стопроцентной уверенности в этом нет, подозрительная часть письма помещается в специальное хранилище – *карантин*.

- Если вредоносного кода в письме не обнаружено, 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. 63), позволяющий производить более тонкую настройку проверки почты.

Если вы используете почтовую программу The Bat!, программа может использоваться наряду с другими антивирусными программами. При этом правила обработки почтового трафика (см. раздел «Проверка почты плагином в The Bat!» на стр. 63) настраиваются непосредственно в программе The Bat! и превалируют над параметрами защиты почты программы.

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.

См. также

Антивирусная защита почты.....58

Изменение уровня безопасности

Под уровнем безопасности подразумевается предустановленный набор параметров Почтового Антивируса. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, пользователь принимает самостоятельно, в зависимости от условий работы и сложившейся ситуации.

- Если вы работаете в опасной среде, вам подходит высокий уровень безопасности почты. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из 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.

Если ни один из предложенных уровней не отвечает вашим требованиям, вы можете настроить параметры работы (см. раздел «Антивирусная защита почты» на стр. 58) 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне 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 (например, *вирус*, *троянская программа*).
- *возможно зараженный*, когда в результате проверки невозможно однозначно определить, заражен объект или нет. Это означает, что в письме или его объекте обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

По умолчанию при обнаружении опасного или возможно зараженного объекта Почтовый Антивирус выдает на экран предупреждение и предлагает на выбор несколько действий над объектом.

Все возможные действия приведены в таблице ниже.

Если в качестве действия вы выбрали	При обнаружении опасного объекта
Запросить действие	Почтовый Антивирус выдаст на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным объектом заражен (возможно заражен) объект, и предложит на выбор одно из дальнейших действий.
Заблокировать доступ	Почтовый Антивирус блокирует доступ к объекту. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Заблокировать доступ **Лечить**	Почтовый Антивирус блокирует доступ к объекту и пытается его лечить. Если объект удалось вылечить, он предоставляется для работы. Если вылечить объект не удалось, он помещается на карантин. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Заблокировать доступ **Лечить** **Удалить, если лечение невозможно**	Почтовый Антивирус блокирует доступ к объекту и пытается его лечить. Если объект удалось вылечить, он предоставляется для работы. Если вылечить объект не удалось, он удаляется. При этом копия объекта сохраняется в резервном хранилище. Объект со статусом *возможно заражен* будет помещен на карантин.
Заблокировать доступ **Лечить** **Удалить**	При обнаружении зараженного или возможно зараженного объекта Почтовый Антивирус удалит его без предварительного уведомления пользователя.

Перед лечением или удалением объекта Почтовый Антивирус формирует его резервную копию и помещает ее в резервное хранилище на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.

4. В открывшемся окне выберите нужное действие.

Формирование области защиты

Под областью защиты подразумевается тип сообщений, которые следует проверять. По умолчанию Почтовый Антивирус проверяет как входящие, так и исходящие сообщения. При выборе проверки только входящих сообщений следует в самом начале работы с программой 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 также относятся:

- параметры интеграции Почтового Антивируса в систему. По умолчанию Почтовый Антивирус интегрируется в почтовые клиенты Microsoft Office Outlook и The Bat!.
- проверяемые протоколы. Почтовый Антивирус проверяет почтовые сообщения по протоколам POP3, SMTP, IMAP и NNTP. Также компонент проверяет трафик интернет-пейджеров ICQ и MSN.

Чтобы отключить проверку исходящей почты, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** задайте нужные значения параметров.

Чтобы задать параметры интеграции и проверяемые протоколы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Встраивание в систему** установите необходимые флажки.

Выбор метода проверки

Под методами проверки подразумевается проверка ссылок, содержащихся в почтовых сообщениях, на принадлежность к списку подозрительных веб-адресов и / или к списку фишинговых веб-адресов.

Проверка ссылок на принадлежность к списку фишинговых адресов позволяет избежать фишинг-атак, которые, как правило, представляют собой почтовые сообщения якобы от финансовых структур, содержащие ссылки на их 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 может быть 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.

Проверка ссылок на принадлежность к списку подозрительных веб-адресов позволяет отследить веб-сайты, которые находятся в «черном» списке. Список формируется специалистами «Лаборатории Касперского» и входит в поставку программы.

- *Чтобы проверять ссылки из почтовых сообщений по базе подозрительных адресов, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
  4. В открывшемся окне нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Общие** в блоке **Методы проверки** установите флажок **Проверять ссылки по базе подозрительных веб-адресов**.

- *Чтобы проверять ссылки из почтовых сообщений по базе фишинговых адресов, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
  4. В открывшемся окне нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Общие** в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

Проверка почты в Microsoft Office Outlook

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

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

Модуль расширения реализован в качестве специальной закладки **Почтовый Антивирус**, 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 **Почтовый Антивирус** 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.

Если отключена проверка потока почтовых сообщений по протоколам POP3/SMTP/NNTP/IMAP, то параметры Почтового Антивируса, определяющие, следует или нет проверять 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 программа 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 вылечить объект невозможно, он 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!, если отключена проверка потока почтовых сообщений по протоколам POP3/SMTP/NNTP/IMAP. Если проверка включена, то почтовые сообщения отмечаются.

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, объект с достаточной долей вероятности будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны еще до того, как их активность станет известна вирусным аналитикам. По умолчанию эвристический анализ включен.

Дополнительно вы можете выбрать уровень детализации проверки: **поверхностный**, **средний** или **глубокий**. Для этого передвиньте ползунок в выбранную позицию.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **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 Антивируса Касперского. Вы можете включать или отключать проверку вложенных архивов, а также ограничивать максимальный размер проверяемых объектов.

Чтобы настроить параметры проверки составных файлов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Производительность** выберите режим проверки составных файлов.

Фильтрация вложений

Вы можете настроить условия фильтрации вложенных в почтовое сообщение объектов. Использование фильтра обеспечит дополнительную безопасность вашего компьютера, поскольку вредоносные программы чаще всего распространяются через почту в виде вложенных файлов. Переименование или удаление вложений определенного типа позволит защитить ваш компьютер, например, от 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В раскрывшемся меню нажмите на кнопку **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 кнопку **Добавить** и в открывшемся окне **Маска имени файла** введите необходимые данные.

Восстановление параметров защиты почты по умолчанию

Настраивая работу Почтового Антивируса, вы всегда можете вернуться к рекомендуемым параметрам его работы. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **По умолчанию**.

Статистика защиты почты

Все операции, производимые Почтовым Антивирусом, фиксируются в специальном отчете, который предоставляет вам детальный отчет о работе компонента, сгруппированный на закладках:

- Все опасные объекты, обнаруженные Почтовым Антивирусом в ваших письмах, перечислены на закладке *Обнаружено*. Для каждого объекта указывается его полное имя и статус, присвоенный программой при его проверке / обработке. Если удалось точно установить, какой вредоносной программой поражен объект, ему присваивается соответствующий статус: например, *вирус*, *троянская программа* и т. д. Если тип вредоносного воздействия точно установить невозможно, объекту присваивается статус *подозрительный*. Рядом со статусом также указывается действие, выполненное над объектом (обнаружен, не найден, вылечен).

  Чтобы данная закладка не содержала информации о вылеченных объектах почтовых сообщений, снимите флажок **Показывать вылеченные объекты**.

- Полный список событий, возникших в работе Почтового Антивируса, ведется на закладке *События*. События могут иметь следующие статусы:

  - *информационное событие* (например: объект не обработан: пропущен по типу);
  - *внимание* (например: обнаружен вирус);
  - *примечание* (например: архив защищен паролем).

  Как правило, информационные сообщения носят справочный характер и не представляют особого интереса. Вы можете отключить просмотр информационных сообщений. Для этого снимите флажок **Показывать все события**.

- *Статистика* проверки приводится на соответствующей закладке. Здесь приведено общее количество проверенных объектов почтовых сообщений, а затем в специальных графах отдельно указано, сколько объектов из общего числа проверенных являются архивами, сколько среди них опасных объектов, сколько вылеченных, сколько помещенных на карантин и т. д.

- *Параметры*, в соответствии с которыми работает Почтовый Антивирус, приводятся на одноименной закладке. Чтобы быстро перейти к настройке компонента, воспользуйтесь ссылкой **Изменить параметры**.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Почтовый Антивирус** выберите пункт **Отчет**.

ВЕБ-ЗАЩИТА

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 просматриваете какую-либо веб-страницу.

Для обеспечения безопасности работы в интернете Антивирус Касперского 6.0 для Windows Workstations MP4 включает специальный 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 (см. раздел «Формирование списка контролируемых портов» на стр. 175). Список портов, которые чаще всего используются для передачи почты и HTTP-трафика, включен в комплект поставки Антивируса Касперского. 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, выходя в сеть с помощью модема, рекомендуется использовать для защиты работы в интернете Сетевой экран. Если же ваш компьютер работает в сети, защищенной сетевым экраном или фильтрами HTTP-трафика, Сетевой экран обеспечит дополнительную степень безопасности.

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 самостоятельно настраивать параметры работы Веб-Антивируса. В большинстве случаев достаточно выбрать другой уровень безопасности.

Если Веб-Антивирус был по каким-либо причинам отключен, то соединения, установленные до его включения, не будут контролироваться. Следует перезапустить интернет-браузер сразу после запуска Веб-Антивируса.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В этом разделе

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 пользователь или некоторая программа обращаются по протоколу HTTP, перехватывается и анализируется Веб-Антивирусом на присутствие вредоносного кода. Распознавание вредоносных объектов происходит на основании баз, используемых в работе программы, 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 доступными 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 об этом 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 программы. 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

Веб-защита.....68

Изменение уровня безопасности HTTP-трафика

Под уровнем безопасности подразумевается предустановленный набор параметров Веб-Антивируса. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, вы принимаете самостоятельно, в зависимости от условий работы и сложившейся ситуации:

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

Если ни один из предложенных уровней не отвечает вашим требованиям, можно настроить параметры работы 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне 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.

Рассмотрим подробнее возможные варианты обработки опасных объектов HTTP-трафика.

Если в качестве действия вы выбрали	При обнаружении опасного объекта в HTTP-трафике
Запросить действие	Веб-Антивирус выдаст на экран предупреждающее сообщение, содержащее информацию о том, каким вредоносным кодом заражен объект, и предложит на выбор одно из дальнейших действий.
Заблокировать	Веб-Антивирус заблокирует доступ к объекту и выведет на экран окно уведомления о блокировке. Аналогичная информация будет зафиксирована в отчете.
Разрешить	Веб-Антивирус разрешает доступ к опасному объекту. Информация об этом зафиксируется в отчете.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне выберите нужное действие.

Формирование области защиты

Под областью защиты подразумевается список доверенных адресов, информация с которых не будет анализироваться компонентом на присутствие опасных объектов. Возможность сформировать такой список может быть использована в том случае, если Веб-Антивирус препятствует загрузке некоторого файла, блокируя попытки его скачать.

Чтобы сформировать список доверенных адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Веб-Антивирус** в блоке **Доверенные адреса** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Маска адреса (URL)** введите доверенный адрес (или его маску).

Выбор метода проверки

Под методами проверки подразумевается проверка ссылок на принадлежность к списку подозрительных адресов и / или к списку фишинговых адресов.

Проверка ссылок на принадлежность к списку фишинговых адресов позволяет избежать фишинг-атак, которые, как правило, представляют собой почтовые сообщения от якобы финансовых структур, содержащие ссылки на их 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.

Поскольку ссылка на фишинг-сайт может быть направлена вам не только письмом (см. раздел «Выбор метода проверки» на стр. 62), но и другими доступными для этого способами, например, в тексте ICQ-сообщения,

компонент Веб-Антивирус отслеживает попытки открытия фишинг-сайта на уровне проверки HTTP-трафика и блокирует его.

Проверка ссылок на принадлежность к списку подозрительных веб-адресов позволяет отследить веб-сайты, которые находят в «черном» списке. Список формируется специалистами «Лаборатории Касперского» и входит в поставку программы.

Чтобы проверять ссылки по базе подозрительных веб-адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Веб-Антивирус** в блоке **Методы проверки** установите флажок **Проверять ссылки по базе подозрительных веб- адресов**.

Чтобы проверять ссылки по базе фишинговых адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Веб-Антивирус** в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

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 высокой долей вероятности данный объект будет признан вредоносным или подозрительным. Следовательно, новые угрозы будут распознаны еще до того, как их активность станет известна вирусным аналитикам. По умолчанию эвристический анализ включен.

Программа уведомит вас об обнаружении вредоносного объекта в сообщении. На уведомление следует отреагировать выбором действия.

Дополнительно вы можете выбрать уровень детализации проверки: **поверхностный**, **средний** или **глубокий**. Для этого передвиньте ползунок в выбранную позицию.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Веб-Антивирус** в блоке **Методы проверки** установите 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 при копировании и обработке больших объектов может вызывать сложности, 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 снижая уровня 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, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Веб-Антивирус** в блоке **Оптимизация проверки** установите флажок **Ограничить время кеширования фрагментов** и задайте время (в секундах) в поле рядом.

Восстановление параметров веб-защиты по умолчанию

Настраивая работу Веб-Антивируса, вы всегда можете вернуться к рекомендуемым параметрам его работы. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы восстановить параметры Веб-Антивируса по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **По умолчанию**.

Статистика веб-защиты

Общая информация о работе Веб-Антивируса фиксируется в специальном отчете, где вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на закладках:

- Все опасные объекты, обнаруженные Веб-Антивирусом в HTTP-трафике, приведены на закладке *Обнаружено*. Здесь приводятся название объекта и имя опасной программы. Чтобы данная закладка не содержала информации о вылеченных объектах HTTP-протокола, снимите флажок **Показывать вылеченные объекты**.

- Полный список событий, возникших в работе Веб-Антивируса, ведется на закладке *События*. События могут быть важными и информационными. Как правило, информационные события носят справочный характер и не представляют особого интереса. Вы можете отключить просмотр таких событий. Для этого снимите флажок **Показывать все события**.

- *Параметры*, в соответствии с которыми работает Веб-Антивирус, приводятся на одноименной закладке. Чтобы быстро перейти к настройке компонента, воспользуйтесь ссылкой **Изменить параметры**.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Веб-Антивирус** выберите пункт **Отчет**.

ПРОАКТИВНАЯ ЗАЩИТА ВАШЕГО КОМПЬЮТЕРА

Антивирус Касперского 6.0 для Windows Workstations MP4 защищает не только от известных, но и от новых угроз, информация о которых отсутствует в базах программы. Это обеспечивает 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. За счет чего это достигается? В отличие от реактивных технологий, где анализ выполняется на основании записей баз программы, превентивные технологии распознают новую угрозу по последовательности действий, выполняемых программой. В комплект поставки Антивируса Касперского включен набор критериев, позволяющих определять, насколько активность той или иной программы опасна. Если в результате анализа активности последовательность действий какой-либо программы вызывает подозрение, Антивирус Касперского применяет действие, заданное правилом для активности подобного рода.

Опасная активность определяется по совокупности действий программы. К опасным действиям относятся:

- изменения файловой системы;
- встраивание модулей в другие процессы;
- скрытие процессов в системе;
- изменение определенных ключей системного реестра Microsoft Windows.

Проактивная защита осуществляется в строгом соответствии с параметрами, определяющими:

- *Подвергается ли контролю активность программ на вашем компьютере*. Такой режим работы Проактивной защиты осуществляет модуль **Анализ активности**. По умолчанию режим включен, что обеспечивает строгий анализ действий любой программы, запускаемой на компьютере.
- *Обеспечивается ли контроль изменений системного реестра*. Такой режим работы Проактивной защиты осуществляет модуль **Мониторинг системного реестра**. По умолчанию работа модуля отключена, а значит, Антивирус Касперского не анализирует попытки внести изменения в контролируемые ключи системного реестра Microsoft Windows.

Чтобы изменить параметры работы Проактивной защитой, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В ЭТОМ РАЗДЕЛЕ

Алгоритм работы компонента

Превентивные технологии, на которых построена Проактивная защита Антивируса Касперского, распознают новую угрозу на вашем компьютере по последовательности действий, выполняемых программой. В комплект поставки Антивируса Касперского включен набор критериев, позволяющих определять, насколько опасна активность той или иной программы. Если в результате анализа активности последовательность действий какой-либо программы вызывает подозрение, Антивирус Касперского применяет действие, заданное правилом для опасной активности.

Рассмотрим алгоритм работы Проактивной защиты.

1. Сразу после запуска компьютера Проактивная защита анализирует следующие аспекты:

   - *Действия каждой запускаемой на компьютере программы*. История выполняемых действий и их последовательность фиксируется и сравнивается с последовательностью, характерной для опасной активности (база видов опасной активности включена в комплект поставки программы и обновляется вместе с базами программы).

   - *Каждую попытку изменения системного реестра* (удаление, добавление ключей системного реестра, ввод значений для ключей в недопустимом формате, препятствующем их просмотру и редактированию, и т. д.).

2. Анализ производится на основании разрешающих и запрещающих правил Проактивной защиты.

3. В результате анализа возможны следующие варианты поведения:

   - Если активность удовлетворяет условиям разрешающего правила Проактивной защиты либо не подпадает ни под одно запрещающее правило, она не блокируется.

   - Если активность описана в запрещающем правиле, дальнейшая последовательность действий компонента соответствует инструкциям, указанным в правиле. Обычно такая активность блокируется. На экран выводится уведомление, где указывается программа, тип ее активности, история выполненных действий. Вам нужно самостоятельно принять решение – запретить или разрешить такую активность. Вы можете создать правило для такой активности и отменить выполненные действия в системе.

См. также

Проактивная защита вашего компьютера 75

Анализ активности

Активность программ на вашем компьютере контролируется компонентом Антивируса Касперского **Анализ активности**. В состав программы входит набор описаний событий, которые могут трактоваться как опасные. Для каждого такого события создано правило. Если активность какой-либо программы классифицируется как опасное событие, Проактивная защита будет следовать инструкциям, указанным в правиле для такого события.

См. также

Использование списка опасной активности 77

Изменение правила контроля опасной активности 77

Контроль системных учетных записей 78

События Проактивной защиты 78

Использование списка опасной активности

Обратите внимание, что настройка контроля активности в программе, установленной на компьютере под управлением операционных систем Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista или Microsoft Windows Vista x64, отличается от аналогичных действий в программе, установленной на компьютере под управлением других операционных систем.

Особенности настройки контроля активности программ под Microsoft Windows XP

Активность программ на вашем компьютере контролируется Антивирусом Касперского. Проактивная защита реагирует на определенную последовательность действий какой-либо программы. К опасным последовательностям действий 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);
- попытки изменения файла HOSTS;
- попытки внедрения в другие процессы;
- появление процессов, перенаправляющих ввод / вывод данных;
- попытки отправки DNS-запросов.

Список опасной активности пополняется автоматически при обновлении Антивируса Касперского, и отредактировать его нельзя. Однако вы можете отказаться от контроля той или иной опасной активности.

Чтобы отказаться от контроля той или иной опасной активности, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Анализ активности программ** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Анализ активности** снимите флажок, установленный рядом с названием той активности, от контроля которой необходимо отказаться.

Особенности настройки контроля активности программ под Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64 или Microsoft Windows 7 x64

Если компьютер работает под управлением перечисленных выше операционных систем, будут контролироваться не все события, что связано с особенностями этих операционных систем.

Изменение правила контроля опасной активности

Список опасной активности пополняется автоматически при обновлении Антивируса Касперского, и отредактировать его нельзя. Вы можете:

- отказаться от контроля той или иной активности (см. стр. 77);

- изменить правило, в соответствии с которым Проактивная защита действует при обнаружении опасной активности;
- составить список исключений (см. стр. 154), перечислив программы, активность которых вы не считаете опасной.

Чтобы изменить правило, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Анализ активности программ** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Анализ активности** в блоке **События** выберите нужное событие, для которого необходимо изменить правило.
6. Для выбранного события, используя ссылки в блоке описания, задайте необходимые параметры правила:
   - нажмите на ссылку с установленным действием и в открывшемся окне **Выбор действия** выберите нужное действие из предложенных;
   - нажмите на ссылку с установленным временным интервалом (задается не для всех видов активности) и в открывшемся окне **Обнаружение скрытых процессов** задайте интервал, с которым будет проводиться проверка на обнаружение скрытых процессов;
   - нажмите на ссылку **Вкл. / Выкл.**, чтобы указать необходимость формирования отчета о выполненной операции.

Контроль системных учетных записей

Учетные записи регулируют доступ в систему, определяют пользователя и его рабочую среду, что предотвращает повреждение операционной системы или данных других пользователей. Системные процессы – это процессы, которые были запущены системной учетной записью.

Чтобы Антивирус Касперского, кроме пользовательских процессов, контролировал активность системных процессов, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Анализ активности программ** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Анализ активности** в блоке **Общие** установите флажок **Контролировать системные учетные записи**.

События Проактивной защиты

В данном разделе представлена информация о событиях Проактивной защиты, которые могут трактоваться как опасные. Обратите внимание, что не все события должны однозначно восприниматься как угроза. Некоторые из этих операций являются нормальным поведением программ, выполняющихся на компьютере, либо реакцией операционной системы на работу данных программ. Однако в некоторых случаях эти же события могут быть вызваны деятельностью злоумышленников либо вредоносных программ. Поэтому важно понимать, что срабатывание Проактивной защиты не всегда однозначно говорит о том, что обнаруженная активность

принадлежит вредоносной программе: это может быть и обычная программа, обладающая признаками поведения вредоносной.

Активность, характерная для P2P-червей / Активность, характерная для троянских программ

Червь – это самовоспроизводящаяся программа, распространяющаяся в компьютерных сетях. P2P-черви распространяются по типу «компьютер-компьютер» минуя централизованное управление. Как правило, распространение таких червей происходит через общие сетевые папки и съемные носители информации.

Троянская программа – это вредоносная программа, проникающая на компьютер под видом безвредной. Троянские программы помещаются злоумышленниками на открытые сетевые ресурсы, открытые для записи носители самого компьютера, на съемные носители информации, а также рассылаются с помощью служб обмена сообщениями (например, электронной почты) с целью их запуска на компьютере.

Активность, характерная для таких программ включает:

- действия, характерные для заражения и укрепления вредоносного объекта в системе;
- непосредственно вредоносные действия;
- действия, характерные для распространения вредоносного объекта.

Клавиатурные перехватчики

Клавиатурный перехватчик – это программа, перехватывающая все нажатия клавиш на клавиатуре. Вредоносная программа такого типа может отправлять информацию, набираемую на клавиатуре (логины, пароли, номера кредитных карт) злоумышленнику. Однако перехват нажатий клавиш может использоваться и обычными программами. Примером таких программ могут служить игровые программы, которые при работе в полноэкранном режиме, вынуждены перехватывать данные, вводимые с клавиатуры, чтобы узнать какие клавиши нажимает пользователь. Также зачастую перехват нажатий клавиш применяется для вызова функций программы из другой программы с помощью «горячих клавиш».

Скрытая установка драйвера

Скрытая установка драйвера – это процесс установки вредоносной программой собственного драйвера с тем, чтобы получить доступ к операционной системе на низком уровне, что позволит скрыть присутствие вредоносной программы в системе и затруднит ее удаление. Процесс скрытой установки можно обнаружить обычными средствами (например, Диспетчером задач Microsoft Windows), но, поскольку во время установки драйвера на экране нет стандартных окон установки, пользователю вряд ли придет в голову отслеживать процессы, происходящие в системе.

Однако, в некоторых случаях срабатывание Проактивной защиты может быть ложным. Например, большинство компьютерных игр в последнее время используют защиту от нелегального распространения и копирования. Для обеспечения данной цели они устанавливают на компьютере пользователя системные драйверы. Данная активность в некоторых случаях может быть классифицирована как «скрытая установка драйвера».

Изменение ядра операционной системы

Ядро операционной системы обеспечивает программам, работающим на компьютере, координированный доступ к ресурсам компьютера: процессору, памяти и внешнему аппаратному обеспечению. Некоторые вредоносные программы пытаются изменить логику работы ядра операционной системы перенаправляя вызовы из стандартных драйверов на себя. Получив таким образом доступ к операционной системе на низком уровне вредоносные программы пытаются скрыть свое присутствие и сделать тяжелым процесс своего удаления из системы.

Примером ложного срабатывания Проактивной защиты может служить реакция компонента на некоторые системы шифрования жестких дисков. Подобные системы для обеспечения максимальной защиты информации устанавливают в систему драйвер и внедряются в ядро операционной системы, чтобы перехватывать обращения к файлам на диске и производить операции шифрования и дешифрования.

Скрытый объект / Скрытый процесс

Скрытый процесс – это процесс, который нельзя обнаружить обычными средствами (Диспетчер задач Microsoft Windows, Process Explorer и др.). Rootkit (руткит, от англ. «root kit», то есть «набор для получения прав суперпользователя root») – программа или набор программ для скрытого контроля взломанной системы. Этот термин пришел из Unix.

В контексте операционной системы Microsoft Windows под rootkit принято подразумевать программу-маскировщик, которая внедряется в систему, перехватывает и искажает системные сообщения, содержащие информацию о запущенных в системах процессах, а также о содержимом папок на диске. Другими словами, rootkit работает аналогично прокси-серверу, пропуская через себя одну информацию и не пропуская или искажая другую. Кроме того, как правило, rootkit может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие программы-маскировщики устанавливают в систему свои драйверы и службы, которые, естественно, являются «невидимыми» как для средств управления системой, таких как Диспетчер задач или Process Explorer, так и для антивирусных программ.

Частным случаем скрытого процесса является активность, представляющая собой попытки создания скрытых процессов с отрицательными значениями идентификаторов (PID). PID – персональный идентификационный номер, который присваивается операционной системой запущенным процессам. PID является уникальным для каждого запущенного процесса и сохраняется одинаковым для каждого из процессов только в текущей сессии работы операционной системы. Если PID процесса имеет отрицательное значение, такой процесс является скрытым и его нельзя обнаружить обычными средствами.

Примером ложного срабатывания может быть срабатывание Проактивной защиты на игровые программы, защищающие свои процессы от хакерских утилит для обхода лицензии или нечестной игры.

Изменение файла HOSTS

Файл hosts – это один из важных системных файлов операционной системы Microsoft Windows. Он предназначен для перенаправления доступа к интернет-ресурсам за счет преобразования URL-адресов в IP-адреса не на DNS-серверах, а непосредственно на локальном компьютере. Файл hosts – это обычный текстовый файл, каждая строка которого определяет соответствие символьного имени (URL) сервера и его IP-адреса.

Вредоносные программы часто используют данный файл для переопределения адресов серверов обновлений антивирусных программ, чтобы заблокировать возможность обновления и предотвратить обнаружение вредоносной программы сигнатурным методом, а также для других целей.

Перенаправление ввода-вывода

Суть уязвимости заключается в запуске командной строки с перенаправленным вводом/выводом (обычно в сеть), что, как правило, используется для получения удаленного доступа к компьютеру.

Вредоносный объект пытается получить доступ к командной строке на компьютере-жертве, из которой будут исполняться дальнейшие команды. Обычно доступ бывает получен в результате удаленной атаки и запуска скрипта, использующего данную уязвимость. Скрипт запускает интерпретатор командной строки с компьютера, подключенный по TCP-соединению. В результате злоумышленник может удаленно управлять системой.

Внедрение в процесс / Внедрение во все процессы

Существует множество разновидностей вредоносных программ, которые маскируются под исполняемые файлы, библиотеки или модули расширения известных программ и внедряются в стандартные процессы. Таким образом, можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит программе, которой разрешен доступ в интернет.

Внедрение в другие процессы широко используется троянскими программами. Однако такая активность характерна также для некоторых безобидных программ, пакетов обновлений и программ установки. Например, программы-переводчики внедряются в другие процессы, чтобы отслеживать нажатие «горячих клавиш».

Подозрительное обращение к реестру

Вредоносные программы модифицируют реестр с целью регистрации себя для автоматического запуска при старте операционной системы, подмены стартовой страницы Microsoft Internet Explorer и других

деструктивных действий. Однако следует помнить, что доступ к системному реестру может осуществляться и обычными программами. Например, обычные программы используют возможность создания и использования скрытых ключей реестра для сокрытия собственной информации от пользователя (в том числе информации о лицензии).

Вредоносные программы создают «скрытые» ключи в реестре, не отображаемые обычными программами (типа regedit). Создаются ключи с некорректными именами. Это делается для того, чтобы редактор реестра не смог отобразить эти значения, в результате чего диагностика на присутствие в системе вредоносного программного обеспечения затрудняется.

Отправка данных посредством доверенных программ

Существует множество разновидностей вредоносных программ, которые маскируются под исполняемые файлы, библиотеки или модули расширения известных программ и внедряются в стандартные процессы. Таким образом, можно, например, организовать утечку данных с компьютера пользователя. Сетевой трафик, инициированный вредоносным кодом, будет свободно пропускаться сетевыми экранами, поскольку, с точки зрения сетевого экрана, этот трафик принадлежит программе, которой разрешен доступ в интернет.

Подозрительная активность в системе

Данный аспект подразумевает под собой обнаружение подозрительного поведения какого-либо конкретного процесса: изменение состояния самой операционной системы, например, прямой доступ к памяти или получение привилегий отладчика. Перехваченная активность не является характерной для большинства программ, но в тоже время является опасной. Поэтому такая активность классифицируется как подозрительная.

Отправка DNS-запросов

DNS-сервер предназначен для ответов на DNS-запросы по соответствующему протоколу. Если в базе данных локального DNS-сервера не содержится соответствующей DNS-запросу записи, то запрос передается дальше, пока не будет достигнут сервер, хранящий нужную информацию. Поскольку DNS-запросы пропускаются большинством систем защиты без проверки, в содержимом DNS-пакета могут быть переданы дополнительные сведения, содержащие персональные данные пользователя. Злоумышленник, контролирующий один из DNS-серверов, обрабатывающих такие DNS-запросы, имеет возможность получить эту информацию.

Попытка доступа к защищенному хранилищу

Процесс пытается получить доступ к защищенному хранилищу операционной системы с персональными данными и паролями пользователя.

Мониторинг системного реестра

Одна из целей многих вредоносных программ – изменение реестра операционной системы на вашем компьютере. Это могут быть как безобидные программы-шутки, так и более опасные вредоносные программы, представляющие серьезную угрозу вашему компьютеру.

Так, например, вредоносные программы могут прописаться в ключ реестра, отвечающий за автоматический запуск программ. В результате сразу после запуска операционной системы будут автоматически запущены вредоносные программы.

Специальный модуль Проактивной защиты – **Мониторинг системного реестра** – отслеживает изменения объектов системного реестра.

См. также

Управление списком правил контроля системного реестра 82

Создание группы контролируемых объектов системного реестра 82

Управление списком правил контроля системного реестра

Список правил, регламентирующих работу с объектами реестра, уже сформирован специалистами «Лаборатории Касперского» и включен в комплект поставки программы. Операции с объектами реестра распределены по логическим группам, таким как *System Security*, *Internet Security* и т. д. Каждая такая группа включает объекты системного реестра и правила работы с ними. Данный список обновляется вместе с обновлением программы.

Каждая группа правил имеет приоритет выполнения, который вы можете повышать или понижать. Чем выше в списке расположена группа, тем выше приоритет ее выполнения. Если один и тот же объект реестра попадает в несколько групп, в первую очередь к нему будет применено правило из группы с более высоким приоритетом.

- *Чтобы повысить или понизить приоритет выполнения для какого-либо правила, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: группы ключей реестра** воспользуйтесь кнопками **Вверх** / **Вниз**.

- *Чтобы отказаться от использования какой-либо группы правил, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: группы ключей реестра** снимите флажок рядом с именем группы. В этом случае группа правил останется в списке, но не будет использоваться. Удалять группу правил из списка не рекомендуется, поскольку они содержат список объектов системного реестра, наиболее часто используемые вредоносными программами.

Создание группы контролируемых объектов системного реестра

Существует возможность создавать собственные группы контролируемых объектов системного реестра.

- *Чтобы создать группу контролируемых объектов системного реестра, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: группы ключей реестра** нажмите на кнопку **Добавить**.

6. В открывшемся окне в поле **Имя группы** введите имя новой группы объектов системного реестра.

   На закладке **Ключи** сформируйте список объектов системного реестра, которые будут входить в контролируемую группу.

   На закладке **Правила** создайте для выбранных объектов реестра правило.

См. также

Выбор объектов реестра для создания правила

Создаваемая группа объектов должна содержать хотя бы один объект системного реестра.

Чтобы добавить объект системного реестра в список, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: группы ключей реестра** нажмите на кнопку **Добавить**.
6. В открывшемся окне на закладке **Ключи** нажмите на кнопку **Добавить**.
7. В открывшемся окне **Выбор пути в реестре** выполните следующие действия:
   a. выберите объект или группу объектов системного реестра, для которой вы хотите создать правило контроля;
   b. в поле **Значение** укажите значение объекта или маску группы объектов, к которым вы хотите применить правило;
   c. чтобы правило применялось ко всем вложенным ключам выбранного для правила объекта системного реестра, установите флажок **Включая вложенные ключи**.

Создание правила для контроля объектов реестра

Правило контроля объектов системного реестра состоит из определения:

- программа, к которой будет применено правило, если она произведет попытку обращения к системному реестру;
- реакции программы на попытку программы выполнить ту или иную операцию над объектами системного реестра.

Чтобы создать правило для выбранных объектов системного реестра, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.

3. В контекстном меню компонента **Проактивная защита** выберите пункт **Настройка**.

4. В открывшемся окне в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.

5. В открывшемся окне **Настройка: группы ключей реестра** нажмите на кнопку **Добавить**.

6. В открывшемся окне на закладке **Правила** нажмите на кнопку **Создать**. Обобщающее правило будет добавлено первым в список правил.

7. Выберите правило в списке и в нижней части закладки задайте параметры правила:

   - Укажите программу.

     По умолчанию правило создается для любой программы. Чтобы правило распространялось на конкретную программу, щелкните левой клавишей мыши по ссылке **любое**, она примет вид **выбранное**. Затем воспользуйтесь ссылкой **укажите программу**. Будет открыто контекстное меню, в котором вы можете из пункта **Обзор** перейти в стандартное окно выбора файлов, или из пункта **Программы** перейти к списку программ, работающих в данный момент, и выбрать нужное.

   - Определите реакцию Проактивной защиты на попытку выбранной программы выполнить операцию чтения, изменения и удаления объектов системного реестра.

     В качестве реакции может быть одно из следующих действий: **разрешить**, **запросить действие** и **запретить**. Щелкайте по ссылке с действием левой клавишей мыши, пока она не примет нужное вам значение.

   - Укажите необходимость формирования отчета о выполненной операции. Для этого воспользуйтесь ссылкой **протоколировать** / **не протоколировать**.

   Вы можете создать несколько правил и определить приоритет их выполнения с помощью кнопок **Вверх** и **Вниз**. Чем выше правило расположено в списке, тем выше его приоритет.

Статистика Проактивной защиты

Все операции, производимые Проактивной защитой, фиксируются в специальном отчете, где вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на следующих закладках:

- *Обнаружено* – на закладке собраны все объекты, отнесенные к рангу опасных.
- *События* – на закладке представлены события, имеющие отношения к контролю активности программ.
- *Реестр* – на закладке зафиксированы все операции, производимые в системном реестре.
- *Параметры* – на закладке представлены параметры, в соответствии с которыми работает Проактивная защита.

➡ *Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:*

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Проактивная защита** выберите пункт **Отчет**. Вы можете выбирать тип информации на каждой закладке отчета, сортировать ее по возрастанию и убыванию каждой из граф, а также производить поиск информации в отчете. Для этого воспользуйтесь пунктами контекстного меню, открыть которое можно по правой клавише мыши на заголовках граф отчета.

ЗАЩИТА ОТ РЕКЛАМЫ И ИНТЕРНЕТ-МОШЕННИЧЕСТВА

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

- навязчивая реклама различного содержания в окнах браузера, всплывающих окнах, в баннерах различных программ;
- попытки несанкционированного модемного соединения.

На кражу информации нацелены перехватчики клавиатуры, на трату ваших средств и времени – программы автоматического дозвона на платные веб-сайты, программы-шутки, программы-рекламы. Для защиты именно от таких программ и предназначен *Анти-Шпион*.

В состав Анти-Шпиона входят следующие модули:

- *Анти-Баннер (на стр. 85)* – блокирует рекламную информацию, размещенную на специальных баннерах в интернете или встроенных в интерфейс различных программ, установленных на вашем компьютере;
- *Анти-Дозвон (на стр. 88)* – обеспечивает защиту от попыток несанкционированного модемного соединения.

Чтобы изменить параметры работы Анти-Шпиона, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры модулей компонента.

В ЭТОМ РАЗДЕЛЕ

АНТИ-БАННЕР

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

Реклама на баннерах не только не содержит полезной информации, но и отвлекает вас от дел и повышает объем скачиваемого трафика. Анти-Баннер блокирует самые распространенные в настоящее время баннеры, маски которых включены в поставку Антивируса Касперского. Вы можете отключить блокировку баннеров либо сформировать собственные списки разрешенных и запрещенных баннеров.

Для интеграции модуля Анти-Баннер с браузером **Opera** добавьте в файл *standard_menu.ini*, раздел **[Image Link Popup Menu]** следующую строку: Item, «New banner» = Copy image address & Execute program, «<диск>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 для Windows Workstations MP4\opera_banner_deny.vbs», «//nologo %C» Вместо <диск> укажите имя вашего системного диска.

См. также

Формирование списка разрешенных адресов баннеров

«Белый» список баннеров формируется пользователем в процессе работы с программой, если возникает необходимость не блокировать некоторые баннеры. Этот список содержит маски баннеров, разрешенных к трансляции.

Чтобы добавить новую маску в «белый» список, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Блокирование рекламных баннеров** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** нажмите на кнопку **Добавить**.
6. 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.

Формирование списка запрещенных адресов баннеров

Вы можете составить список запрещенных адресов баннеров, которые будут блокироваться Анти-Баннером при обнаружении.

Чтобы добавить новую маску в «черный» список, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Блокирование рекламных баннеров** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **«Черный» список** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Маска адреса (URL)** введите маску запрещенного баннера. Чтобы отказаться от использования какой-либо маски, необязательно удалять ее из списка – достаточно снять флажок рядом с ней.

ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ РАБОТЫ КОМПОНЕНТА

Список масок наиболее распространенных рекламных баннеров составлен специалистами «Лаборатории Касперского» по результатам специально проведенного исследования и включен в комплект поставки Антивируса Касперского. Рекламные баннеры, подпадающие под маски из этого списка, будут блокироваться программой, если блокировка баннеров не отключена.

При создании списков разрешенных / запрещенных баннеров можно вводить как IP-адрес баннера, так и его символьное имя (URL-адрес). Чтобы избежать дублирования, вы можете воспользоваться дополнительной функцией, позволяющей преобразовывать введенные IP-адреса в доменные имена и наоборот.

- *Чтобы отключить использование списка баннеров, входящего в комплект поставки программы, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
  4. В открывшемся окне в блоке **Блокирование рекламных баннеров** нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Дополнительно** установите флажок **Не использовать стандартный список баннеров**.

- *Чтобы использовать возможность преобразования введенных IP-адресов баннеров в доменные имена (или доменные имена в IP-адреса), выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
  4. В открывшемся окне в блоке **Блокирование рекламных баннеров** нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Дополнительно** установите флажок **Преобразовывать IP-адреса в доменные имена**.

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 программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
  4. В открывшемся окне в блоке **Блокирование рекламных баннеров** нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **«Белый» список** (или на закладке **«Черный» список**) воспользуйтесь кнопками **Импорт** или **Экспорт**.

Анти-Дозвон

Анти-Дозвон обеспечивает защиту от попыток несанкционированного модемного соединения. 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, сообщающее вам об этом. В данном уведомлении вам нужно определить, разрешить или запретить данное соединение. Если вы его не инициировали, 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Шпион** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Блокирование попытки дозвона на платные номера** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Доверенные номера** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Телефонный номер** задайте доверенный номер или маску.

Статистика Анти-Шпиона

Детальное описание всех операций по защите от интернет-мошенничества приводится в специальном отчете. Все события распределены по разным закладкам в зависимости от того, каким именно модулем Анти-Шпиона они были отслежены:

- на закладке *Баннеры* приведены рекламные баннеры, обнаруженные и заблокированные в текущей сессии работы программы;
- на закладке *Попытки автодозвона* зафиксированы все попытки вредоносных программ соединения вашего компьютера с платными телефонными номерами;
- на закладке *Параметры* представлены параметры, в соответствии с которыми работает Анти-Шпион.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Проактивная защита** выберите пункт **Отчет**. Вы можете выбирать тип информации на каждой закладке отчета, сортировать ее по возрастанию и убыванию каждой из граф, а также производить поиск информации в отчете. Для этого воспользуйтесь пунктами контекстного меню, открыть которое можно по правой клавише мыши на заголовках граф отчета.

ЗАЩИТА ОТ СЕТЕВЫХ АТАК

Для обеспечения безопасности вашей работы в локальных сетях и интернете предназначен специальный компонент Антивируса Касперского – *Анти-Хакер*. Он защищает ваш компьютер на сетевом и прикладном уровнях, а также обеспечивает невидимость компьютера в сети для предотвращения атак.

Исходя из двух уровней защиты Анти-Хакера существуют два типа правил:

- *Правила для пакетов*. Используются для ввода общих ограничений сетевой активности независимо от установленных программ. Пример: при создании пакетного правила, запрещающего входящие соединения на порт 21, ни одна программа, использующая этот порт (например, FTP-сервер), не будет доступна извне.

- *Правила для программ*. Используются для ввода ограничений сетевой активности конкретной программы. Пример: если запрещено соединение по порту 80 для каждой из программ, вы можете создать правило, разрешающее соединения с использованием этого порта, только для веб-браузера FireFox.

Правила для сетевых пакетов и правила для программ могут быть *разрешающими* и *запрещающими*. В поставку Антивируса Касперского включен набор правил, регламентирующих сетевую активность наиболее распространенных программ, а также работу компьютера с распространенными протоколами и портами. Кроме того в дистрибутив программы включен набор разрешающих правил для доверенных программ, сетевая активность которых не вызывает сомнений.

Для упрощения настройки и применения правил в Антивирусе Касперского существует разделение всего сетевого пространства на зоны безопасности, зачастую совпадающие с подсетями, в которые включен компьютер. Каждой из зон вы можете присвоить статус (*Интернет*, *Локальная сеть*, *Доверенная*), на основании которого будет определена политика применения правил и контроля сетевой активности в данной зоне.

Специальный режим работы Анти-Хакера – режим невидимости – предотвращает обнаружение компьютера извне. В результате хакеры теряют объект атаки. В то же время на вашу работу в интернете режим не оказывает никакого влияния (при условии, что компьютер не используется в качестве сервера).

Чтобы изменить параметры работы Анти-Хакера, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.

4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В этом разделе

Схема работы компонента

Анти-Хакер защищает ваш компьютер на сетевом и прикладном уровнях, а также обеспечивает невидимость компьютера в сети для предотвращения атак. Рассмотрим подробнее, как построена работа Анти-Хакера.

Защита на сетевом уровне обеспечивается за счет использования глобальных правил для сетевых пакетов, где на основании анализа таких параметров, как направление движения пакета, протокол передачи пакета,а также порт назначения или выхода пакета, сетевая активность разрешается или блокируется. Правила для пакетов определяют сетевую доступность независимо от установленных на вашем компьютере программ, использующих сеть.

В дополнение к правилам для пакетов защита на сетевом уровне обеспечивается *подсистемой обнаружения вторжений* (см. раздел «Система обнаружения вторжений» на стр. 101) (IDS). Задача этой подсистемы заключается в анализе входящих соединений, определении факта сканирования портов вашего компьютера, а также фильтрации сетевых пакетов, направленных на использование уязвимостей программного обеспечения. При срабатывании подсистемы обнаружения вторжений все входящие соединения с атаковавшего компьютера блокируются на определенное время, а пользователь получает уведомление о том, что его компьютер подвергся сетевой атаке.

Работа подсистемы обнаружения вторжений основана на использовании в ходе анализа специальной базы атак (см. раздел «Виды сетевых атак» на стр. 102), которая регулярно пополняется специалистами «Лаборатории Касперского» и обновляется вместе с базами программы.

Защита на прикладном уровне обеспечивается за счет применения правил использования сетевых ресурсов программами, установленными на вашем компьютере. Как и защита на сетевом уровне, защита на прикладном уровне строится на анализе сетевых пакетов с учетом направления движения пакета, типа протокола его передачи, а также используемого порта. Однако на прикладном уровне учитываются характеристики не только сетевого пакета, но и конкретной программы, которой адресован данный пакет, или которая инициировала отправку этого пакета.

Использование правил для программ дает возможность более тонкой настройки защиты, когда, например, определенный тип соединения запрещен для одних программ, но разрешен для других.

См. также

Защита от сетевых атак 89

Изменение уровня защиты от сетевых атак

Защита вашей работы в сети может осуществляться на одном из следующих уровней:

- **Максимальная защита** – уровень защиты, допускающий сетевую активность, для которой предусмотрено разрешающее правило. Анти-Хакер использует правила, включенные в комплект поставки или созданные вами. Набор правил, поставляемый вместе с Антивирусом Касперского, включает разрешающие правила для программ, сетевая активность которых не вызывает подозрений, и пакетов данных, прием / передача которых абсолютно не опасны. Однако если в списке правил для программы существует запрещающее правило более высокого приоритета, чем разрешающее, сетевая активность данной программы будет запрещена.

  На данном уровне защиты любая программа, сетевая активность которой не зафиксирована в разрешающем правиле Анти-Хакера, будет блокироваться. Поэтому рекомендуется использовать этот уровень только в том случае, если вы уверены, что все необходимые для вашей работы программы разрешены соответствующими правилами, и вы не планируете установку нового программного обеспечения.

  Обратите внимание, что на данном уровне, может быть затруднена работа с Microsoft Office Outlook. Так, если почтовый клиент для обработки сообщений, поступающих в почтовый ящик пользователя, использует свои внутренние правила, то доставка почты осуществляться не будет, поскольку на данном уровне защиты от сетевых атак почтовый клиент не сможет получить доступ к Exchange-серверу. Аналогичная ситуация возникает при переносе почтового ящика пользователя на новый Exchange-сервер. Для решения подобных проблем следует сформировать разрешающее правило для Microsoft Office Outlook (или изменить, если оно было создано ранее), в котором будет разрешена любая активность с IP-адресом Exchange-сервера.

- **Обучающий режим** – уровень защиты, на котором происходит формирование правил Анти-Хакера. На данном уровне Анти-Хакер при каждой попытке некоторой программы воспользоваться сетевым ресурсом проверяет, есть ли для такого соединения правило. Если правило есть, Анти-Хакер действует в соответствии с его условиями. Если же правила нет, на экран выводится уведомление с описанием сетевого соединения (какой программой инициируется, по какому порту и протоколу и т. д.). Вам необходимо принять решение, стоит ли разрешать такое соединение или нет. С помощью специальной кнопки в окне уведомления вы можете создать правило для такого соединения, чтобы впредь при аналогичном соединении Анти-Хакер использовал условия, заданные в нем, не выводя уведомления на экран.

- **Минимальная защита** – уровень защиты, на котором блокируется только явным образом запрещенная сетевая активность. Анти-Хакер блокирует активность в соответствии с запрещающими правилами, включенными в комплект поставки или созданными вами. Однако если в списке правил существует разрешающее правило для программы более высокого приоритета, чем запрещающее, сетевая активность данной программы будет разрешена.

- **Разрешить все** – уровень защиты, разрешающий любую сетевую активность на вашем компьютере. Рекомендуется устанавливать такой уровень в крайне редких случаях, когда не наблюдается активных сетевых атак, и вы абсолютно доверяете любой сетевой активности.

Вы можете повысить или понизить степень защиты вашей работы в сети, выбрав соответствующий уровень или изменив параметры текущего уровня.

Чтобы изменить установленный уровень защиты от сетевых атак, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне выберите нужный уровень защиты от сетевых атак.

Правила для программ и пакетов

Правило Сетевого экрана представляет собой действие, совершаемое Сетевым экраном при обнаружении попытки соединения с заданными параметрами. Вы можете сформировать:

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

См. также

Правила для программ. Создание правила вручную

В комплект поставки Антивируса Касперского включен набор правил для наиболее распространенных программ, работающих под управлением операционной системы Microsoft Windows. Для одной и той же программы может быть создано несколько правил, как разрешающих, так и запрещающих. Обычно это программы, сетевая активность которых детально проанализирована специалистами «Лаборатории Касперского» и строго определена как опасная или неопасная.

В зависимости от уровня защиты, выбранного для работы Сетевого экрана, и типа сети, в которой работает компьютер, список правил для программ используется по-разному. Так, например, на уровне **Максимальная защита** вся сетевая активность программ, не подпадающая под разрешающие правила, блокируется.

Чтобы создать правило для программы вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для программ** нажмите на кнопку **Добавить**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов, или из пункта **Программы** перейти к списку программ, работающих в данный момент, и выбрать нужную. В результате будет открыт список правил для выбранной программы. Если для нее уже существуют правила, все они будут приведены в верхней части окна. Если правил не существует, окно правил будет пустым.
6. В окне правил для выбранной программы нажмите на кнопку **Добавить**.
7. Открывшееся окно **Новое правило** представляет собой форму для создания правила, где вы можете произвести детальную настройку правила.

Правила для программ. Создание правила на основе шаблона

В комплект поставки Антивируса Касперского входят готовые шаблоны правил, которые вы можете использовать при создании собственных правил.

Все многообразие существующих сетевых программ можно условно разделить на несколько типов: почтовые клиенты, веб-браузеры и т. п. Каждый тип характеризуется набором специфической активности, например, получение и отправка почты, получение и отображение HTML-страниц. Каждый тип использует определенный набор сетевых протоколов и портов. Таким образом, наличие шаблонов правил позволяет быстро и удобно производить начальную настройку правила исходя из типа программы.

Чтобы создать правило для программы, используя в качестве основы шаблон правил, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для программ** установите флажок **Группировать правила по программам**, если он был снят, и нажмите на кнопку **Добавить**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов или из пункта **Программы** перейти к списку программ, работающих в данный момент, и выбрать нужную. В результате будет открыто окно правил для выбранной программы. Если для нее уже существуют правила, все они будут приведены в верхней части окна. Если правил не существует, окно правил будет пустым.
6. В окне правил для программы нажмите на кнопку **Шаблон** и из контекстного меню выберите один из шаблонов правила.

   Так, **Разрешить все** – правило, разрешающее любую сетевую активность программы. **Запретить все** – правило, запрещающее любую сетевую активность программы. Все попытки инициировать сетевое соединение программой, для которой создано такое правило, будут блокироваться без предварительного уведомления пользователя.

Остальные шаблоны, приведенные в контекстном меню, создают набор правил, характерных для соответствующих программ. Например, шаблон **Почтовый клиент** создает набор правил, разрешающих стандартную для почтового клиента сетевую активность, например, отправку почты.

7. Если необходимо, откорректируйте созданные правила. Вы можете изменить действие, направление сетевого соединения, адрес, порты (локальный и удаленный), а также время действия правила.

   Если вы хотите, чтобы правило применялось к программе, запущенной с определенными параметрами командной строки, установите флажок **Командная строка** и в поле справа введите строку.

   Созданное правило (или набор правил) будет добавлено в конец списка с самым низким приоритетом. Вы можете повысить приоритет выполнения правила.

Правила для пакетов. Создание правила

В комплект поставки Антивируса Касперского включен набор правил, по которым осуществляется фильтрация передаваемых и принимаемых вашим компьютером пакетов данных. Передача пакетов может быть инициирована вами или какой-либо программой, установленной на вашем компьютере. В поставку Антивируса Касперского входят правила фильтрации для пакетов, передача которых детально проанализирована специалистами «Лаборатории Касперского» и строго определена как опасная или неопасная.

В зависимости от уровня защиты, выбранного для работы Сетевого экрана, и типа сети, в которой работает компьютер, список правил используется по-разному. Так, например, на уровне **Максимальная защита** вся сетевая активность, не попадающая под разрешающие правила, блокируется.

Обратите внимание, что правила для зон безопасности имеют более высокий приоритет, чем запрещающие пакетные правила. Так, например, при выборе статуса **Локальная сеть** будет разрешен обмен пакетами, а также доступ к папкам общего доступа, независимо от наличия запрещающих пакетных правил.

Чтобы создать новое пакетное правило, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для пакетов** нажмите на кнопку **Добавить**.
6. Открывшееся окно **Новое правило** представляет собой форму для создания правила, где вы можете произвести детальную настройку правила.

Изменение приоритета правила

Для каждого правила, созданного для программы или пакета, установлен приоритет выполнения. При прочих равных условиях (например, параметрах сетевого соединения) к сетевой активности программы будет применено то действие, которое определено правилом с наибольшим приоритетом.

Приоритет правила определяется его положением в списке правил. Самое первое правило в списке обладает самым высоким приоритетом выполнения. Каждое создаваемое вручную правило добавляется в начало списка. Правила, формируемые на основе шаблона или из специального уведомления, добавляются в конец списка правил.

Чтобы изменить приоритет правила для программы, выполните следующие действия:

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для программ** выберите имя программы в списке и нажмите на кнопку **Изменить**.
6. В открывшемся окне созданных для программы правил используйте кнопки **Вверх** и **Вниз**, чтобы переместить их по списку, меняя таким образом их приоритет.

Чтобы изменить приоритет правила для пакета, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для пакетов** выберите правило. Используйте кнопки **Вверх** и **Вниз**, чтобы перемещать выбранное правило в списке, изменяя таким образом его приоритет.

Экспорт и импорт сформированных правил

С помощью экспорта и импорта вы можете переносить сформированные правила на другие компьютеры. Это полезно для быстрой настройки Анти-Хакера.

Чтобы копировать сформированные правила для программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для программ** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию правил.

Чтобы копировать сформированные правила для пакета, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила для пакетов** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию правил.

Детальная настройка правил для программ и пакетов

Детальная настройка создаваемых и изменяемых правил осуществляется согласно следующим действиям:

- Определение имени правила. По умолчанию программа использует стандартное имя, которое вы можете изменить.
- Выбор параметров сетевого соединения, в соответствии с которыми будет действовать правило: удаленный IP-адрес, удаленный порт, локальный IP-адрес, локальный порт и время действия правила.
- Задание дополнительных параметров, отвечающих за информирование пользователя о применении правила.
- Задание значений для параметров правила и выбор действия для правила. Действие каждого создаваемого правила – *разрешающее*. Чтобы заменить его на запрещающее правило, в разделе описания правила щелкните левой клавишей мыши по ссылке **Разрешать**. Она примет значение **Запрещать**.
- Определение направления сетевого соединения (см. раздел «Изменение направления соединения» на стр. 97) для правила. По умолчанию предлагается создать правило как для входящего, так и для исходящего сетевого соединения.
- Определение протокола, по которому выполняется сетевое соединение. По умолчанию предлагается использовать соединение по TCP-протоколу. При создании правила для программы вы можете выбирать один из двух типов протоколов – TCP или UDP. Если вы создаете правило для пакета, можно изменить тип протокола (см. раздел «Изменение протокола передачи данных» на стр. 96). При выборе ICMP-протокола вам может понадобиться дополнительно указать его тип (см. раздел «Изменение типа ICMP-пакета» на стр. 98).
- Задание точных параметров сетевого соединения (адрес (см. раздел «Определение адреса сетевого соединения» на стр. 97), порт (см. раздел «Определение порта для соединения» на стр. 97), время правила (см. раздел «Определение времени действия правила» на стр. 98)), если они были выбраны.
- Изменение приоритета выполнения правила (см. раздел «Изменение приоритета правила» на стр. 94).

Создать правило можно также из окна уведомления об обнаружении сетевой активности.

Детальная настройка правил осуществляется в окне **Новое правило**, которое представляет собой форму для создания правила (для программ (см. стр. 92), для пакетов (см. стр. 94)).

См. также

Изменение протокола передачи данных

Один из параметров правила для программ и пакетов – протокол передачи данных при сетевом соединении. По умолчанию при создании правила и для программ, и для пакетов используется TCP-протокол.

Чтобы изменить протокол передачи данных, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92), для пакетов (см. стр. 94)) в блоке **Описание** нажмите на ссылку с именем протокола.

2. В открывшемся окне **Протокол** выберите нужное значение параметра.

Изменение направления соединения

Один из параметров правила для программ и пакетов – направление сетевого соединения.

Если вам важно зафиксировать в правиле именно направление пакета, определите, исходящий это пакет или входящий. Если же вы хотите создать правило для потока данных, выберите тип потока: входящий, исходящий или и тот, и другой.

Отличие *направления потока* от *направления пакета* состоит в том, что при создании правила для потока определяется, в каком направлении будет открыто соединение. Направление пакетов при передаче данных по этому соединению не учитывается.

Например, если вы настраиваете правило для обмена данными с FTP-сервером, работающим в пассивном режиме, нужно разрешить исходящий поток. Для обмена данными с FTP-сервером в активном режиме следует разрешить как исходящий, так и входящий поток.

Чтобы изменить направление потока данных, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92), для пакетов (см. стр. 94)) в блоке **Описание** нажмите на ссылку с направлением соединения.

2. В открывшемся окне **Направление** выберите нужное значение параметра.

Определение адреса сетевого соединения

Если в качестве параметра правила был выбран удаленный или локальный IP-адрес сетевого соединения, вам нужно задать для него значение, в соответствии с которым будет срабатывать правило.

Чтобы указать адрес сетевого соединения, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92), для пакетов (см. стр. 94)) в блоке **Параметры** установите флажок ☑ **Удаленный IP-адрес** (или **Локальный IP-адрес**). Затем в блоке **Описание** нажмите на ссылку **укажите IP-адрес**.

2. В открывшемся окне **IP-Адрес** выберите тип IP-адреса и задайте его значение.

Определение порта для соединения

При настройке правил существует возможность задавать значения локальных или удаленных портов.

- *Удаленный порт* – порт удаленного компьютера для соединения.

- *Локальный порт* – порт вашего компьютера.

Корректное определение локального и удаленного порта для передачи данных выполняется при создании правила из уведомления о подозрительной активности. Эта информация фиксируется автоматически.

Чтобы при настройке правил указать порт, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92), для пакетов (см. стр. 94)) в блоке **Параметры** установите флажок ☑ **Удаленный порт** (или **Локальный порт**). Затем в блоке **Описание** нажмите на ссылку **укажите порт**.

2. В открывшемся окне **Порт** введите значение порта или диапазон.

Определение времени действия правила

Для каждого правила вы можете задать интервал его действия в течение суток. Так, например, вы можете запретить использование программы ICQ с 9.30 до 18.30.

Чтобы определить время действия правила, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92), для пакетов (см. стр. 94)) в блоке **Параметры** установите флажок **Время**. Затем в блоке **Описание** нажмите на ссылку **укажите временной промежуток**.

2. В открывшемся окне **Временной промежуток** в полях **С** и **До** определите интервал действия правила.

Определение типа сокета

Для каждого правила вы можете определить тип сокета, поддерживающего передачу данных по тем или иным протоколам.

Чтобы изменить тип сокета, выполните следующие действия:

1. В окне **Новое правило** (для программ (см. стр. 92)) в блоке **Параметры** установите флажок **Тип сокета**. Затем в блоке **Описание** нажмите на ссылку с установленным типом сокета.

2. В открывшемся окне **Тип сокета** выберите нужное значение параметра.

Изменение типа ICMP-пакета

Протокол ICMP (межсетевой протокол управляющих сообщений) – это протокол сообщения отправителю пакета о возникших ошибках или затруднительных ситуациях при передаче данных.

Если в создаваемом вами правиле для пакетов в качестве протокола передачи данных указан протокол ICMP, вы можете указать дополнительно тип ICMP-сообщения.

Например, с помощью утилиты Ping, посылающей ICMP-запросы определенного типа и получающей на них отклики, злоумышленник может попытаться выяснить, включен ли ваш компьютер. В комплект поставки программы входит правило, по которому такие ICMP-запросы и отклики на них будут заблокированы, что, в свою очередь, позволит предотвратить потенциальную атаку на ваш компьютер.

Чтобы изменить тип ICMP-пакета, выполните следующие действия:

1. В окне **Новое правило** (для пакетов (см. стр. 94)) в блоке **Параметры** установите флажок **ICMP-тип**. Затем в блоке **Описание** нажмите на ссылку с именем типа ICMP-пакета.

2. В открывшемся окне **Тип ICMP-пакета** выберите нужное значение параметра.

Правила для зон безопасности

После установки программы компонент Анти-Хакер проводит анализ сетевого окружения вашего компьютера. По результатам анализа все сетевое пространство делится на условные зоны:

- *Интернет* – глобальная сеть Интернет. В данной зоне Антивирус Касперского работает как персональный сетевой экран. При этом вся сетевая активность регламентируется правилами для пакетов и программ, созданными по умолчанию для обеспечения максимальной безопасности. Вы не можете изменять условия защиты при работе в данной зоне; можно лишь включить режим невидимости компьютера для дополнительной безопасности.

- *Зоны безопасности* – некоторые условные зоны, зачастую совпадающие с подсетями, в которые включен ваш компьютер (это могут быть локальные подсети дома или на работе). По умолчанию данные зоны считаются зонами средней степени риска при работе в них. Вы можете изменять статус данных зон исходя из степени доверия той или иной подсети, а также настраивать правила для пакетов и программ.

Если включен режим обучения Анти-Хакера, при каждом подключении компьютера к некоторой новой зоне будет выводиться окно, содержащее ее краткое описание. Вам нужно присвоить данной зоне статус, на основании которого будет разрешена та или иная сетевая активность:

- **Интернет**. Этот статус по умолчанию присваивается сети Интернет, поскольку при работе в ней компьютер подвержен любым возможным типам угроз. Также данный статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами и т. д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне, а именно:

  - блокируется любая сетевая NetBios-активность в рамках подсети;

  - запрещается выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям подсети с таким статусом. Кроме того, при выборе данного статуса вы не сможете получить доступ к файлам и принтерам на других компьютерах сети.

- **Локальная сеть**. Этот статус присваивается по умолчанию большинству зон безопасности, обнаруженных при анализе сетевого окружения компьютера, за исключением сети Интернет. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети). При выборе данного статуса разрешается:

  - любая сетевая NetBios-активность в рамках подсети;

  - выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

  Выбирайте этот статус, если вы хотите предоставить доступ к некоторым каталогам или принтерам на вашем компьютере, но запретить любую другую внешнюю активность.

- **Доверенная**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность. Даже если установлен уровень **Максимальной защиты** и созданы запрещающие правила, они не будут действовать для удаленных компьютеров доверенной зоны.

Обратите внимание: любые ограничения / доступ на работу к файлам действуют только в рамках указанной подсети.

Для сети со статусом **Интернет** вы можете для дополнительной безопасности использовать режим невидимости. В этом режиме разрешена только сетевая активность, инициированная с вашего компьютера. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на вашу работу в интернете данный режим не оказывает никакого влияния.

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, HTTP-сервера). Иначе, компьютеры, обращающиеся к данному серверу, не будут видеть его в сети.

См. также

Добавление новых зон безопасности

Список зон, в которых был зарегистрирован ваш компьютер, отображается на закладке **Зоны**. Для каждой из них приведен статус, дано краткое описание сети и указано, используется или нет режим невидимости.

Чтобы добавить в список новую зону, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Зоны** воспользуйтесь кнопкой **Найти**. Анти-Хакер произведет поиск возможных для регистрации зон и, если таковые будут обнаружены, предложит вам определить их статус. Кроме того, вы можете добавить новую зону в список вручную (например, в случае, когда вы включаете мобильный компьютер в новую сеть). Для этого воспользуйтесь кнопкой **Добавить** и укажите требующуюся информацию в открывшемся окне **Параметры зоны**.

   Чтобы удалить сеть из списка, воспользуйтесь кнопкой **Удалить**.

Изменение статуса зоны безопасности

При автоматическом добавлении новой зоны адрес и маска подсети определяются автоматически. По умолчанию каждой добавляемой зоне присваивается статус **Локальная сеть**. Вы можете его изменить.

Чтобы изменить статус зоны безопасности, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Зоны** выберите зону в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующей ссылкой. Аналогичные действия, а также редактирование адреса и маски подсети можно выполнить в окне **Параметры зоны**, открывающемся по кнопке **Изменить**.

Включение / отключение режима невидимости

Для зоны **Интернет** вы можете дополнительно включить режим невидимости.

Чтобы включить режим невидимости, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт Настройка.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Зоны** выберите зону в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующей ссылкой.

Изменение режима работы Сетевого экрана

Режим работы Сетевого экрана регламентирует совместимость Анти-Хакера с программами, устанавливающими множественные сетевые соединения, а также с сетевыми играми.

- **Максимальная совместимость** – режим работы Сетевого экрана, обеспечивающий оптимальное функционирование компонента Анти-Хакер и программ, устанавливающих множественные сетевые соединения (клиенты файлообменных сетей). Использование данного режима в некоторых случаях может приводить к замедлению времени реакции сетевых программ, поскольку разрешающие правила имеют больший приоритет, чем режим невидимости (в режиме невидимости разрешена только сетевая активность, инициированная с вашего компьютера). При возникновении подобной ситуации рекомендуется использовать режим **Максимальная скорость**.

- **Максимальная скорость** – режим работы Сетевого экрана, обеспечивающий максимальную скорость реакции сетевых программ. Однако в данном режиме возможны проблемы с соединением в некоторых сетевых программах, поскольку в режиме невидимости блокируются все входящие соединения вне зависимости от заданных правил. Для решения проблемы рекомендуется отключить режим невидимости.

Изменение режима работы сетевого экрана вступит в силу только после перезапуска компонента Анти-Хакер.

Чтобы изменить установленный режим работы Сетевого экрана, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Сетевой экран** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Режим работы сетевого экрана** выберите нужный режим работы компонента.

Система обнаружения вторжений

Все известные на настоящее время сетевые атаки, которым подвержен компьютер, приведены в базах программы. На основе списка этих атак работает **модуль обнаружения вторжений** компонента Анти-Хакер. Пополнение списка атак, обнаруживаемых этим модулем, выполняется в процессе обновления баз (см. раздел «Обновление программы» на стр. 138). По умолчанию Антивирус Касперского не обновляет базы атак.

Система обнаружения вторжений отслеживает сетевую активность, характерную для сетевых атак, и при обнаружении попытки атаковать ваш компьютер блокирует любого рода сетевую активность атакующего компьютера в отношении вашего компьютера на один час. На экран выводится уведомление о том, что была

произведена попытка сетевой атаки, с указанием информации об атакующем компьютере. Вы можете приостановить или отключить работу модуля обнаружения вторжений.

Чтобы отключить работу Системы обнаружения вторжений, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне снимите флажок **Включить Систему обнаружения вторжений**.

   Чтобы остановить работу модуля, не открывая окно настройки программы, в контекстном меню выберите пункт **Стоп**.

Чтобы заблокировать атакующий компьютер на некоторое время, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Система обнаружения вторжений** установите флажок **Блокировать атакующий компьютер на ... мин** и укажите время (в минутах) в поле рядом.

Мониторинг сети

Вы можете просмотреть детальную информацию обо всех установленных на вашем компьютере соединениях, открытых портах, а также об объеме входящего и исходящего трафика. Для этого воспользуйтесь командой **Мониторинг сети** контекстного меню.

В открывшемся окне будет представлена информация, сгруппированная на следующих закладках:

- *Установленные соединения* – закладка отображает все активные на данный момент сетевые соединения с вашим компьютером. Здесь приводятся как соединения, инициированные вашим компьютером, так и входящие соединения.
- *Открытые порты* – на закладке перечислены все открытые на вашем компьютере порты.
- *Трафик* – закладка содержит объем принятой и переданной вами информации с другими компьютерами сети, в которой вы в данный момент работаете.

Виды сетевых атак

В настоящее время существует множество различных видов сетевых атак, которые используют уязвимости как операционной системы, так и иного установленного программного обеспечения системного и прикладного характера. Злоумышленники постоянно совершенствуют методы нападения, результатом которых могут стать кража конфиденциальной информации, выведение системы из строя либо ее полный «захват» с последующим использованием как части зомби-сети для совершения новых атак.

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

- **Сканирование портов** – угрозы этого вида сами по себе не являются атакой, но обычно ей предшествуют, поскольку это один 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 злоумышленнику представление о типе операционной системы на удаленном компьютере. 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.

- **DoS-атаки или атаки, вызывающие отказ в обслуживании** – это атаки, результатом которых является приведение атакуемой системы в нестабильное или полностью нерабочее состояние. Последствиями атак такого типа могут стать повреждение или разрушение информационных ресурсов, на которые они направлены, и, следовательно, невозможность их использования.

  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.

- **Атаки-вторжения**, целью которых является «захват» системы. Это самый опасный тип атак, поскольку в случае успешного выполнения система оказывается полностью скомпрометированной перед злоумышленником.

  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).

  В данную группу включено самое большое количество атак. Их можно разделить на три подгруппы в зависимости от операционной системы: атаки под Microsoft Windows, атаки под Unix, а также общая группа для сетевых сервисов, использующихся в обеих операционных системах.

  Наиболее распространены следующие виды атак, использующих сетевые сервисы операционной системы:

  - *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 (на стр. 101) автоматически анализирует и предотвращает использование подобных уязвимостей в наиболее распространенных сетевых сервисах (FTP, POP3, IMAP), 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 уязвимостей системных компонент, доступных по сети, – DCom, SMB, Wins, LSASS, IIS5.

Например, компонент Анти-Хакер защищает компьютер от атак, использующих следующие известные уязвимости программного обеспечения (список уязвимостей приведен в соответствии с нумерацией Microsoft Knowledge Base):

(MS03-026) DCOM RPC Vulnerability(Lovesan worm)

(MS03-043) Microsoft Messenger Service Buffer Overrun

(MS03-051) Microsoft Frontpage 2000 Server Extensions Buffer Overflow

(MS04-007) Microsoft Windows ASN.1 Vulnerability

(MS04-031) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(MS04-032) Microsoft Windows XP Metafile (.emf) Heap Overflow

(MS05-011) Microsoft Windows SMB Client Transaction Response Handling

(MS05-017) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(MS05-039) Microsoft Windows Plug-and-Play Service Remote Overflow

(MS04-045) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(MS05-051) Microsoft Windows Distributed Transaction Coordinator Memory Modification

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 атаки последнего типа состоит в отправке на удаленный компьютер UDP-пакета специального вида, способного выполнить вредоносный код.

Помните, что при работе в сети ваш компьютер ежедневно подвергается риску быть атакованным злоумышленниками. Чтобы обеспечить безопасную работу компьютера, обязательно включайте компонент Анти-Хакер при работе в интернете и регулярно обновляйте базы сетевых атак (см. раздел «Выбор предмета обновления» на стр. 143).

Статистика Анти-Хакера

Все операции, производимые Анти-Хакером, фиксируются с отчете. Информация по работе компонента сгруппирована на закладках:

- *Сетевые атаки* – на этой закладке приведен список всех сетевых атак, попытка реализовать которые была выполнена в текущей сессии работы Антивируса Касперского;
- *Заблокированные хосты* – на закладке приведен список всех хостов, работа с которыми заблокирована по ряду причин: например, в результате попытки атаковать ваш компьютер или при выполнении запрещающего правила;

- *Активность программ* – на закладке зафиксирована активность программ на вашем компьютере;
- *Фильтрация пакетов* – на закладке перечислены все пакеты данных, подвергнутые фильтрации в соответствии с тем или иным правилом Сетевого экрана;
- *Параметры* – на закладке представлены параметры, в соответствии с которыми работает Анти-Хакер.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Хакер** выберите пункт **Отчет**.

ЗАЩИТА ОТ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ

В состав Антивируса Касперского 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. 107), что позволяет компоненту с течением времени более точно различать спам и полезную почту. Источником данных для алгоритма служит содержимое письма. Для того, чтобы Анти-Спам эффективно распознавал спам и полезную почту, обучите (см. раздел «Обучение Анти-Спама» на стр. 109) его.

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

- Microsoft Office Outlook.
- Microsoft Outlook Express (Windows Mail).
- The Bat!

Путем формирования списков разрешенных или запрещенных отправителей 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 и запрещенного списков.

Анти-Спам позволяет просматривать почту на сервере и удалять ненужные сообщения, не загружая их на ваш компьютер.

Чтобы изменить параметры работы Анти-Спама, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В этом разделе

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 списках разрешенных и запрещенных отправителей:

   - если адрес отправителя находится в списке разрешенных отправителей, сообщению присваивается статус *не спам*;

- если адрес отправителя находится в списке запрещенных отправителей, почтовому сообщению присваивается статус *спам*.

2. Если сообщение было отправлено с помощью Microsoft Exchange Server, и проверка таких сообщений отключена, то сообщению присваивается статус *не спам*.

3. Сообщение анализируется на наличие строк из списка разрешенных фраз. Если найдена хотя бы одна строка из этого списка, сообщению присваивается статус *не спам*.

4. Сообщение анализируется на наличие строк из списка запрещенных фраз. 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 подозрительных и фишинговых веб-адресов, 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. Почтовое сообщение анализируется 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 окончании анализа Анти-Спам вычисляет, насколько увеличилась вероятность того, что сообщение является спамом.

9. Проверяется наличие дополнительных признаков (см. раздел «Использование дополнительных признаков фильтрации спама» на стр. 115), 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 представляет собой спам, 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 его маскировку, 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. 119), которые вы задали для вашего почтового клиента.

См. также

Защита от нежелательной почты 106

Обучение Анти-Спама

Один из инструментов распознавания спама – 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, то есть обучить его.

Существует несколько подходов к обучению Анти-Спама:

- использование Мастера обучения (см. раздел «Обучение с помощью Мастера обучения» на стр. 109) (пакетное обучение), предпочтительно в самом начале работы с Анти-Спамом;
- обучение Анти-Спама на исходящих сообщениях (см. раздел «Обучение на исходящих письмах» на стр. 110);
- обучение непосредственно во время работы с электронной корреспонденцией (см. раздел «Обучение с помощью почтового клиента» на стр. 110), с использованием специальных кнопок в панели инструментов почтового клиента или пунктов меню;
- обучение при работе с отчетами Анти-Спама (см. раздел «Обучение с помощью отчетов» на стр. 111).

См. также

Обучение с помощью Мастера обучения

Мастер обучения позволяет провести обучение Анти-Спама в пакетном режиме, указав, какие папки почтового ящика 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 кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Чтобы запустить Мастер обучения, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Обучение** нажмите на кнопку **Мастер обучения**.

При обучении на полезных письмах адрес отправителя письма добавляется в список разрешенных отправителей.

- *Чтобы отключить добавление адреса отправителя в список разрешенных отправителей, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке Уровень агрессивности нажмите на кнопку **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**.

Обучение на исходящих письмах

Вы можете обучить Анти-Спам на примере 50 исходящих сообщений. Адреса получателей этих сообщений будут автоматически занесены в список разрешенных отправителей.

- *Чтобы обучить Анти-Спам на исходящих сообщениях, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Исходящие сообщения** установите флажок **Обучаться на исходящих письмах**.

- *Чтобы отключить добавление адреса отправителя в список разрешенных отправителей, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке Уровень агрессивности нажмите на кнопку **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**.

Обучение с помощью почтового клиента

Обучение в процессе непосредственной работы с электронной корреспонденцией предполагает использование специальных кнопок в панели инструментов вашего почтового клиента.

- *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!

Анти-Спам проводит обучение на выбранном письме. Если вы выделяете несколько писем, обучение происходит на всех выделенных письмах.

При отметке письма как полезного адрес отправителя письма добавляется в список разрешенных отправителей.

Чтобы отключить добавление адреса отправителя в список разрешенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **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.

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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Отчет**.
4. В открывшемся окне на закладке **События** выберите письмо, на основе которого вы хотите провести дополнительное обучение.
5. В контекстном меню для письма выберите одно из следующих действий:
   - **Отметить как спам**.
   - **Отметить как не спам**.
   - **Добавить в «белый» список**.
   - **Добавить в «черный» список**.

Изменение уровня агрессивности

Антивирус Касперского 6.0 для Windows Workstations MP4 обеспечивает защиту от спама на одном из следующих уровней:

- **Блокировать все** – самый высокий уровень агрессивности, на котором спамом признается любая почта, кроме сообщений, отправители которых перечислены в списке разрешенных адресов, и которые содержат строки из списка разрешенных фраз. Использование остальных технологий отключено.

- **Высокий** – высокий уровень, при активации которого возникает вероятность того, что некоторые электронные письма, на самом деле не являющиеся спамом, будут помечены как *спам*. На данном уровне анализ письма выполняется по спискам разрешенных и запрещенных адресов и фраз, а также с использованием технологий PDB и GSG, Recent Terms а также алгоритма iBayes.

  Данный режим имеет смысл применять в тех случаях, когда высока вероятность того, что адрес получателя корреспонденции неизвестен спамерам: например, когда получатель не зарегистрирован в почтовых рассылках и не имеет почтового ящика на бесплатных / не корпоративных почтовых серверах.

- **Рекомендуемый** – наиболее универсальный уровень настройки с точки зрения классификации электронных сообщений.

  При таком уровне возможно возникновение ситуаций, когда нежелательные письма не будут распознаны. Это указывает на то, что Анти-Спам недостаточно хорошо обучен. Рекомендуется провести дополнительное обучение модуля с помощью Мастера обучения или кнопок **Спам** / **Не спам** (для программы The Bat! – пункты меню) на тех письмах, которые были распознаны неверно.

- **Низкий** – более лояльный уровень настройки. Он может быть рекомендован пользователям, чья входящая корреспонденция по каким-либо причинам содержит значительное количество слов, распознаваемых Анти-Спамом как спам, но таковым не является. Причиной такой ситуации может служить профессиональная деятельность получателя, в силу которой он вынужден использовать в своей переписке с коллегами профессиональные термины, широко встречающиеся в спаме. Для анализа сообщений на данном уровне используются все технологии обнаружения спама.

- **Пропускать все** – самый низкий уровень агрессивности, на котором спамом признается только та почта, которая содержит строки запрещенного списка фраз и отправители которой перечислены в списке запрещенных отправителей. Использование остальных технологий отключено.

По умолчанию защита от спама осуществляется на **Рекомендуемом** уровне агрессивности. Вы можете повысить или понизить уровень, или изменить параметры текущего уровня.

Чтобы изменить установленный уровень агрессивности Анти-Спама, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне переместите ползунок по шкале уровней агрессивности. Регулируя уровень агрессивности, вы определяете соотношение факторов спама, потенциального спама и полезной почты.

Фильтрация писем на сервере. Диспетчер Писем

Диспетчер писем предназначен для просмотра списка сообщений электронной почты на сервере, без загрузки 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 если 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. В данной ситуации, используя лишь адрес отправителя, невозможно определить, отправлено письмо вашим коллегой или спамером. Используйте заголовки письма! Просмотрите внимательно, кем и когда отправлено данное письмо, каков его объем. Проследите путь следования письма от отправителя до вашего почтового сервера. Вся эта информация должна присутствовать 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** 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 флажки напротив сообщения в столбце **Удалить**.
2. В верхней части окна нажмите на кнопку **Удалить выбранные**.

Сообщения 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 на серверах, соединенных X400-коннекторами.

По умолчанию Анти-Спам не проверяет сообщения Microsoft Exchange Server.

Чтобы Анти-Спам анализировал сообщения, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** снимите флажок **Не проверять сообщения Microsoft Exchange Server**.

Выбор метода проверки

Под методами проверки подразумевается проверка ссылок, содержащихся в почтовых сообщениях, на принадлежность к списку подозрительных веб-адресов и / или к списку фишинговых адресов.

Проверка ссылок на принадлежность к списку фишинговых адресов позволяет избежать фишинг-атак, которые, как правило, представляют собой почтовые сообщения якобы от финансовых структур, содержащие ссылки на их 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 может служить 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.

- *Чтобы проверять ссылки из почтовых сообщений по базе подозрительных веб-адресов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** установите флажок **Проверять ссылки по базе подозрительных веб-адресов**.

- *Чтобы проверять ссылки из почтовых сообщений по базе фишинговых веб-адресов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

Выбор технологий фильтрации спама

Анализ почтовых сообщений на предмет спама осуществляется на основе современных технологий фильтрации.

По умолчанию используются все технологии фильтрации, что позволяет проводить максимально полный анализ почтового сообщения на спам.

- *Чтобы отключить использование какой-либо технологии фильтрации, выполните следующие действия:*

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **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 вычисляются 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 значения, 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 программы.

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

3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **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, по которым производится фильтрация сообщений на спам (формирование «белого» и «черного» списков, анализ с помощью технологий фильтрации и т. д.), вы можете задавать дополнительные . 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, набранным мелким шрифтом. Также спамом могут быть письма с невидимыми символами (цвет текста совпадает с цветом фона), содержащие скрытые (не отображаемые) элементы 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Алгоритмы** нажмите на кнопку **Дополнительно**.
6. В открывшемся окне **Дополнительно** установите флажки 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%.

   Вероятность принадлежности к спаму, полученная при использовании дополнительных признаков фильтрации спама, добавляется к общему вердикту, который Анти-Спам выносит всему сообщению.

   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 том случае, если адрес не совпадет ни с одним адресом из вашего списка, сообщению будет присвоен статус **спам**.

Формирование списка разрешенных отправителей

В списке разрешенных отправителей хранятся адреса отправителей писем, от которых, по вашему убеждению, спама приходить не должно. Список разрешенных отправителей заполняется автоматически во время обучения компонента Анти-Спам. Вы можете его откорректировать.

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 с *ivan.*, а имя почтового домена начинается на *test* и оканчивается тремя любыми символами, всегда является полезной; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Чтобы сформировать список разрешенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** установите флажок **Считать полезными письма от следующих адресатов** и нажмите на кнопку **Добавить**.

5. В открывшемся окне **Маска адреса электронной почты** введите нужный адрес или маску.

Формирование списка разрешенных фраз

В 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, содержащее обращение к пользователю по имени *Иван*, после которого идет любой символ, 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные фразы** установите флажок **Считать полезными письма со следующими фразами** и нажмите на кнопку **Добавить**.
6. В открывшемся окне **Разрешенная фраза** введите нужную строку или маску.

Импорт списка разрешенных отправителей

Для адресов списка разрешенных отправителей предусмотрена возможность импорта из файлов формата **.txt*, **.csv* или адресной книги Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail).

Чтобы импортировать список разрешенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **«Белый» список** в блоке **Разрешенные отправители** нажмите на кнопку **Импорт**.

6. В раскрывшемся меню выберите источник импорта:

   - Если вы выбрали пункт меню **Из файла**, вам будет предложено окно выбора файла. Программа поддерживает импорт из файлов типа *.csv* или *.txt*.

   - Если вы выбрали пункт меню **Из адресной книги**, откроется окно выбора адресной книги. Выберите в этом окне нужную адресную книгу.

Формирование списка запрещенных отправителей

В списке запрещенных отправителей 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 с *ivan.*, а имя почтового домена начинается на *test* и оканчивается тремя любыми символами, всегда является спамом; например: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Чтобы сформировать список запрещенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.

4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **«Черный» список** в блоке **Запрещенные отправители** установите флажок **Считать спамом письма от следующих адресатов** и нажмите на кнопку **Добавить**.

6. В открывшемся окне **Маска адреса электронной почты** введите нужный адрес или маску.

Формирование списка запрещенных фраз

В списке запрещенных фраз 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 в качестве строк списка.
- *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 по имени *Иван*, после 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 \?.

При проверке сообщения Анти-Спам анализирует его на наличие строк из списка запрещенных фраз. Обнаружение в сообщении слов из этого списка увеличивает вероятность того, что сообщение является спамом. Когда вычисленная вероятность превышает 100%, сообщению присваивается статус *спам*.

Чтобы сформировать список запрещенных фраз, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **«Черный» список** в блоке **Запрещенные фразы** установите флажок **Считать спамом письма со следующими фразами** и нажмите на кнопку **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, Microsoft Outlook Express (Windows Mail) и The Bat! для этого предусмотрены специальные модули расширения. Для других почтовых клиентов можно 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 программы.

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.

Дополнительные действия над спамом и потенциальным спамом в Microsoft Office Outlook приведены на специальной закладке **Анти-Спам** в меню **Сервис** → **Параметры**.

Она открывается автоматически при первой загрузке почтового клиента после установки программы и предлагает вам настроить обработку нежелательной корреспонденции.

При обучении Анти-Спама с помощью почтового клиента 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. Иными словами, 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, когда 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 Outlook. 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 программы. Команда вызова мастера зависит от вашей версии Microsoft 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**. В открывшемся окне выберите из раскрывающегося списка **Kaspersky Anti-Spam** и 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**). Убедитесь, 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; приоритет каждого последующего правила ниже, чем предыдущего. 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 установить в параметрах этого правила флажок **остановить дальнейшую обработку правил** (см. шаг третий окна создания правил).

Если вы имеете опыт создания правил обработки электронных сообщений в Microsoft Office Outlook, можете создать собственное правило для Анти-Спама на основе предложенного выше алгоритма.

См. также

Настройка обработки спама в Microsoft Outlook Express (Windows Mail)

Окно настройки обработки спама открывается при первом запуске почтового клиента после установки программы.

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как *спам* или *потенциальный спам*, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**.

Дополнительные действия над спамом и потенциальным спамом в Microsoft Outlook Express (Windows Mail) приведены в специальном окне, которое открывается по кнопке **Настройка**, расположенной рядом с другими кнопками Анти-Спама в панели задач: **Спам** и **Не Спам**.

Окно открывается автоматически при первой загрузке почтового клиента после установки программы и предлагает вам настроить обработку нежелательной корреспонденции.

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 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.

Настройки обработки спама хранятся в виде правил Microsoft Outlook Express (Windows Mail), поэтому для сохранения изменений необходимо перезапустить Microsoft Outlook Express (Windows Mail).

См. также

Настройка обработки спама в The Bat!

Действия над спамом и потенциальным спамом в почтовом клиенте The Bat! определяются средствами самого клиента.

Чтобы перейти к настройке правил обработки спама в The Bat!, выполните следующие действия:

1. В меню **Свойства** почтового клиента выберите пункт **Настройка**.
2. В дереве настройки выберите пункт **Защита от спама**.

Представленные параметры защиты от спама распространяются на все установленные на компьютере модули Анти-Спама, поддерживающие работу с The Bat!

Вам нужно определить уровень рейтинга и указать, как поступать с сообщениями 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 Антивирус Касперского 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 Антивирусе Касперского 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!

См. также

Восстановление параметров Анти-Спама по умолчанию

Настраивая работу Анти-Спама, вы всегда можете вернуться к рекомендуемым параметрам его работы. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы восстановить параметры защиты от нежелательной почты по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Настройка**.
4. В открывшемся окне в блоке **Уровень агрессивности** нажмите на кнопку **По умолчанию**.

Статистика Анти-Спама

Общая информация о работе компонента фиксируется в специальном отчете, где вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на нескольких закладках:

- Полный список событий, возникших в работе компонента, ведется на закладке *События*. Здесь приводятся результаты обучения Анти-Спама с указанием фактора, категории и причин той или иной классификации письма.

  С помощью специального контекстного меню вы можете проводить обучение при просмотре отчета. Для этого выберите имя письма, по правой клавише мыши откройте контекстное меню и выберите в нем **Отметить как спам**, если это письмо является спамом, или **Отметить как не спам**, если выбранное письмо – полезная почта. Кроме того, на основе информации, полученной при анализе письма, вы можете пополнить «белый» и «черный» списки Анти-Спама. Для этого воспользуйтесь соответствующими пунктами контекстного меню.

- Параметры, в соответствии с которыми осуществляется фильтрация и обработка почтовых сообщений, приводятся на закладке *Параметры*.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Анти-Спам** выберите пункт **Отчет**.

КОНТРОЛЬ ДОСТУПА

Контроль доступа – новый компонент Антивируса Касперского. С помощью модуля Контроль устройств он контролирует доступ пользователей к устройствам, установленным на компьютере. Модуль позволяет блокировать обращения программы к определенным типам внешних устройств.

После установки Контроль устройств отключен.

- *Чтобы включить использование Контроля устройств, выполните следующие действия:*

  1. Откройте окно настройки программы.
  2. В левой части окна выберите раздел **Контроль устройств**.
  3. В правой части окна установите флажок **Включить Контроль устройств**.

- *Чтобы изменить параметры работы Контроля устройств, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Контроль устройств** выберите пункт **Настройка**.
  4. В открывшемся окне внесите необходимые изменения в параметры компонента.

В ЭТОМ РАЗДЕЛЕ

Контроль устройств. Ограничение использования внешних устройств

Модуль Контроль устройств контролирует работу программ с внешними устройствами, установленными на компьютере.

По умолчанию Контроль устройств разрешает доступ ко всем устройствам.

- *Чтобы ограничить доступ программ к устройствам, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Защита**.
  3. В контекстном меню компонента **Контроль устройств** выберите пункт **Настройка**.
  4. В открывшемся окне нажмите на кнопку **Настройка**.
  5. В открывшемся окне **Настройка: Контроль устройств** установите флажки напротив типов устройств, работу с которыми вы хотите заблокировать.

Чтобы изменения вступили в силу, необходимо выполнить повторное подключение устройства (в случае Firewire- или USB-устройств) или перезагрузить компьютер (для остальных типов устройств).

Контроль устройств. Запрет автозапуска

Вы можете запретить автозапуск, используя следующие возможности:

- Запретить автозапуск для всех устройств, что приводит к отключению функциональности AutoRun / AutoPlay, реализованной в Microsoft Windows. Функциональность позволяет считывать данные и автоматически выполнять программы со съемного носителя информации, который подключается к компьютеру.

- Запретить обработку файла autorun.inf, что приводит к запрету несанкционированного запуска программ со съемных носителей информации. Возможность позволяет, не отключая полностью функциональность AutoPlay, запретить операционной системе выполнение потенциально опасных инструкций в файле autorun.inf.

По умолчанию автозапуск запрещен. Поскольку злоумышленники часто используют возможность автозапуска для распространения вирусов через съемные диски, специалисты «Лаборатории Касперского» не рекомендуют вам его разрешать.

Чтобы запретить возможность автозапуска, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Контроль устройств** выберите пункт **Настройка**.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне **Настройка: Контроль устройств** в блоке **Автозапуск** установите соответствующие флажки  .

Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

Статистика Контроля доступа

Все операции, производимые Контролем доступа, фиксируются в специальном отчете, где вашему вниманию будет предоставлен детальный отчет о работе компонента, сгруппированный на нескольких закладках:

- Все внешние устройства, заблокированные модулем, перечислены на закладке *Устройства*.

- На закладке *Параметры* представлены параметры, в соответствии с которыми работает Контроль доступа.

Чтобы ознакомиться с информацией о работе компонента, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Защита**.
3. В контекстном меню компонента **Контроль доступа** выберите пункт **Отчет**.

ПРОВЕРКА КОМПЬЮТЕРА НА ВИРУСЫ

Проверка на вирусы – одна из важнейших функций обеспечения безопасности компьютера. Антивирус Касперского 6.0 для Windows Workstations MP4 позволяет проверять на присутствие вирусов как отдельные объекты (файлы, папки, диски, сменные устройства), так и весь компьютер в целом.

В состав Антивируса Касперского 6.0 для Windows Workstations MP4 по умолчанию включены следующие задачи проверки:

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.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами. Вы можете изменять эти параметры, а также устанавливать расписание запуска задач.

Кроме того, вы можете проверить на вирусы любой объект (например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п.), не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского или 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**.

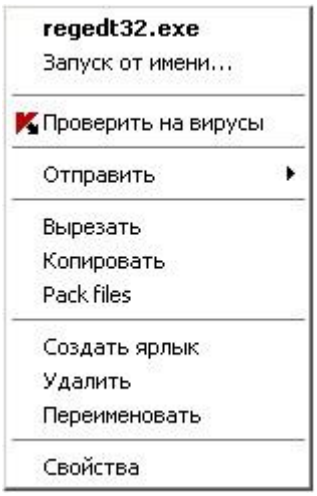


Рисунок 7. Контекстное меню Microsoft Windows

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 программы.
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 открывшемся окне в параметры выбранной задачи внесите необходимые изменения.

Чтобы перейти к отчету о проверке на вирусы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Нажмите на кнопку **Отчеты**.

В этом разделе

Запуск проверки на вирусы

Запустить задачу проверки на вирусы можно двумя способами:

- из контекстного меню Антивируса Касперского;

- из главного окна Антивируса Касперского.

Информация о процессе выполнения задачи будет отображаться в главном окне Антивируса Касперского.

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.).

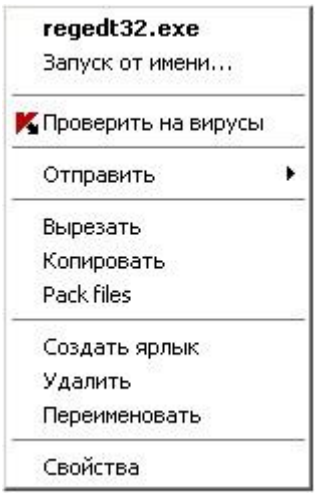


Рисунок 8. Контекстное меню Microsoft Windows

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

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок программы.
2. В раскрывшемся меню выберите пункт **Проверка**. В открывшемся главном окне Антивируса Касперского выберите нужную задачу **Проверка** (**Полная проверка**, **Быстрая проверка**). Произведите, если необходимо, настройку параметров выбранной задачи и нажмите на кнопку **Выполнить проверку**.
3. Либо в контекстном меню выберите пункт **Проверка Моего компьютера**. Будет запущена полная проверка компьютера. Процесс выполнения задачи будет отображаться в главном окне Антивируса Касперского.

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

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**).
3. Для выбранного раздела нажмите на кнопку **Выполнить проверку**. Процесс выполнения задачи будет отображаться в главном окне программы.

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 окне статистики.

ФОРМИРОВАНИЕ СПИСКА ОБЪЕКТОВ ПРОВЕРКИ

По умолчанию каждой задаче проверки на вирусы соответствует свой список объектов. Чтобы просмотреть этот список, в разделе **Проверка** главного окна программ выберите имя задачи (например, **Полная проверка**). Список объектов будет представлен в правой части окна.

Для задач, созданных по умолчанию при установке программы, списки объектов для проверки уже сформированы.

Для удобства пользователей доступно добавление в область проверки таких категорий, как почтовые ящики пользователя, системная память, объекты автозапуска, резервное хранилище операционной системы, объекты, находящиеся в карантинном каталоге Антивируса Касперского.

Кроме того, при добавлении в область проверки каталога, содержащего вложенные объекты, вы можете изменять рекурсию. Для этого выберите объект в списке объектов проверки, откройте контекстное меню и воспользуйтесь командой **Включая вложенные папки**.

Чтобы сформировать список объектов для проверки, выполните следующие действия:

1. Откройте главное окно программы.
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 проверки, снимите флажки рядом с ними в списке. Чтобы удалить объект из списка, выберите его и нажмите на ссылку **Удалить**.

ИЗМЕНЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

Под уровнем безопасности подразумевается предустановленный набор параметров проверки. Специалистами «Лаборатории Касперского» сформированы три уровня безопасности. Решение о том, какой уровень выбрать, вы принимаете самостоятельно на основе собственных предпочтений:

- если вы подозреваете, что вероятность заражения вашего компьютера очень высока, выберите высокий уровень безопасности.
- рекомендуемый уровень подходит для большинства случаев, и именно его рекомендуют использовать специалисты «Лаборатории Касперского».
- если вы работаете с программами, требующими значительных ресурсов оперативной памяти, выберите низкий уровень безопасности, поскольку набор проверяемых файлов на данном уровне сокращен.

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. По умолчанию проверка осуществляется на **Рекомендуемом** уровне.

Чтобы изменить установленный уровень безопасности, выполните следующие действия:

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** переместите ползунок по шкале. Регулируя уровень безопасности, вы определяете соотношение между скоростью выполнения проверки и

количеством проверяемых файлов: чем меньше файлов анализируется на присутствие вирусов, тем выше скорость проверки. Либо нажмите на кнопку **Настройка** и в открывшемся окне настройте необходимые параметры. Уровень безопасности изменится на **Другой**.

Изменение действия при обнаружении угрозы

Если в результате проверки объекта на вирусы выясняется, что он заражен или подозревается на заражение, дальнейшие операции программы зависят от статуса объекта и выбранного действия.

По результатам проверки объекту может быть присвоен один из следующих статусов:

- статус одной из вредоносных программ (например, *вирус*, *троянская программа*).
- статус *возможно зараженный*, когда в результате проверки однозначно невозможно определить, заражен объект или нет. Вероятно, в файле обнаружена последовательность кода неизвестного вируса или модифицированный код известного вируса.

По умолчанию все зараженные файлы подвергаются лечению, а все возможно зараженные помещаются на карантин.

Если в качестве действия вы выбрали	При обнаружении вредоносного / возможно зараженного объекта
Запросить по окончании проверки	Программа откладывает обработку объектов до конца проверки. По окончании проверки на экран будет выведено окно статистики со списком обнаруженных объектов и вам будет предложено провести обработку объектов.
Запросить во время проверки	Программа выводит на экран предупреждающее сообщение, содержащее информацию о том, какой вредоносный код содержит зараженный / возможно зараженный объект, и предлагает на выбор одно из дальнейших действий.
Не запрашивать	Программа фиксирует информацию об обнаруженных объектах в отчете, не обрабатывая их и не уведомляя пользователя. Не рекомендуется устанавливать данный режим работы программы, поскольку зараженные и возможно зараженные объекты остаются на вашем компьютере, и избежать заражения практически невозможно.
Не запрашивать **Лечить**	Программа, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если вылечить объект не удалось, он либо блокируется (если вылечить объект невозможно), либо ему присваивается статус *возможно зараженный* (если объект считается подозрительным), и он помещается на карантин. Информация об этом фиксируется в отчете. Позже можно попытаться вылечить этот объект.
Не запрашивать **Лечить** **Удалить, если лечение невозможно**	Программа, не запрашивая подтверждения пользователя, выполняет попытку лечения обнаруженного объекта. Если попытка лечения объекта не удалась, он удаляется.
Не запрашивать **Лечить** **Удалить**	Программа автоматически удаляет объект.

Перед лечением или удалением объекта Антивирус Касперского формирует его резервную копию и помещает ее в резервное хранилище на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

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

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Действие** внесите необходимые изменения.

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:

- Для файлов некоторых форматов (например, *txt*) вероятность внедрения и последующей активации вредоносного кода достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, *exe*, *dll*, *doc)*. Риск внедрения и активации в такие файлы вредоносного кода весьма высок.
- Не стоит забывать, что злоумышленник может отправить вирус на ваш компьютер в файле с расширением *txt*, тогда как на самом деле это будет исполняемый файл, переименованный в *txt*-файл. Если вы выберете вариант **Файлы, проверяемые по расширению**, то в процессе проверки такой файл будет пропущен. Если же выбран вариант **Файлы, проверяемые по формату**, невзирая на расширение, защита файлов проанализирует заголовок и выяснит, 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 программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **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 Антивируса Касперского. 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.

Кроме того, вы можете задать ограничение длительности проверки. По истечении заданного времени проверка файлов будет прекращена. Размер файла, подвергаемого проверке, также можно ограничить. Если он превысит установленное значение, файл будет исключен из проверки.

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

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **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 программы.

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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **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 одного файла в поле рядом.

Чтобы ограничить размер проверяемого файла, выполните следующие действия:

1. Откройте главное окно программы.

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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Область действия** нажмите на кнопку **Дополнительно**.

6. В открывшемся окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и задайте размер файла в поле рядом.

Проверка составных файлов

Распространенная практика сокрытия вирусов – внедрение их 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, следует ли 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, выбор типа проверяемых составных файлов будет недоступен.

Чтобы изменить список проверяемых составных файлов, выполните следующие действия:

1. Откройте главное окно программы.

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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** выберите нужный тип проверяемых составных файлов.

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 программы, дату предыдущей проверки объекта, а также изменение параметров проверки.

  Например, у вас есть файл архива, который был проверен Антивирусом Касперского и получил статус *не заражен*. 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 программы, архив будет проверен повторно.

  Технология iChecker имеет ограничение: она не работает с файлами больших размеров и применима только к объектам с известной программе 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 кроме того, применима только к объектам, расположенным в файловой системе NTFS.

Чтобы использовать технологию проверки объектов, выполните следующие действия:

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** включите использование нужной технологии.

ИЗМЕНЕНИЕ МЕТОДА ПРОВЕРКИ

В качестве метода проверки 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 этого метода проверки вы можете использовать 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 программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выберите нужные методы проверки.

Производительность компьютера при выполнении задач

В целях ограничения нагрузки на центральный процессор и дисковые подсистемы выполнение задач проверки на вирусы можно отложить.

Выполнение задач проверки увеличивает нагрузку на центральный процессор и дисковые подсистемы, тем самым замедляя работу других программ. По умолчанию при возникновении такой ситуации Антивирус Касперского приостанавливает выполнение задач проверки и высвобождает ресурсы системы для программ пользователя.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы системы.

Обратите внимание, что данный параметр можно настраивать индивидуально для каждой задачи проверки на вирусы. В этом случае настройка параметра, произведенная для конкретной задачи, имеет более высокий приоритет.

Чтобы отложить выполнение задач проверки на вирусы при замедлении работы других программ, выполните следующие действия:

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** установите флажок **Уступать ресурсы другим программам**.

Режим запуска: задание учетной записи

Вы можете задать учетную запись, с правами которой будет производиться проверка.

Чтобы запустить задачу с правами другой учетной записи, выполните следующие действия:

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами учетной записи**. В полях ниже задайте имя учетной записи и пароль.

Режим запуска: формирование расписания

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

По умолчанию для задач, созданных при установке программы, отключен автоматический запуск по расписанию. Исключение составляет задача быстрой проверки, которая выполняется каждый раз при включении компьютера.

При формировании расписания запуска задач необходимо определить интервал, с которым должна выполняться проверка.

Если по каким-либо причинам запуск невозможен (например, в заданное время компьютер был выключен), вы можете настроить автоматический запуск в тот момент, когда это станет возможным.

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

  1. Откройте главное окно программы.
  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 открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
  5. В открывшемся окне **Расписание** внесите необходимые изменения.

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

  1. Откройте главное окно программы.
  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 открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
  5. В открывшемся окне **Расписание** в блоке **Настройка расписания** установите флажок **Запускать пропущенную задачу**.

Особенности запуска задачи проверки по расписанию

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

Для задач, запускаемых по сформированному расписанию, вы можете использовать дополнительную возможность – *приостанавливать проверку по расписанию в том случае, если выключен скринсейвер или компьютер разблокирован*. Данная возможность позволяет отложить запуск задачи до того момента, когда пользователь закончит работу на компьютере. Таким образом, задача проверки не будет занимать ресурсы компьютера во время его работы.

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

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Полная проверка**, **Быстрая проверка**.
  3. Для выбранного раздела нажмите на ссылку с установленным уровнем безопасности.

4. В открывшемся окне в блоке **Режим запуска** установите флажок **Приостанавливать проверку по расписанию, если выключен скринсейвер или разблокирован компьютер**.

Статистика проверки на вирусы

Общая информация о работе каждой задачи проверки на вирусы приводится в окне статистики. Здесь вы можете узнать, сколько объектов было проверено, сколько обнаружено вредоносных объектов и объектов, требующих обработки. Кроме того, здесь приведена информация о времени начала и окончания последнего выполнения задачи, а также о длительности проверки.

Основная информация о результатах проверки сгруппирована на следующих закладках:

- *Обнаружено* – содержит все опасные объекты, обнаруженные в процессе выполнения задачи;
- *События* – содержит полный список событий, возникших при выполнении задачи;
- *Статистика* – содержит статистические данные о проверенных объектах;
- *Параметры* – содержит параметры, в соответствии с которыми выполняется задача.

Если в результате выполнения задачи возникли какие-то ошибки, попробуйте запустить ее еще раз. Если попытка будет завершена с ошибкой, сохраните отчет с результатами выполнения задачи в файл по кнопке **Сохранить как**. Затем отправьте отчет в Службу технической поддержки. Специалисты «Лаборатории Касперского» обязательно помогут вам.

Чтобы просмотреть статистику выполнения задачи проверки на вирусы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Проверка** (**Полная проверка**, **Быстрая проверка**), сформируйте задачу проверки и запустите ее на выполнение. Прогресс выполнения задачи будет отображаться в главном окне. Нажмите на ссылку **Подробно**, чтобы перейти в окно статистики.

Назначение единых параметров проверки для всех задач

Каждая задача проверки выполняется в соответствии со своими параметрами. По умолчанию задачи, сформированные при установке программы на компьютер, выполняются с параметрами, которые рекомендованы экспертами «Лаборатории Касперского».

Вы можете настроить единые параметры проверки для всех задач. За основу будет взят набор параметров, используемых при проверке на вирусы отдельного объекта.

Чтобы назначить единые параметры проверки для всех задач, выполните следующие действия:

1. Откройте окно настройки программы.
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.

Восстановление параметров проверки по умолчанию

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

Чтобы восстановить параметры проверки объектов по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
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 открывшемся окне в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

ОБНОВЛЕНИЕ ПРОГРАММЫ

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 программы. Важнейший элемент обеспечения актуальности защиты – обновление баз.

Обновление программы загружает и устанавливает на ваш компьютер:

- **Базы программы**

  Защита информации 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 базы настоятельно рекомендуется регулярно обновлять.

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

- **Модули программы**

  Помимо баз программы, можно обновлять и программные модули. Пакеты обновлений устраняют уязвимости Антивируса Касперского, добавляют новые функции или улучшают существующие.

Основным источником обновлений Антивируса Касперского служат 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 программы и базы на вашем компьютере сравниваются с расположенными в источнике обновлений. Если на вашем компьютере установлена последняя версия баз и модулей, на экран выводится информационное сообщение об актуальности защиты вашего компьютера. Если базы и модули различаются, на ваш компьютер будет установлена именно недостающая часть обновлений. Полного копирования баз и модулей не производится, что позволяет существенно увеличить скорость обновления и заметно снизить объем трафика.

Перед обновлением баз Антивирус Касперского создает их резервную копию, если по каким-либо причинам вы захотите вернуться к их использованию.

Возможность отката необходима, например, если вы обновили базы, и в процессе работы они были повреждены. Можно вернуться к предыдущему варианту баз, а позже попробовать обновить их еще раз.

Одновременно с обновлением программы вы можете выполнять копирование полученных обновлений в локальный источник. Данный сервис позволяет обновлять базы и модули программы 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 программы.

Вы можете перейти к отчету об обновлении, где будет представлена полная информация о событиях, произошедших в ходе выполнения задачи обновления. Также можно ознакомиться с обзором вирусной активности на сайте www.kaspersky.ru (ссылка **Обзор вирусной активности**).

Чтобы изменить параметры какой-либо задачи обновления, выполните следующие действия:

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в параметры выбранной задачи внесите необходимые изменения.

Чтобы перейти к отчету об обновлении, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Нажмите на кнопку **Отчеты**.

В этом разделе

Запуск обновления

В любой момент вы можете запустить обновление программы. Оно будет производиться из выбранного вами источника обновлений.

Запустить обновление Антивируса Касперского можно двумя способами:

- из контекстного меню;
- из главного окна программы.

Информация о процессе обновления будет отображаться в главном окне программы.

Обратите внимание, что при выполнении обновления одновременно будет произведено копирование обновлений в локальный источник, при условии, что данный сервис включен.

- *Чтобы запустить обновление Антивируса Касперского из контекстного меню, выполните следующие действия:*

  1. В области уведомлений панели задач нажмите правой клавишей мыши на значок программы.
  2. В раскрывшемся меню выберите пункт **Обновление**.

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

  1. Откройте главное окно программы.
  2. В левой части окна выберите раздел **Обновление**.
  3. Нажмите на кнопку **Выполнить обновление**. Процесс выполнения задачи будет отображаться в главном окне программы.

Откат последнего обновления

Каждый раз, когда вы запускаете обновление, Антивирус Касперского 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 программы 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 программы.
  2. В левой части окна выберите раздел **Обновление**.
  3. Нажмите на ссылку **Откат к предыдущим базам**.

Выбор источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Антивируса Касперского.

В качестве источника обновления вы можете использовать:

- *Сервер администрирования* – централизованное хранилище обновлений, расположенное на Сервере администрирования Kaspersky Administration Kit (подробнее смотрите Руководство администратора «Kaspersky Administration Kit»);
- *Серверы обновлений «Лаборатории Касперского»* – специальные интернет-сайты, на которые выкладываются обновления баз и модулей программы для всех продуктов «Лаборатории Касперского»;
- *HTTP- или FTP-серверы, локальные или сетевые каталоги* – локальный сервер или каталог, содержащий актуальный набор обновлений.

Если серверы обновлений «Лаборатории Касперского» вам недоступны (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- или HTTP-сайте, так и в локальном или сетевом каталоге.

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

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 программа обращается к ним строго по списку и обновляется с первого доступного источника.

Чтобы выбрать источник обновлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник обновлений** нажмите на кнопку **Добавить**.
6. В открывшемся окне **Выбор источника обновлений** выберите FTP-, HTTP-сайт или укажите его IP-адрес, символьное имя или URL-адрес.

Региональные настройки

Если в качестве источника обновлений вы используете серверы обновлений «Лаборатории Касперского», можно выбрать предпочтительное для вас местоположение сервера для загрузки обновлений. Серверы «Лаборатория Касперского» расположены 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 программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник обновлений** в блоке **Региональные параметры** выберите вариант **Выбрать из списка** и в раскрывающемся списке выберите ближайшую к вашему текущему местоположению страну.

   Если выбрать вариант **Определять автоматически**, то при обновлении будет использоваться информация о текущем регионе из реестра операционной системы.

Использование прокси-сервера

Если для выхода в интернет используется прокси-сервер, необходимо настроить его параметры.

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Параметры прокси** настройте параметры прокси-сервера.

Режим запуска: задание учетной записи

В Антивирусе Касперского реализован сервис запуска обновления программы от имени другой учетной записи (имперсонация). По умолчанию данный сервис отключен, и задачи запускаются от имени текущей учетной записи, под которой вы зарегистрированы в системе.

Поскольку обновление программы может производиться из источника, к которому у вас нет доступа (например, к сетевому каталогу обновлений) или прав авторизованного пользователя прокси-сервера, вы можете воспользоваться данным сервисом, чтобы запускать обновление программы от имени пользователя, обладающего такими привилегиями.

Обратите внимание, что без использования запуска с правами обновление по расписанию будет выполняться с правами текущей учетной записи. В том случае, если на компьютере в данный момент не зарегистрирован ни один пользователь, не настроен запуск обновления с правами и выполняется обновление по расписанию, оно будет запущено с правами SYSTEM.

Чтобы запустить задачу с правами другой учетной записи, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Режим запуска** установите флажок **Запускать задачу с правами учетной записи**. Ниже введите данные учетной записи, под которой будет запускаться задача: имя учетной записи и пароль.

Режим запуска: формирование расписания

Все задачи проверки на вирусы можно запускать вручную или по сформированному расписанию.

При формировании расписания запуска задач необходимо определить интервал, с которым должно выполняться обновление.

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

Чтобы настроить расписание запуска задачи проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.

5. В открывшемся окне **Расписание** внесите необходимые изменения.

Чтобы настроить автоматический запуск пропущенной задачи, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** нажмите на кнопку **Изменить**.
5. В открывшемся окне **Расписание** в блоке **Настройка расписания** установите флажок **Запускать пропущенную задачу**.

Изменение режима запуска задачи обновления

Режим запуска задачи обновления Антивируса Касперского вы выбираете в ходе работы мастера настройки программы (см. раздел «Настройка параметров обновления» на стр. 33). Выбранный режим запуска можно изменить.

Запуск задачи обновления может производиться в одном из следующих режимов:

- **Автоматически**. Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим обновления используется по умолчанию.

  Антивирус Касперского будет производить попытку обновления через интервал, указанный в предыдущем пакете обновлений, что позволяет автоматически регулировать частоту обновлений в случае вирусных эпидемий и других опасных ситуаций. Программа будет своевременно получать самые последние обновления баз, сетевых атак и модулей программы, что исключит возможность проникновения опасных программ на ваш компьютер.

- **По расписанию** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию.

- **Вручную**. В этом случае вы самостоятельно запускаете обновление программы. Антивирус Касперского обязательно уведомит вас о необходимости обновления.

Чтобы настроить режим запуска задачи обновления, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Режим запуска** выберите режим запуска задачи обновления. Если выбран режим обновления по расписанию сформируйте расписание.

Выбор предмета обновления

Предмет обновления определяет, что именно будет обновляться:

- базы программы;
- сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты;

- база сетевых атак, используемых в работе Анти-Хакера;
- модули программы.

Базы программы, сетевые драйверы и база сетевых атак обновляются всегда, а модули программы – только в том случае, если установлен специальный режим.

Если на момент обновления в источнике присутствует пакет модулей программы, Антивирус Касперского получит и установит его после перезагрузки компьютера. До перезагрузки полученные обновления модулей установлены не будут.

Если следующее обновление программы происходит до перезагрузки компьютера и установки полученных ранее обновлений модулей программы, будет произведено только обновление баз программы.

Чтобы в процессе обновления на ваш компьютер копировались и устанавливались обновления модулей программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне в блоке **Параметры обновления** установите флажок **Обновлять модули программы**.

Обновление из локальной папки

Процедура получения обновлений из локальной папки организована следующим образом:

1. Один из компьютеров сети получает пакет обновлений Антивируса Касперского с веб-серверов «Лаборатории Касперского» в интернете либо из другого веб-ресурса, содержащего актуальный набор обновлений. Полученные обновления помещаются в папку общего доступа.
2. Другие компьютеры сети для получения обновлений программы обращаются к папке общего доступа.

Антивирус Касперского 6.0 получает с серверов «Лаборатории Касперского» только собственный пакет обновлений. Копирование обновлений для других программ «Лаборатории Касперского» рекомендуется выполнять через Kaspersky Administration Kit.

Чтобы включить режим копирования обновлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В левой части окна выберите раздел **Обновление**.
3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.
4. В открывшемся окне нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Распространение обновлений** установите флажок **Копировать обновления в папку** и в поле ниже укажите путь к папке общего доступа, куда будут помещаться полученные обновления. Кроме того, путь можно выбрать в окне, открывающемся по кнопке **Обзор**.

Чтобы обновление программы выполнялось из выбранной папки общего доступа, выполните на всех компьютерах сети следующие действия:

1. Откройте главное окно программы.

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

3. Для выбранного раздела нажмите на ссылку с установленным режимом запуска.

4. В открывшемся окне нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Источник обновлений** нажмите на кнопку **Добавить**.

6. В открывшемся окне **Выбор источника обновлений** выберите папку или введите полный путь к ней в поле **Источник**.

7. На закладке **Источник обновлений** снимите флажок **Серверы обновлений «Лаборатории Касперского»**.

Статистика обновления

Общая информация о работе задач обновления приводится в окне статистики. Здесь вы можете узнать о событиях, возникших при выполнении задачи (закладка *События*) и просмотреть список параметров, в соответствии с которыми выполняется задача (закладка *Параметры*).

Если в результате выполнения задачи возникли какие-то ошибки, попробуйте запустить задачу еще раз. Если попытка завершится с ошибкой, сохраните отчет с результатами выполнения задачи в файл по кнопке **Сохранить как**. Затем отправьте отчет в Службу технической поддержки. Специалисты «Лаборатории Касперского» обязательно помогут вам.

Краткая статистика обновления приведена в верхней части окна статистики и содержит размер скопированных и установленных обновлений, скорость, с которой производилось обновление, длительность процедуры и другую информацию.

Чтобы просмотреть статистику выполнения задачи проверки на вирусы, выполните следующие действия:

1. Откройте главное окно программы.

2. В левой части окна выберите раздел **Обновление**, сформируйте задачу обновления и запустите ее на выполнение. Процесс выполнения задачи будет отображаться в главном окне. По ссылке **Подробно** можно перейти в окно статистики.

Возможные проблемы при обновлении

В процессе обновления программных модулей Антивируса Касперского или сигнатур угроз могут возникнуть ошибки, связанные с неверной настройкой обновления, проблемами связи и т. д. В данном разделе справки мы постараемся рассмотреть большинство ошибок и дать советы, как их устранить. При возникновении ошибок, не описанных в справке, а также для получения детальных рекомендаций по их устранению попытайтесь найти информацию в Базе знаний на интернет-портале Службы технической поддержки в разделе «Если программа выдала ошибку...». Если рекомендации, представленные в данном разделе, не помогли решить проблему, или информация об ошибке отсутствует в Базе знаний, отправьте запрос в Службу технической поддержки.

Ошибки конфигурации

Ошибки данной группы возникают преимущественно из-за неправильной установки программы либо из-за изменения конфигурации программы, приводящей к ее неработоспособности.

Общие рекомендации:

При возникновении ошибок данной группы рекомендуется повторить попытку запуска обновления. При повторении ошибки в дальнейшем обратитесь в Службу технической поддержки.

В случае, если проблема связана с неправильной установкой программы, рекомендуется переустановить ее.

Не указан ни один источник обновления

Ни один из источников не содержит файлов для обновления. Возможно, в параметрах обновления не указан ни один источник обновления. Проверьте корректность настройки параметров обновления и повторите попытку.

Ошибка проверки лицензии

Данная ошибка возникает в случае, если используемый программой файл ключа заблокирован и помещен в «черный» список лицензий.

Ошибка получения параметров обновления

Внутренняя ошибка при получении параметров задачи обновления. Пожалуйста, проверьте корректность настройки параметров обновления и повторите попытку.

Недостаточно прав на обновление

Данная ошибка обычно возникает при отсутствии прав доступа к источнику обновления или папке размещения обновлений у учетной записи, под которой обновление запускается. Рекомендуется проверить наличие прав у данной учетной записи.

Подобная ошибка возникает также при попытке копирования файлов обновления в папку, которая не может быть создана.

Внутренняя ошибка

Внутренняя ошибка логики работы задачи обновления. Пожалуйста, проверьте корректность параметров обновления и повторите попытку.

Ошибка проверки обновления

Данная ошибка возникает в случае, если файлы, загруженные с источника обновления, не прошли внутреннюю проверку. Пожалуйста, повторите попытку обновления позже.

Ошибки, возникающие при работе с папками и файлами

Ошибки данной группы возникают при ограничении либо отсутствии у учетной записи, от имени которой запускается обновление, прав на доступ к источнику обновления или папке размещения обновлений.

Общие рекомендации:

При возникновении ошибок данной группы рекомендуется проверить наличие прав на доступ к указанным файлам и папкам у данной учетной записи.

Невозможно создать папку

Данная ошибка возникает в случае, если невозможно создать папку в процессе выполнения процедуры обновления.

Недостаточно прав для выполнения файловой операции

Данная ошибка возникает в случае, если учетная запись, от имени которой запущено обновление, не обладает необходимыми правами для выполнения операций с файлами.

Не найден файл или папка

Данная ошибка возникает при отсутствии файла или папки, необходимых при обновлении. Рекомендуется проверить, что указанные файл, папка существуют и доступны.

Ошибка файловой операции

Данная ошибка является внутренней ошибкой логики работы модуля обновления при выполнении операций с файлами.

Сетевые ошибки

Ошибки данной группы возникают при наличии проблем связи либо при некорректной настройке параметров подключения к сети.

Общие рекомендации:

При возникновении ошибок данной группы рекомендуется проверить подключение вашего компьютера к сети, корректность настройки параметров подключения, доступность источника обновления. После этого повторите попытку обновления. В случае неудачи обратитесь в Службу технической поддержки.

Сетевая ошибка

В процессе получения файлов обновления произошла ошибка. При возникновении данной ошибки проверьте подключение вашего компьютера к сети.

Соединение разорвано

Данная ошибка возникает в том случае, если по каким-либо причинам разорвано соединение с источником обновления.

Истекло время ожидания сетевой операции

Превышено время ожидания соединения с источником обновления. При настройке параметров обновления программы вы могли установить строгий тайм-аут соединения с источником обновления. Если за данное время вашему компьютеру не удается подключиться к серверу или каталогу обновлений, возникает такая ошибка. Рекомендуем в этом случае проверить правильность настроек сервиса обновления, а также доступность источника обновления.

Ошибка авторизации на FTP-сервере

Данная ошибка возникает в случае, если неверно указаны параметры авторизации на FTP-сервере, который является источником обновления. Пожалуйста, убедитесь, что в параметрах FTP-сервера разрешена загрузка файлов для данной учетной записи.

Ошибка авторизации на прокси-сервере

Данная ошибка возникает в случае, если при настройке параметров обновления через прокси-сервер неверно указаны имя и пароль, либо учетная запись, от имени которой запускается обновление, не обладает правами доступа к источнику обновления. Пожалуйста, отредактируйте параметры авторизации и повторите попытку обновления.

Ошибка разрешения DNS-имени

Данная ошибка возникает в случае, если не обнаружен ни один источник обновления. Возможно, некорректно указан адрес источника обновления, неверны параметры соединения с сетью, либо недоступен DNS-сервер. Рекомендуется проверить параметры обновления, доступность источника обновления и повторить попытку.

Соединение с источником обновления не может быть установлено

Данная ошибка возникает, если нет связи с источником обновления. Пожалуйста, проверьте корректность адреса источника обновления и повторите попытку.

Соединение с прокси-сервером не может быть установлено

Данная ошибка возникает, если неверно указаны параметры подключения к прокси-серверу. Для решения проблемы рекомендуется проверить корректность данных параметров, доступность прокси-сервера, доступность сети и повторить попытку обновления.

Ошибка разрешения DNS-имени прокси-сервера

Данная ошибка возникает в случае, если не обнаружен прокси-сервер. Рекомендуется проверить корректность параметров подключения к прокси-серверу и доступность DNS-сервера.

Ошибки, связанные с повреждением баз

Ошибки данной группы связаны с наличием поврежденных файлов на источнике обновления.

Общие рекомендации:

При выполнении обновления с веб-серверов «Лаборатории Касперского» повторите попытку запуска обновления. В случае неудачи обратитесь в Службу технической поддержки.

При обновлении из другого источника (например, из локальной папки) рекомендуется обновить его содержимое с веб-серверов «Лаборатории Касперского». В случае повторения ошибки обратитесь в Службу технической поддержки.

Файл отсутствует на источнике обновления

Все файлы, которые скачиваются и устанавливаются на ваш компьютер в процессе обновления, перечисляются в специальном файле, включенном в пакет. Данная ошибка возникает в том случае, если какой-либо файл присутствует в списке обновляемых, но отсутствует на источнике обновления.

Ошибка проверки подписи

Данная ошибка может быть возвращена программой в случае, если электронная цифровая подпись загружаемого пакета обновлений повреждена либо не соответствует подписи «Лаборатории Касперского».

Индексный файл поврежден или отсутствует

Данная ошибка возникает, если на источнике обновления отсутствует либо поврежден индексный файл в формате xml, согласно которому выполняется обновление.

Ошибки, связанные с обновлением с Сервера администрирования Kaspersky Administration Kit

Ошибки данной группы связаны с наличием проблем обновления программы через Сервер администрирования Kaspersky Administration Kit.

Общие рекомендации:

В первую очередь убедитесь, что программа Kaspersky Administration Kit и ее компоненты (Сервер администрирования и Агент администрирования) установлены и запущены. Повторите попытку обновления. В случае неудачи перезапустите Агент администрирования и Сервер администрирования, повторите попытку обновления еще раз. Если решить проблему не удалось, обратитесь в Службу технической поддержки.

Ошибка соединения с Сервером администрирования

Данная ошибка возникает, если подключение к Серверу администрирования Kaspersky Administration Kit невозможно. Рекомендуется проверить, что Агент администрирования установлен и запущен.

Ошибка регистрации в Агенте администрирования

При возникновении данной ошибки следуйте общим рекомендациям по устранению ошибок данной группы. Если ошибка повторится, соберите подробный файл отчета (трассировку) обновления и Агента администрирования на этом компьютере и отправьте их в Службу технической поддержки через веб-форму, сопроводив описанием ситуации.

Невозможно установить соединение. Сервер администрирования перегружен и не может обслужить запрос

В данном случае попытку обновления рекомендуется произвести позже.

Невозможно установить соединение с Сервером администрирования / Главным Сервером администрирования / Агентом администрирования, физическая ошибка / неизвестная ошибка

При возникновении подобных ошибок рекомендуется повторить попытку обновления позже. В случае неудачи обратитесь в Службу технической поддержки.

Ошибка получения файла с Сервера администрирования, неверный аргумент для транспорта

Если данная ошибка будет воспроизводиться в дальнейшем, обратитесь в Службу технической поддержки.

Ошибка получения файла с Сервера администрирования

При возникновении подобных ошибок рекомендуется повторить попытку обновления позже. В случае неудачи обратитесь в Службу технической поддержки.

Разные коды

В данную группу включены ошибки, не относящиеся ни к одной из перечисленных выше групп.

Отсутствуют файлы для операции отката

Данная ошибка возникает, если после выполненного отката обновлений произошла еще одна попытка отката, но между ними не было произведено обновление. Повторная операция отката будет невозможна до тех пор, пока не будет выполнено успешное обновление, в результате которого будет восстановлен резервный набор файлов.

НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ

Окно настройки параметров программы предназначено для быстрого доступа к основным настройкам Антивируса Касперского 6.0.

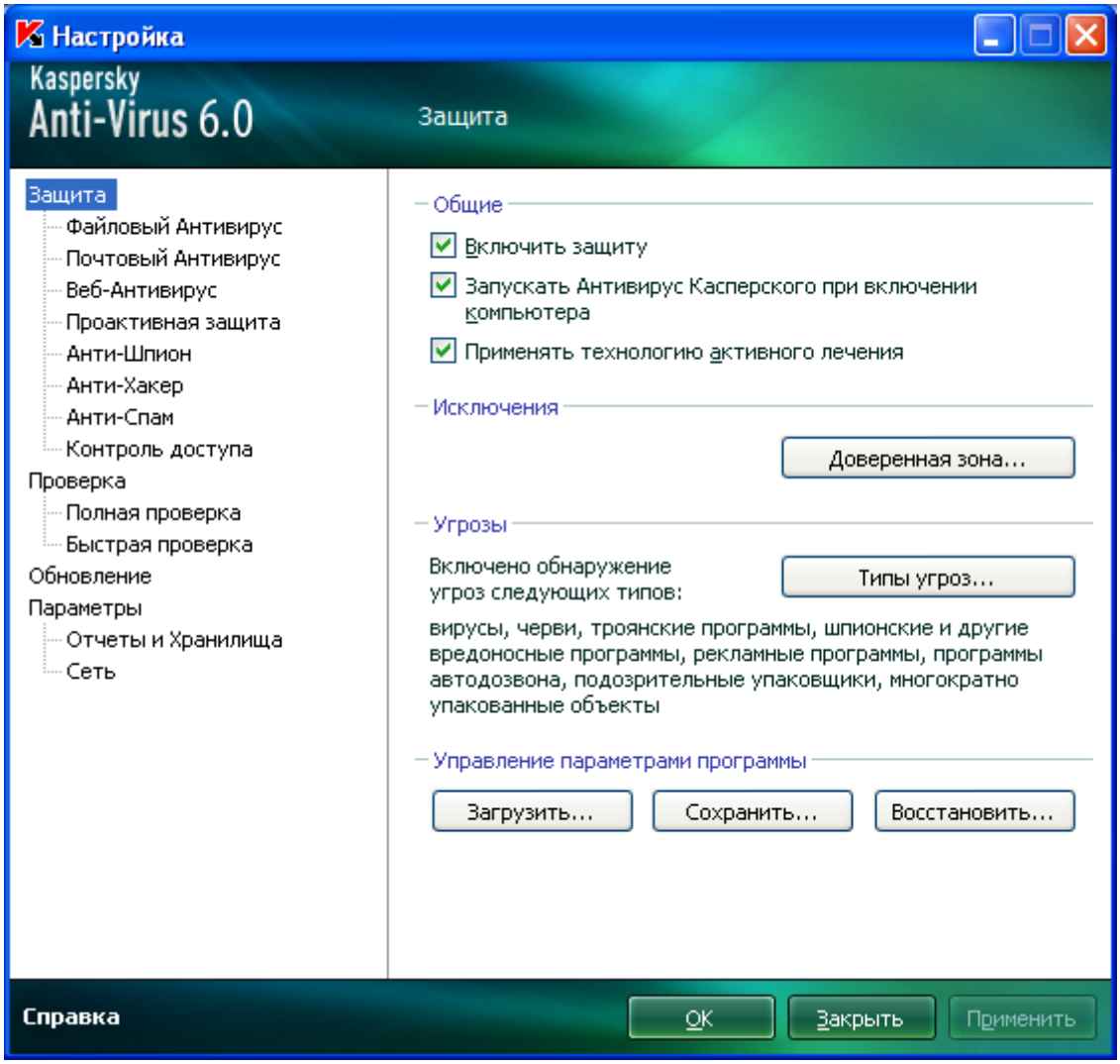


Рисунок 9. Окно настроек параметров приложения

Окно состоит из двух частей:

- левая часть обеспечивает доступ к компонентам Антивируса Касперского, задачам проверки на вирусы, обновления и т. д;
- правая часть окна содержит перечень параметров выбранного в левой части компонента, задачи и т. п.

Открыть окно можно несколькими способами:

- Из главного окна программы. Для этого нажмите на кнопку **Настройка** в верхней части главного окна.

- Из контекстного меню. Для этого выберите пункт **Настройка** в контекстном меню программы.

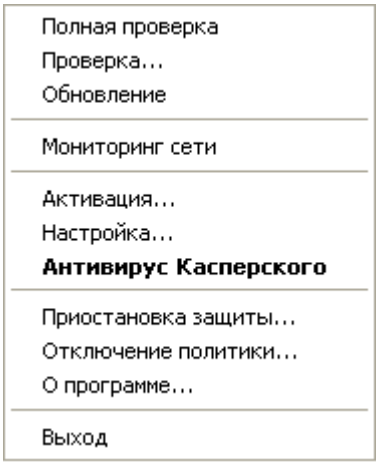


Рисунок 10. Контекстное меню

- Из контекстного меню для отдельных компонентов. Для этого выберите пункт **Настройка** в меню.

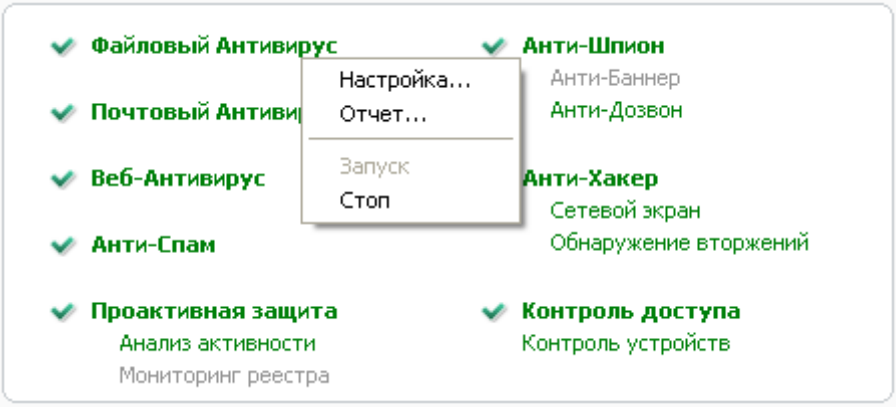


Рисунок 11. Вызов окна настройки параметров из контекстного меню для отдельного компонента

В этом разделе

Защита

В окне **Защита** вы можете воспользоваться следующими дополнительными функциями Антивируса Касперского:

- Отключение / включение защиты программы (см. стр. 152).
- Запуск программы при старте операционной системы (см. стр. 153).
- Использование технологии активного лечения (см. стр. 153).
- Выбор категорий обнаруживаемых угроз (см. стр. 154).
- Формирование доверенной зоны (см. стр. 154):
  - создание правила исключения (см. стр. 155);
  - задание дополнительных параметров исключения (см. стр. 156);
  - формирование списка доверенных программ (см. стр. 157);
  - экспорт / импорт компонентов доверенной зоны (см. стр. 158).
- Экспорт / импорт параметров работы программы (см. стр. 159).
- Восстановление параметров работы программы по умолчанию (см. стр. 159).

Отключение / включение защиты компьютера

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

Вы можете отключить защиту, обеспечиваемую программой, 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 (серые) названия выключенных компонентов в главном окне программы;
- неактивный (серый) значок программы в области уведомлений панели задач;
- красный цвет индикатора безопасности.

Обратите внимание, что в данном случае защита рассматривается именно в контексте компонентов защиты. Отключение работы компонентов защиты не оказывает влияния на выполнение задач проверки на вирусы и обновления Антивируса Касперского.

Чтобы отключить защиту полностью, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. Снимите флажок **Включить защиту**.

ЗАПУСК ПРОГРАММЫ ПРИ СТАРТЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Если по какой-либо причине вам требуется полностью завершить работу Антивируса Касперского, выберите пункт **Выход** контекстного меню программы. В результате программа будет выгружена из оперативной памяти. Это подразумевает, что в данный период компьютер работает в незащищенном режиме.

Теперь включить защиту компьютера снова вы можете, загрузив программу из меню **Пуск** → **Программы** → **Антивирус Касперского 6.0** → **Антивирус Касперского 6.0**.

Кроме того, защита может быть запущена автоматически после перезагрузки операционной системы.

Чтобы включить режим запуска программы при старте операционной системы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. Установите флажок **Запускать Антивирус Касперского при включении компьютера**.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ АКТИВНОГО ЛЕЧЕНИЯ

Современные вредоносные программы могут внедряться на самые низкие уровни операционной системы, что делает процесс их удаления практически невозможным. При обнаружении угрозы, которая в данный момент активна в системе, Антивирус Касперского 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 этого рекомендуется запустить полную проверку на вирусы.

Чтобы применить технологию расширенного лечения, выполните следующие действия:

1. Откройте окно настройки программы.

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

3. Установите флажок **Применять технологию активного лечения**.

Выбор категорий обнаруживаемых угроз

Антивирус Касперского предлагает вам защиту от разных видов вредоносного программного обеспечения. Вне зависимости от установленных параметров, программа всегда проверяет и обезвреживает вирусы и троянские программы. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера вы можете расширить список обнаруживаемых угроз, включив контроль потенциально опасных программ разного рода.

Чтобы выбрать категории обнаруживаемых угроз, выполните следующие действия:

1. Откройте окно настройки программы.

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

3. В блоке **Угрозы** нажмите на кнопку **Типы угроз**.

4. В открывшемся окне **Типы угроз** установите флажки для тех категорий угроз, от которых вы хотите защитить свой компьютер.

Формирование доверенной зоны

Доверенная зона – это сформированный пользователем перечень объектов, которые Антивирус Касперского не контролирует в процессе своей работы. Другими словами, это набор исключений из защиты программы.

Доверенную зону пользователь формирует самостоятельно, в зависимости от особенностей объектов, с которыми он работает, а также от того, какие программы установлены на его компьютере. Создание такого списка исключений может потребоваться, например, в случае, если Антивирус Касперского блокирует доступ к какому-либо объекту или программе, а вы уверены, что данный объект / программа абсолютно безвредны.

Исключать из проверки можно файл определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по классификации Вирусной энциклопедии (статусу, присвоенному объекту Антивирусом Касперского при проверке).

Объект исключения не подлежит проверке, если проверяется диск или папка, в которой он расположен. Однако при выборе проверки именно этого объекта правило исключения применено не будет.

Чтобы сформировать список исключений из защиты, выполните следующие действия:

1. Откройте окно настройки программы.

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

3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.

4. В открывшемся окне настройте правила исключений для объектов (см. стр. 155), а также сформируйте список доверенных программ (см. стр. 157).

См. также

СОЗДАНИЕ ПРАВИЛА ИСКЛЮЧЕНИЯ

Правило исключения – это совокупность условий, при которых объект не будет проверяться Антивирусом Касперского.

Исключать из проверки можно файл определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по классификации Вирусной энциклопедии.

Тип угрозы – это статус, который присвоен объекту Антивирусом Касперского при проверке. Статус присваивается на основании классификации вредоносных и потенциально опасных программ, представленных в Вирусной энциклопедии «Лаборатории Касперского».

Потенциально опасное программное обеспечение не имеет какой-либо вредоносной функции, но может быть использовано в качестве вспомогательного компонента 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 Антивирусом Касперского, смотрите в Вирусной энциклопедии на сайте www.viruslist.ru (http://www.viruslist.com/ru/viruses/encyclopedia)). В результате проверки такие программы могут быть заблокированы. Поскольку некоторые из них широко применяются пользователями, предусмотрена возможность исключить их из проверки. Для этого нужно добавить в доверенную зону имя или маску угрозы по классификации Вирусной энциклопедии.

Например, вы часто используете в своей работе программу Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. Такая активность программы рассматривается Антивирусом Касперского как потенциально опасная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключающее правило, где в качестве классификации указать Remote Admin.

При добавлении исключения формируется правило, которое потом может использоваться некоторыми компонентами программы (Файловый Антивирус, Почтовый Антивирус, Проактивная защита, Веб-Антивирус), а также при выполнении задач проверки на вирусы

Чтобы создать правило исключения, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Правила исключений** нажмите на кнопку **Добавить**.

5. В открывшемся окне **Правило исключения** в блоке **Параметры** выберите тип исключения. Затем в блоке **Описание** задайте значения для выбранных типов исключений и определите, в работе каких компонентов Антивируса Касперского должно быть использовано создаваемое правило.

Чтобы создать правило исключения из окна отчета, выполните следующие действия:

1. В отчете выберите объект, который вы хотите добавить к исключениям.

2. В контекстном меню для этого объекта выберите пункт **Добавить в доверенную зону**.

3. Откроется окно **Правило исключения**. Убедитесь, что все параметры исключающего правила вас устраивают. Поля с именем объекта и типом угрозы, который ему присвоен, заполняются автоматически на основании информации из отчета. Для создания правила нажмите на кнопку **ОК**.

Дополнительные параметры исключения

Для некоторых объектов по типу угрозы 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 можно 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 окне **Правило исключений** 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 символ;

   - **C:\dir\test** – только файл *C:\dir\test.*

     Чтобы не проверялись файлы во всех вложенных папках указанного каталога, при создании маски установите флажок **Включая вложенные папки**.

3. Маски путей 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 символ.

  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 классификации исключаемой угрозы согласно Вирусной энциклопедии. В этом случае указанная угроза не будет обнаруживаться во всех объектах. Использование данных масок без указания классификации равносильно отключению защиты. Не рекомендуется также выбирать в качестве исключения путь, относящийся к виртуальному диску, сформированному на основе каталога файловой системы посредством команды subst, или к диску, который является отображением сетевой папки. Дело в том, что разные пользователи компьютера могут обозначать одним и тем же именем диска разные ресурсы, что неизбежно приведет к некорректному срабатыванию правил исключения.

См. также

Разрешенные маски исключений по классификации Вирусной энциклопедии 157

Разрешенные маски исключений по классификации Вирусной энциклопедии

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 (http://www.viruslist.com/ru/viruses/encyclopedia) (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.

См. также

Разрешенные маски исключений файлов 156

Формирование списка доверенных программ

Вы можете формировать список доверенных программ, активность которых, в том числе и подозрительная, а также файловая, сетевая активность и обращения 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 программ. Однако исполняемый файл и процесс доверенной программы по-прежнему будут проверяться на вирусы. Для полного исключения программы из проверки следует пользоваться правилами исключений (см. раздел «Создание правила исключения» на стр. 155).

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 Антивируса Касперского с другими программами (например, сетевой трафик с другого компьютера, уже проверенный антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

По умолчанию Антивирус Касперского проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и сетевой трафик, создаваемый ими.

Чтобы добавить программу в список доверенных, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Доверенные программы** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Доверенная программа** выберите программу воспользовавшись кнопкой **Обзор**. Будет открыто контекстное меню, в котором из пункта **Обзор** вы можете перейти в стандартное окно выбора файлов и указать путь к исполняемому файлу, или из пункта **Программы** перейти к списку программ, работающих в данный момент, и выбрать нужную. Для выбранной программы укажите нужные параметры.

Экспорт / импорт компонентов доверенной зоны

С помощью экспорта и импорта вы можете переносить сформированные правила исключений и списки доверенных программ на другие компьютеры.

Чтобы копировать сформированные правила исключений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Правила исключений** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию правил.

Чтобы копировать сформированный список доверенных программ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Исключения** нажмите на кнопку **Доверенная зона**.
4. В открывшемся окне на закладке **Доверенные программы** воспользуйтесь кнопками **Экспорт** и **Импорт**, чтобы выполнить необходимые действия по копированию списка.

Экспорт / импорт параметров работы Антивируса Касперского

Антивирус Касперского предоставляет возможность экспортировать и импортировать свои параметры.

Это полезно, например, в том случае, когда программа установлена у вас на домашнем компьютере и в офисе. Дома вы можете настроить программу на удобный для себя режим работы, 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 программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** 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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** нажмите на кнопку **Загрузить**.
4. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Антивируса Касперского.

Восстановление параметров по умолчанию

Вы всегда можете вернуться к рекомендуемым параметрам работы Антивируса Касперского. Они считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского». Восстановление настроек осуществляется Мастером первоначальной настройки программы.

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 Антивируса Касперского, параметры которых были изменены пользователем или накоплены программой в результате обучения компонентов Сетевой экран и Анти-Спам. Если для какого-либо компонента в процессе работы были сформированы уникальные параметры, они также будут представлены в списке.

К таким уникальным параметрам относятся «белые» и «черные» списки фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, используемых компонентами Веб-Антивирус и Анти-Шпионом, сформированные правила исключений защиты для компонентов программы, правила фильтрации пакетов и программ Сетевого экрана.

Данные списки формируются в процессе работы с программой, исходя из индивидуальных задач и требований безопасности, и их формирование зачастую занимает много времени. Поэтому мы рекомендуем сохранять их при восстановлении первоначальных настроек программы.

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 программы.
2. В левой части окна выберите раздел **Защита**.
3. В блоке **Управление параметрами программы** 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.

Файловый Антивирус

В окне сгруппированы параметры для компонента **Файловый Антивирус** (см. раздел «Антивирусная защита файловой системы компьютера» на стр. 47). Изменяя значения параметров, вы можете:

- изменять уровень безопасности (см. стр. 49);
- изменять действие над обнаруженными объектами (см. стр. 50);
- формировать область защиты (см. стр. 51);
- оптимизировать проверку (см. стр. 52);
- настраивать проверку составных файлов (см. стр. 53);
- изменять режим проверки (см. стр. 54);
- использовать эвристический анализ (см. стр. 52);
- приостанавливать работу компонента (см. стр. 55);
- выбирать технологию проверки (см. стр. 54);
- восстанавливать параметры защиты по умолчанию (см. стр. 56), если они были изменены;
- отключать работу Файлового Антивируса.

Чтобы отключить использование Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Файловый Антивирус**.
3. В правой части окна снимите флажок **Включить Файловый Антивирус**.

Чтобы перейти к настройке параметров Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Файловый Антивирус**.
3. В правой части окна выберите уровень безопасности и реакцию на угрозу для компонента. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров Файлового Антивируса.

Почтовый Антивирус

В окне сгруппированы параметры для компонента **Почтовый Антивирус** (см. раздел «Антивирусная защита почты» на стр. 58). Изменяя значения параметров, вы можете:

- изменять уровень безопасности (см. стр. 60);
- изменять действие над обнаруженными объектами (см. стр. 61);
- формировать область защиты (см. стр. 62);
- изменять методы проверки (см. стр. 62);
- использовать эвристический анализ (см. стр. 64);
- настраивать проверку составных файлов (см. стр. 65);
- настраивать условия фильтрации объектов, вложенных в почтовое сообщение (см. стр. 65);
- восстанавливать параметры защиты по умолчанию (см. стр. 66);
- отключать работу Почтового Антивируса.

Чтобы отключить использование Почтового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Почтовый Антивирус**.
3. В правой части окна снимите флажок **Включить Почтовый Антивирус**.

Чтобы перейти к настройке параметров Почтового Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Почтовый Антивирус**.
3. В правой части окна выберите уровень безопасности и реакцию на угрозу для компонента. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров Почтового Антивируса.

В окне сгруппированы параметры для компонента **Веб-Антивирус** (см. раздел «Веб-защита» на стр. 68). Изменяя значения параметров, вы можете:

- изменять уровень безопасности (см. стр. 70);
- изменять действие (см. стр. 70) над обнаруженными объектами;
- формировать область защиты (см. стр. 71);
- изменять методы проверки (см. стр. 71);
- оптимизировать проверку (см. стр. 73);
- использовать эвристический анализ (см. стр. 72);
- восстанавливать параметры веб-защиты по умолчанию (см. стр. 73);
- отключать работу Веб-Антивируса.

Чтобы отключить использование Веб-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Веб-Антивирус**.
3. В правой части окна снимите флажок **Включить Веб-Антивирус**.

Чтобы перейти к настройке параметров Веб-Антивируса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Веб-Антивирус**.
3. В правой части окна выберите уровень безопасности и реакцию на угрозу для компонента. Нажмите на кнопку **Настройка**, чтобы перейти к настройкам других параметров Веб-Антивируса.

Проактивная защита

В окне сгруппированы параметры для компонента **Проактивная защита** (см. раздел «Проактивная защита вашего компьютера» на стр. 75). Изменяя значения параметров, вы можете:

- управлять списком (см. стр. 77) опасной активности;
- изменять реакцию программы на опасную активность (см. стр. 77) в системе;
- контролировать системные учетные записи (см. стр. 78);
- управлять списком (см. стр. 82) правил контроля системного реестра;
- создавать правила для контроля объектов реестра (см. стр. 83);
- создавать группы контролируемых объектов системного реестра (см. стр. 82);
- отключать работу модулей Анализ активности (см. стр. 76) и Мониторинг системного реестра (см. стр. 81);
- отключать работу Проактивной защиты.

Чтобы отключить использование Проактивной защиты, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Проактивная защита**.
3. В правой части окна снимите флажок **Включить Проактивную защиту**.

*Чтобы отключить использование **Анализа активности** или **Мониторинга системного реестра**, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Проактивная защита**.
3. В правой части окна снимите флажок **Включить анализ активности** или флажок **Включить мониторинг системного реестра**.

Чтобы перейти к настройке параметров Проактивной защиты, выполните следующие действия:

1. Откройте окно настройки программы.

2. В левой части окна выберите раздел **Проактивная защита**.

3. В правой части окна в блоке **Анализ активности** или в блоке **Мониторинг системного реестра** нажмите на кнопку **Настройка**.

Анти-Шпион

В окне сгруппированы параметры для компонента **Анти-Шпион** (см. раздел «Защита от рекламы и интернет-мошенничества» на стр. 85). Изменяя значения параметров, вы можете:

- формировать список разрешенных адресов баннеров (см. стр. 86);
- формировать список запрещенных адресов баннеров (см. стр. 86);
- экспортировать / импортировать списки баннеров (см. стр. 87);
- формировать список доверенных номеров (см. стр. 88);
- отключать работу модулей Анти-Баннер (см. стр. 85) и Анти-Дозвон (см. стр. 88);
- отключать работу Анти-Шпиона.

Чтобы отключить использование Анти-Шпиона, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Шпион**.
3. В правой части окна снимите флажок **Включить Анти-Шпион**.

*Чтобы отключить использование **Анти-Баннера** или **Анти-Дозвона**, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Шпион**.
3. В правой части окна снимите флажок **Включить Анти-Баннер** (**Включить Анти-Дозвон**).

Чтобы перейти к настройке параметров Анти-Шпиона, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Шпион**.
3. В правой части окна в блоке **Анти-Баннер** или в блоке **Анти-Дозвон** нажмите на кнопку **Настройка**.

Анти-Хакер

В окне сгруппированы параметры для компонента **Анти-Хакер** (см. раздел «Защита от сетевых атак» на стр. 89). Изменяя значения параметров, вы можете:

- изменять уровень защиты от сетевых атак (см. стр. 91);
- создавать правила для программ вручную (см. стр. 92) и на основе шаблона (см. стр. 93);
- создавать правила для пакетов (см. стр. 94);
- изменять приоритет созданного правила (см. стр. 94);

- экспортировать / импортировать сформированные правила (см. стр. 95);
- детально настраивать правила для программ и пакетов (см. стр. 95);
- создавать правила для зон безопасности (см. стр. 98);
- изменять статус зоны безопасности (см. стр. 100);
- включать / отключать режим невидимости (см. стр. 100);
- изменять режим работы Сетевого экрана (см. стр. 101);
- отключать работу модулей Сетевой экран и Система обнаружения вторжений (см. стр. 101);
- отключать работу Анти-Хакера.

Чтобы отключить использование Анти-Хакера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Хакер**.
3. В правой части окна снимите флажок **Включить Анти-Хакер**.

*Чтобы отключить использование **Сетевого экрана** или **Системы обнаружения вторжений**, выполните следующие действия:*

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Хакер**.
3. В правой части окна снимите флажок **Включить сетевой экран** или флажок **Включить систему обнаружения вторжений**.

Чтобы перейти к настройке параметров Анти-Хакера, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Хакер**.
3. В правой части окна в блоке **Сетевой экран** нажмите на кнопку **Настройка**.

Анти-Спам

В окне сгруппированы параметры для компонента **Анти-Спам** (см. раздел «Защита от нежелательной почты» на стр. 106). Изменяя значения параметров, вы можете:

- изменять уровень агрессивности (см. стр. 112);
- использовать Диспетчер Писем (см. стр. 112);
- исключать из проверки сообщения Microsoft Exchange Server (см. стр. 113);
- изменять методы проверки (см. стр. 114);
- выбирать технологию фильтрации спама (см. стр. 114);
- определять факторы спама и потенциального спама (см. стр. 115);

- использовать дополнительные признаки фильтрации спама (см. стр. 115);
- формировать список разрешенных отправителей (см. стр. 116);
- формировать список разрешенных фраз (см. стр. 117);
- импортировать список разрешенных отправителей (см. стр. 117);
- формировать список запрещенных отправителей (см. стр. 118);
- формировать список запрещенных фраз (см. стр. 118);
- настраивать обработку спама в Microsoft Office Outlook (см. стр. 120), Microsoft Outlook Express (Windows Mail) (см. стр. 121), The Bat! (см. стр. 122);
- обучать Анти-Спам с помощью мастера обучения (см. стр. 109), на исходящих сообщениях (см. стр. 110), с помощью почтового клиента (см. стр. 110), с помощью отчетов (см. стр. 111);
- отключать работу Анти-Спама.

Чтобы отключить использование Анти-Спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Спам**.
3. В правой части окна снимите флажок **Включить Анти-Спам**.

Чтобы перейти к настройке параметров Анти-Спама, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Анти-Спам**.
3. В правой части окна в блоке **Уровень агрессивности** нажмите на кнопку **Настройка**.

ПРОВЕРКА

То, каким образом осуществляется проверка объектов на вашем компьютере, определяется набором параметров, заданных для каждой задачи.

Специалистами ЗАО «Лаборатория Касперского» выделены несколько задач проверки на вирусы. В их число входят следующие:

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 (см. стр. 129), на основе параметров которого будет выполняться задача;
- выбрать действие (см. стр. 130), которое будет применено программой при обнаружении зараженного / возможно зараженного объекта;
- сформировать расписание (см. стр. 135) автоматического запуска задачи;
- определить типы файлов (см. стр. 131), анализируемые на вирусы;
- определить параметры проверки составных файлов (см. стр. 132);
- выбрать методы и технологии проверки (см. стр. 133);
- назначить единые параметры проверки для всех задач (см. стр. 136).

Чтобы перейти к настройке параметров задачи, выполните следующие действия:

1. Откройте окно настройки программы.
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 **По умолчанию**.

Обновление

Обновление Антивируса Касперского осуществляется в соответствии с параметрами, которые определяют:

- с какого ресурса (см. стр. 140) производится копирование и установка обновлений программы;
- в каком режиме (см. стр. 143) запускается процесс обновления программы, и что именно обновляется (см. стр. 143);
- как часто требуется запускать обновление, в случае если настроен запуск по расписанию (см. стр. 142);
- от имени какой учетной записи (см. стр. 142) будет запущено обновление;
- требуется ли копировать полученные обновления в локальный источник (см. стр. 144);
- использование прокси-сервера (см. стр. 141).

Чтобы перейти к настройке параметров обновления, выполните следующие действия:

1. Откройте окно настройки программы.
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.

Параметры

В окне **Параметры** вы можете воспользоваться следующими дополнительными функциями Антивируса Касперского:

САМОЗАЩИТА ПРОГРАММЫ

Антивирус Касперского обеспечивает безопасность компьютера от воздействия вредоносных программ и в силу этого само становится объектом интереса вредоносного программного обеспечения, пытающегося заблокировать работу программы или даже удалить ее с компьютера.

Чтобы обеспечить стабильность системы безопасности вашего компьютера, в программу добавлены механизмы самозащиты и защиты от удаленного воздействия.

В 64-разрядных операционных системах Microsoft Windows Vista (без установленных Пакетов обновлений) и Microsoft Windows XP доступна только защита от изменений или удаления файлов программы на диске, а также записей в системном реестре.

При использовании защиты от удаленного воздействия возникает необходимость предоставить доступ к управлению программой программ удаленного администрирования (например, RemoteAdmin). Для этого следует добавить эти программы в список доверенных программ и включить для них параметр **Разрешать взаимодействие с интерфейсом программы**.

Чтобы включить использование механизмов самозащиты программы, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Самозащита** установите флажок **Включить самозащиту**, чтобы задействовать механизм защиты программы 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 программы.

   При попытке выполнить какое-либо из перечисленных действий над значком программы в области уведомлений панели задач Microsoft Windows будет открыто уведомление (если сервис уведомлений не отключен пользователем).

ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

Персональный компьютер может использоваться несколькими людьми, в том числе имеющими разные уровни компьютерной грамотности. Открытый доступ к программе, его параметрам может значительно снизить уровень безопасности компьютера в целом.

Чтобы повысить безопасность компьютера, используйте пароль для доступа к Антивирусу Касперского. Вы можете заблокировать все операции за исключением работы с уведомлениями об обнаружении опасных объектов; или запретить выполнение одного из следующих действий:

- изменение параметров работы программы;
- завершение работы программы;
- отключение работы компонентов защиты и задач проверки;
- отключение политики (при работе программы через Kaspersky Administration Kit);
- удаление программы.

Каждое из перечисленных выше действий приводит к снижению уровня защиты вашего компьютера, поэтому постарайтесь определить, кому из пользователей компьютера вы доверяете выполнять такие действия.

Чтобы защитить доступ к программе с помощью пароля, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
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 выполнить на вашем компьютере выбранные вами действия программа всегда будет запрашивать пароль.

Работа программы на портативном компьютере

В целях экономии питания портативного компьютера (заряда аккумулятора) вы можете отложить выполнение задач проверки и обновления.

Поскольку проверка на вирусы на компьютере и обновление программы подчас требуют достаточного количества ресурсов и занимают некоторое время, мы рекомендуем отключать запуск таких задач по расписанию. Это позволит вам сэкономить заряд аккумулятора. По мере необходимости вы сможете самостоятельно обновить программу или запустить проверку на вирусы.

Чтобы воспользоваться сервисом экономии заряда аккумулятора, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Ресурсы** установите флажок **Не запускать задачи по расписанию при работе от аккумулятора**.

Ограничение размера iSwift-файлов

iSwift-файлы – это файлы, содержащие информацию об уже проверенных на содержание вирусов объектах файловой системы NTFS (технология iSwift). Наличие таких файлов позволяет ускорить проверку объектов, поскольку Антивирус Касперского проверяет только те объекты, которые изменились со времени последней проверки. Со временем iSwift-файлы достигают большого размера. Рекомендуем вам установить ограничение размера таких файлов. При достижении заданного значения iSwift-файл будет очищен.

Чтобы ограничить размер iSwift-файлов, выполните следующие действия:

1. Откройте окно настройки программы.

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

3. В блоке **Ресурсы** установите флажок **Обнулять базу iSwift по достижении** и рядом укажите размер базы в мегабайтах.

УВЕДОМЛЕНИЯ О СОБЫТИЯХ АНТИВИРУСА КАСПЕРСКОГО

В процессе работы Антивируса Касперского возникают различного рода события. Они могут иметь информационный характер или нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении программы, а может фиксировать ошибку в работе некоторого компонента, которую необходимо срочно устранить.

Чтобы быть в курсе событий в работе Антивируса Касперского, воспользуйтесь сервисом уведомлений.

Уведомления могут быть реализованы одним из следующих способов:

- всплывающие сообщения над значком программы в системной панели;
- звуковое оповещение;
- сообщения электронной почты;
- запись информации в журнал событий.

Чтобы воспользоваться сервисом уведомлений, выполните следующие действия:

1. Откройте окно настройки программы.

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

3. В блоке **Вид** установите флажок **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.

4. В открывшемся окне **Настройка уведомлений** определите типы событий Антивируса Касперского, о возникновении которых вы хотите быть уведомлены, а также способ уведомления.

См. также

ВЫБОР ТИПА СОБЫТИЯ И СПОСОБА ОТПРАВКИ УВЕДОМЛЕНИЙ

В процессе работы Антивируса Касперского возникают события следующих типов:

- **Критические события** – события критической важности, уведомления о которых настоятельно рекомендуется получать, поскольку они указывают на проблемы в работе программы или на уязвимости в защите вашего компьютера. Например, *базы сильно устарели* или *срок действия лицензии истек*.

- **Отказ функциональности** – события, приводящие к неработоспособности программы. Например, *базы отсутствуют или повреждены*.

- **Важные события** – события, на которые обязательно нужно обратить внимание, поскольку они отражают важные ситуации в работе программы. Например, *базы устарели* или *срок действия лицензии скоро закончится*.

- **Информационные события** – события справочного характера, как правило, не несущие важной информации. Например, *объект помещен на карантин*.

Чтобы указать, о каких событиях и каким образом вы должны быть уведомлены, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки для тех событий и тех способов отправки уведомлений, для которых хотите получать уведомления.

Настройка отправки уведомлений по электронной почте

После того как выбраны события (см. раздел «Выбор типа события и способа отправки уведомлений» на стр. 169), уведомления о возникновении которых вы хотите получать по электронной почте, следует настроить отправку уведомлений.

Чтобы настроить отправку уведомлений по электронной почте, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки для нужных событий в графе **Email** и нажмите на кнопку **Настройка email**.
5. В открывшемся окне **Настройка параметров почтовых уведомлений** задайте необходимые значения параметров. Для уведомления о событиях за определенный промежуток времени сформируйте расписание отправки информационного письма, нажав на кнопку **Изменить**. В открывшемся окне **Расписание** внесите необходимые изменения.

Настройка параметров журнала событий

Антивирус Касперского предоставляет возможность вносить информацию о событиях, возникающих в работе программы, в общий журнал событий Microsoft Windows (**Программа**) либо в отдельный журнал событий Антивируса Касперского (**Kaspersky Event Log**).

Просмотр журналов осуществляется в стандартном окне Microsoft Windows **Event Viewer**, которое можно вызвать с помощью команды **Пуск/Настройка/Панель управления/Администрирование/Просмотр событий**.

Чтобы настроить параметры журнала событий, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите флажок **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.
4. В открывшемся окне **Настройка уведомлений** установите флажки для нужных событий в графе **Журнал** и нажмите на кнопку **Настройка журнала**.

5. В открывшемся окне **Параметры журнала событий** выберите журнал, в который будет записываться информация о событиях.

АКТИВНЫЕ ЭЛЕМЕНТЫ ИНТЕРФЕЙСА

Под активными элементами интерфейса понимаются следующие возможности Антивируса Касперского:

Анимировать значок в области уведомлений панели задач.

В зависимости от выполняемой программой операции значок в системной панели меняется. Так, например, при проверке почтового сообщения на фоне значка появляется небольшая пиктограмма письма. По умолчанию анимация значка программы используется. В этом случае значок будет отражать только статус защиты вашего компьютера: если защита включена, значок будет цветным, а если она приостановлена или выключена, значок приобретет серый цвет.

Показывать «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows.

По умолчанию такой индикатор появляется в правом верхнем углу экрана в момент запуска Антивируса Касперского. Он информирует вас о том, что защита вашего компьютера от любого рода угроз включена.

Если программа установлена на компьютере под управлением операционной системы семейства Microsoft Windows Vista, данная возможность недоступна.

Чтобы настроить активные элементы интерфейса, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Параметры**.
3. В блоке **Вид** установите нужные флажки.

ОТЧЕТЫ И ХРАНИЛИЩА

В разделе собраны параметры, регулирующие работу с файлами данных программы.

Файлы данных программы – это объекты, помещенные в процессе работы Антивируса Касперского на карантин, в резервное хранилище, а также файлы отчета о работе компонентов программы.

В данном разделе вы можете:

- настроить параметры формирования и хранения отчетов (см. стр. 172);
- настроить параметры карантина и резервного хранилища (см. стр. 175);
- очистить содержимое хранилища отчетов, карантина и резервного хранилища.

Чтобы очистить содержимое хранилищ, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В открывшемся окне нажмите на кнопку **Очистить**.
4. В открывшемся окне **Файлы данных** укажите, объекты каких хранилищ требуется удалить.

См. также

Принципы работы с отчетами

Работа каждого компонента Антивируса Касперского и выполнение каждой задачи проверки и обновления фиксируются в отчете.

- *Чтобы перейти к просмотру отчетов, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. Нажмите на кнопку **Отчеты**.

- *Чтобы ознакомиться со всеми событиями, зафиксированными в отчете о работе компонента или о выполнении задачи, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Отчеты**.
  2. В открывшемся окне на закладке **Отчеты** выберите имя компонента или задачи и нажмите на ссылку **Подробно**. В результате будет открыто окно, содержащее детальную информацию о работе выбранного компонента или задачи. Результирующая статистика работы приведена в верхней части окна, а подробная информация размещена на разных закладках в центральной части. В зависимости от компонента или задачи состав закладок может быть разный.

- *Чтобы импортировать отчет в текстовый файл, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Отчеты**.
  2. В открывшемся окне на закладке **Отчеты** выберите имя компонента или задачи и нажмите на ссылку **Подробно**.
  3. В открывшемся окне будет представлена информация о работе выбранного компонента или задачи. Нажмите на кнопку **Сохранить как** и укажите, куда бы вы хотели сохранить файл отчета.

Настройка параметров отчетов

Вы можете настроить следующие параметры формирования и хранения отчетов:

- Разрешить или запретить запись в отчет событий информационного характера. Как правило, такие события не принципиально важны для обеспечения защиты (флажок **Записывать некритические события**).

- Включить хранение в отчете только событий, произошедших при последнем запуске задачи. Это позволит сэкономить место на диске за счет уменьшения размера отчета (флажок **Хранить только текущие события**). Если флажок установлен, информация, представленная в отчете, будет обновляться при каждом перезапуске задачи. Однако перезаписи подлежит только информация некритического характера.

- Установить срок хранения отчетов (флажок **Хранить отчеты не более**). По умолчанию срок хранения отчетов составляет 14 дней, после чего отчеты удаляются. Вы можете изменить максимальный срок хранения или совсем отменить это ограничение.

- Указать максимальный размер отчета (флажок **Максимальный размер**). По умолчанию максимальный размер составляет 100 МБ. Вы можете отменить ограничение размера отчета или установить другое значение.

Чтобы настроить параметры формирования и хранения отчетов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В блоке **Отчеты** установите необходимые флажки и, если потребуется, установите срок хранения отчетов и укажите максимальный размер отчета.

КАРАНТИН ВОЗМОЖНО ЗАРАЖЕННЫХ ОБЪЕКТОВ

Карантин – это специальное хранилище, в которое помещаются объекты, возможно зараженные вирусами.

Возможно зараженные объекты – это объекты, подозреваемые на заражение вирусами или их модификациями.

Почему объекты называются *возможно зараженными*? Не всегда можно однозначно определить, заражен объект или нет. Причины могут быть следующие:

- *Код анализируемого объекта похож на известную угрозу, но частично изменен*.

  Базы программы содержат те угрозы, которые на настоящее время изучены специалистами «Лаборатории Касперского». Если вредоносная программа изменяется, и в базы эти изменения еще не внесены, то Антивирус Касперского отнесет объект, пораженный измененной вредоносной программой, к возможно зараженным объектам и обязательно укажет, на какую угрозу похоже это заражение.

- *Код обнаруженного объекта напоминает по структуре вредоносную программу, однако в базах программы ничего подобного не зафиксировано*.

  Вполне возможно, что это новый вид угроз, поэтому Антивирус Касперского относит такой объект к возможно зараженным объектам.

Подозрение файла на присутствие в нем вируса определяется *эвристическим анализатором кода*. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Возможно зараженный объект может быть обнаружен и помещен на карантин в процессе проверки на вирусы, а также Файловым Антивирусом, Почтовым Антивирусом и Проактивной защитой.

При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

См. также

Действия с объектами на карантине

С объектами, помещенными на карантин, вы можете производить следующие действия:

- помещать на карантин файлы, подозреваемые вами на присутствие вируса;
- проверять и лечить с использованием текущей версии баз программы все возможно зараженные объекты карантина;
- восстанавливать файлы в каталог, заданный пользователем, или каталоги, откуда они были перенесены на карантин (по умолчанию);
- удалять любой объект карантина или группу выбранных объектов.

Чтобы произвести какие-либо действия над объектами карантина, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Карантин** выполните необходимые действия.

Резервные копии опасных объектов

Иногда при лечении объектов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, можно попытаться восстановить исходный объект из его резервной копии.

Резервная копия – копия оригинального опасного объекта, которая создается при первом лечении или удалении данного объекта и хранится в резервном хранилище.

Резервное хранилище – это специальное хранилище, содержащее резервные копии опасных объектов, подвергнутых обработке или удалению. Основная функция резервного хранилища – обеспечить возможность в любой момент восстановить исходный объект. Файлы в резервном хранилище хранятся в специальном формате и не представляют опасности.

См. также

Действия с резервными копиями

С объектами, находящимися в резервном хранилище, вы можете производить следующие действия:

- восстанавливать выбранные копии;
- удалять объекты.

Чтобы произвести какие-либо действия над объектами резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Обнаружено**.
2. В открывшемся окне на закладке **Резервное хранилище** выполните необходимые действия.

НАСТРОЙКА ПАРАМЕТРОВ КАРАНТИНА И РЕЗЕРВНОГО ХРАНИЛИЩА

Вы можете настроить следующие параметры работы карантина и резервного хранилища:

- Задать режим автоматической проверки объектов на карантине после каждого обновления баз программы (флажок **Проверять файлы на карантине после обновления**).

  Антивирус Касперского не сможет проверить объекты карантина сразу после обновления баз программы, если в этот момент вы будете работать с карантином.

- Определить максимальный срок хранения объектов на карантине и копий объектов в резервном хранилище (флажок **Хранить объекты не более**). По умолчанию срок хранения объектов составляет 30 дней, после чего объекты удаляются. Вы можете изменить максимальный срок хранения или совсем отменить это ограничение.

- Указать максимальный размер хранилища данных (флажок **Максимальный размер**). По умолчанию максимальный размер составляет 250 МБ. Вы можете отменить ограничение размера отчета или установить для него другое значение.

Чтобы настроить параметры карантина и резервного хранилища, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Отчеты и хранилища**.
3. В блоке **Карантин и Резервное хранилище** установите необходимые флажки и, если потребуется, установите максимальный размер хранилища данных.

СЕТЬ

В разделе собраны параметры, позволяющие:

- сформировать список контролируемых портов (см. стр. 175);
- включить / отключить режим проверки защищенных соединений (по протоколу SSL) (см. стр. 176).

ФОРМИРОВАНИЕ СПИСКА КОНТРОЛИРУЕМЫХ ПОРТОВ

В работе таких компонентов защиты, как Почтовый Антивирус, Веб-Антивирус, Анти-Хакер и Анти-Спам, 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, а Веб-Антивирус – HTTP-пакеты.

Вы можете выбрать один из двух режимов контроля портов:

- **Контролировать все порты.**

- **Контролировать только выбранные порты**. Список портов, которые обычно используются для передачи почты и HTTP-трафика, включен в комплект поставки программы.

Вы можете добавить новый порт или отключить контроль некоторого порта, тем самым отказавшись от анализа трафика, проходящего через данный порт, на присутствие опасных объектов.

Например, на вашем компьютере есть нестандартный порт, через который настроен обмен данными с удаленным компьютером по HTTP-протоколу. Контроль HTTP-трафика осуществляется компонентом Веб-Антивирус. Чтобы анализировать данный трафик на присутствие вредоносного кода, вам следует добавить этот порт в список контролируемых.

При запуске любого из компонентов Антивирус Касперского открывает на прослушивание всех входящих соединений порт 1110. В случае, если данный порт в этот момент занят какой-либо программой, для прослушивания выбирается порт 1111, 1112 и т. д.

Если вы одновременно пользуетесь Антивирусом Касперского и сетевым экраном (firewall) другой компании-производителя, в параметрах этого сетевого экрана требуется создать разрешающие правила для процесса *avp.exe* (внутренний процесс Антивируса Касперского) на всех перечисленных портах.

Например, в вашем сетевом экране создано правило для процесса *iexplorer.exe*, согласно которому данному процессу разрешено устанавливать соединения на порту 80. Однако Антивирус Касперского, перехватывая запрос на соединение, инициируемое процессом *iexplorer.exe* на порту 80, передает его процессу *avp.exe*, который, в свою очередь, пытается самостоятельно установить соединение с запрашиваемой веб-страницей. Если для процесса *avp.exe* отсутствует разрешающее правило, сетевой экран заблокирует этот запрос. В результате веб-страница будет недоступна пользователю.

Чтобы добавить порт в список контролируемых портов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Контролируемые порты** нажмите на кнопку **Настройка портов**.
4. В открывшемся окне **Настройка портов** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Порт** укажите необходимые данные.

Чтобы исключить порт из списка контролируемых портов, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Контролируемые порты** нажмите на кнопку **Настройка портов**.
4. В открывшемся окне **Настройка портов** 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 стороны, обменивающиеся данными, на основе электронных сертификатов, а также 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.

Антивирус Касперского 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, которое предложит вам принять / отвергнуть сертификат или просмотреть информацию о нем.

Чтобы включить проверку защищенных соединений, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите раздел **Сеть**.
3. В блоке **Проверка защищенных соединений** установите флажок **Проверять защищенные соединения** и нажмите на кнопку **Установить сертификат**.
4. В открывшемся окне нажмите на кнопку **Установить сертификат**. Будет запущен мастер, следуя указаниям которого вы установите сертификат.

Автоматическая установка сертификата действует только при работе с браузером Microsoft Internet Explorer. Для проверки защищенных соединений в браузерах Mozilla Firefox (см. стр. 177) и Opera (см. стр. 178) установите сертификат «Лаборатории Касперского» вручную.

См. также

ПРОВЕРКА ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В MOZILLA FIREFOX

Браузер Mozilla Firefox не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при использовании Firefox необходимо установить сертификат «Лаборатории Касперского» вручную.

Чтобы установить сертификат «Лаборатории Касперского», выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройки**.
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\AVP60MP4\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 **Просмотреть**.

Чтобы установить сертификат «Лаборатории Касперского» для Mozilla Firefox версии 3.x, выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройки**.
2. В открывшемся окне выберите раздел **Дополнительно**.

3. На закладке **Шифрование** нажмите на кнопку **Просмотр сертификатов**.

4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импортировать**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\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 **Просмотреть**.

Если ваш компьютер работает под управлением операционной системы Microsoft Windows Vista, то путь к файлу сертификата «Лаборатории Касперского» будет таким: *%AllUsersProfile%\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

Проверка защищенных соединений в Opera

Браузер Opera не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при пользовании Opera необходимо установить сертификат «Лаборатории Касперского» вручную.

- *Чтобы установить сертификат «Лаборатории Касперского», выполните следующие действия:*

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.

2. В открывшемся окне выберите раздел **Дополнительно**.

3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.

4. В открывшемся окне выберите закладку **Поставщики** и нажмите на кнопку **Импорт**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен. Для просмотра информации о сертификате и выбора действий, при которых будет использоваться сертификат, выберите сертификат в списке и нажмите на кнопку **Просмотреть**.

- *Чтобы установить сертификат «Лаборатории Касперского» для Opera версии 9.x, выполните следующие действия:*

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.

2. В открывшемся окне выберите раздел **Дополнительно**.

3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.

4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импорт**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен.

ДИСК АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

В Антивирусе Касперского реализован сервис создания диска аварийного восстановления.

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда невозможно вылечить компьютер с помощью антивирусных программ или утилит лечения (например, Kaspersky AVPTool), запускаемых под управлением операционной системы. При этом эффективность лечения повышается за счет того, что находящиеся в системе вредоносные программы не получают управления во время загрузки операционной системы.

Диск аварийного восстановления формируется на базе ядра операционной системы Linux и представляет собой файл .iso, который включает:

- системные и конфигурационные файлы Linux;
- набор утилит для диагностики операционной системы;
- набор вспомогательных утилит (файловый менеджер и др.);
- файлы Kaspersky Rescue Disk;
- файлы, содержащие базы программы.

Загрузка компьютера с поврежденной операционной системой может осуществляться двумя способами:

- *локально*, с CD/DVD-ROM-устройства. Для этого на компьютере должно быть установлено соответствующее устройство.
- *удаленно*, с рабочего места администратора или другого компьютера сети.

Удаленная загрузка возможна только в случае, если загружаемый компьютер поддерживает технологию Intel® vPro™ или Intel® Active Management.

Чтобы создать диск аварийного восстановления, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Диск аварийного восстановления** для запуска мастера создания диска (см. стр. 180).
3. Следуйте указаниям мастера.
4. С помощью полученного в результате работы мастера файла создайте загрузочный CD/DVD-диск. Для этого можно воспользоваться одной из программ записи CD/DVD-дисков, например, Nero.

См. также

Создание диска аварийного восстановления

Создание диска аварийного восстановления заключается в формировании образа диска (файла .iso) с актуальными базами программы и конфигурационными файлами.

Исходный образ диска, на основе которого формируется новый файл, может быть загружен с сервера «Лаборатории Касперского» или скопирован с локального источника.

Сформированный мастером файл образа сохраняется в папке «*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk*» («*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk*» – для Microsoft Vista) с именем *rescuecd.iso*. Если мастер обнаружил ранее созданный файл образа в указанной папке, то установив флажок ☑ **Использовать существующий образ**, вы можете использовать его в качестве исходного образа диска и перейти сразу к шагу 3 – обновление образа (см. стр. 181). Если мастер не обнаружил файл образа, то данный флажок будет отсутствовать.

Диск аварийного восстановления создается с помощью мастера, который состоит из последовательности окон (шагов). Переключение между окнами осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Рассмотрим подробнее шаги мастера

Шаг 1. Выбор источника образа диска

Если в предыдущем окне мастера вы установили ☑ **Использовать существующий образ**, то этот шаг будет пропущен.

На данном этапе вам следует выбрать источник файла образа из предложенных вариантов:

- Выберите вариант ◉ **Копировать образ с CD/DVD-диска или из локальной сети**, если у вас уже есть записанный CD/DVD-диск аварийного восстановления или подготовленный для него образ, сохраненный на вашем компьютере или на ресурсе локальной сети.

- Выберите вариант ◉ **Загрузить образ с сервера «Лаборатории Касперского»**, если у вас нет сформированного файла образа, то вы можете загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 100 МБ).

Шаг 2. Копирование (загрузка) образа диска

Если на предыдущем шаге вы выбрали вариант копирования образа из локального источника (◉ **Копировать образ с CD/DVD-диска или из локальной сети**), то на данном шаге вам следует указать к нему путь. Для этого воспользуйтесь кнопкой **Обзор**. Далее будет отображен процесс копирования файла.

Если же вы выбрали вариант ◉ **Загрузить образ с сервера «Лаборатории Касперского»**, то процесс загрузки файла отображается сразу.

Шаг 3. Обновление файла образа

Процедура обновления файла образа включает:

- обновление баз программы;
- обновление конфигурационных файлов.

Конфигурационные файлы определяют способ применения диска аварийного восстановления: на локальном или удаленном компьютере, поэтому перед обновлением файла образа вам следует выбрать нужный вариант из предложенных:

- **Загрузка удаленного компьютера**, если предполагается загрузка удаленного компьютера.

  Обратите внимание, что в случае загрузки удаленного компьютера, он должен поддерживать технологию Intel® vPro™ или Intel® Active Management.

  Если доступ в интернет с удаленного компьютера осуществляется через прокси-сервер, то обновление при использовании диска аварийного восстановления будет недоступно. В этом случае рекомендуется предварительно выполнить обновление Антивируса Касперского.

- **Загрузка системы с CD/DVD-диска**, если создаваемый образ диска в дальнейшем будет записан на CD/DVD-диск.

Выбрав нужный вариант, нажмите на кнопку **Далее**. В следующем окне мастера будет отображен ход выполнения обновления.

Если выбран вариант **Загрузка удаленного компьютера**, то созданный образ не может быть использован для записи CD/DVD-диска и последующей загрузки компьютера. Для загрузки компьютера с CD/DVD-диска, необходимо запустить мастер заново и на этом шаге выбрать **Загрузка системы с CD/DVD-диска**.

Шаг 4. Загрузка удаленного компьютера

Данный шаг мастера появляется только в случае, если на предыдущем шаге вы выбрали вариант **Загрузка удаленного компьютера**.

Укажите данные о компьютере:

- **IP-адрес или имя компьютера** в сети;
- данные учетной записи с правами администратора: **Имя пользователя** и **Пароль**.

Следующее окно мастера представляет собой консоль iAMT, где вы управляете процессом загрузки компьютера (см. стр. 182).

Шаг 5. Завершение работы мастера

В данном окне мастер проинформирует вас об успешном создании диска аварийного восстановления.

Загрузка компьютера с помощью диска аварийного восстановления

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

Для загрузки операционной системы необходим файл образа (.iso) загрузочного диска. Вы можете загрузить (см. стр. 180) файл с сервера «Лаборатории Касперского» или обновить (см. стр. 181) существующий.

Рассмотрим подробнее работу диска аварийного восстановления. В процессе загрузки диска проводятся следующие операции:

1. Автоматическое определение аппаратного обеспечения компьютера.

2. Поиск файловых систем на жестких дисках. Найденным файловым системам назначаются имена начиная с *C*.

   Имена, назначаемые жестким дискам и съемным устройствам, могут не совпадать с их наименованиями в операционной системе.

   Если операционная система загружаемого компьютера находится в спящем режиме, или файловая система приведена в состояние *unclean* вследствие некорректного завершения работы, вам будет предложено принять решение о монтировании файловой системы или перезагрузке компьютера.

   Монтирование файловой системы может привести к ее повреждению.

3. Поиск файла подкачки Microsoft Windows *pagefile.sys*. В случае его отсутствия размер виртуальной памяти ограничивается размером оперативной памяти.

4. Выбор языка локализации. Если в течение некоторого времени выбор не был сделан, то по умолчанию выбирается английский язык.

   При загрузке удаленного компьютера данный шаг отсутствует.

5. Поиск (создание) папок для размещения антивирусных баз, отчетов, карантина и вспомогательных файлов. По умолчанию используются папки программы «Лаборатории Касперского», установленного на зараженном компьютере (*ProgramData/Kaspersky Lab/AVP8* – для Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – для более ранних версий Microsoft Windows). Если папки программы не найдены, будет произведена попытка создать их. В случае, если папки не были обнаружены и создать их не удалось, на одном из дисков создается папка *kl.files*.

6. Попытка настройки сетевых соединений на основе данных, обнаруженных в системных файлах загружаемого компьютера.

7. Загрузка графической подсистемы и запуск Kaspersky Rescue Disk (в случае загрузки компьютера с CD/DVD-диска).

   В случае загрузки удаленного компьютера в консоли iAMT загружается командная строка. Для управления задачами используются команды для работы с Kaspersky Rescue Disk из командной строки (см. стр. 184).

В режиме аварийного восстановления доступны только задачи проверки на вирусы и обновления баз с локального источника, а также откат обновлений и просмотр статистики.

Чтобы произвести загрузку операционной системы зараженного компьютера с CD/DVD-ROM-диска, выполните следующие действия:

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

2. Поместите в дисковод зараженного компьютера диск с предварительно записанным образом диска аварийного восстановления.

3. Перезагрузите компьютер.

4. Далее загрузка происходит в соответствии с описанным выше алгоритмом.

Чтобы произвести загрузку операционной системы удаленного компьютера, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Диск аварийного восстановления** для запуска мастера создания диска (см. стр. 180). Следуйте указаниям мастера.

   Обратите внимание, что на этапе обновления (см. стр. 181) образа диска вам необходимо выбрать вариант **Загрузка удаленного компьютера**.

Далее загрузка происходит в соответствии с описанным выше алгоритмом.

Работа с Kaspersky Rescue Disk из командной строки

Работать с Kaspersky Rescue Disk можно посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- проверка выбранных объектов;
- обновление баз и программных модулей;
- откат последнего обновления
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

```
<команда> [параметры]
```

В качестве команд используются:

HELP	помощь по синтаксису команды, вывод списка команд
SCAN	проверка объектов на присутствие вирусов
UPDATE	запуск задачи обновления
ROLLBACK	откат последнего произведенного обновления
EXIT	завершение работы с Kaspersky Rescue Disk

В этом разделе

Проверка на вирусы

Командная строка запуска проверки некоторой области на присутствие вирусов и обработки вредоносных объектов имеет следующий общий вид:

```
SCAN [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>] [<параметры отчета>]
```

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.
/discs/	Проверка всех дисков.
/discs/<disc_name>:/<folder>	Проверка указанного диска, где <disc_name> – наименование диска, а <folder> – путь к проверяемому каталогу.
<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 базы.
-e:m	Не проверять почтовые сообщения в формате plain text.
-e:<filemask>	Не проверять объекты по маске.
-e:<seconds>	Пропускать объекты, которые проверяются дольше указанного параметром **<seconds>** времени.
-es:<size>	Пропускать объекты, размер которых (в мегабайтах) превышает значение, заданное параметром **<size>**.

Примеры:

- *Запустить проверку каталога Documents and Settings и диска <D>:*

```
SCAN /discs/D: «/discs/C:/Documents and Settings»
```

Обновление Антивируса Касперского

Команда для обновления баз и программных модулей Антивируса Касперского имеет следующий синтаксис:

```
UPDATE [<источник_обновлений>] [-R[A]:<файл_отчета>]
```

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 Антивируса Касперского.
-R[A]:<файл_отчета>	**-R:<файл_отчета> –** фиксировать в отчете только важные события. **-RA:<файл_отчета> –** записывать в отчет все события. Допускается использование абсолютного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

Примеры:

- *Обновить базы, зафиксировав все события в отчете:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

Откат последнего обновления

Синтаксис команды:

```
ROLLBACK [-R[A]:<файл_отчета>]
```

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 пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

Пример:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

Просмотр справки

Для просмотра справки по синтаксису командной строки предусмотрена команда:

```
[ -? | HELP ]
```

Для получения справки по синтаксису конкретной команды можно воспользоваться одной из следующих команд:

```
<команда> -?
HELP <команда>
```

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ АНТИВИРУСА КАСПЕРСКОГО

После установки и настройки Антивируса Касперского 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 нанести вред вашему компьютеру, однако 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 программой как зараженный объект, перемещаемый по HTTP-протоколу. Не забудьте включить антивирусную защиту сразу после загрузки тестового «вируса».

Программа идентифицирует файл, загруженный с сайта компании **EICAR** как зараженный объект, содержащий **не подлежащий лечению** вирус, и выполняет действие, установленное для такого объекта.

Вы также можете использовать модификации стандартного тестового «вируса» для проверки работы программы. 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 антивирусной программы 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 программой объектов с указанным статусом. Обращаем ваше внимание, что действия над объектами определяются значениями параметров программы.

После добавления префикса к тестовому «вирусу» сохраните полученный файл, например, под именем: *eicar_dele.com*. Дайте аналогичные названия всем модифицированным «вирусам».

Таблица 1. Модификации тестового «вируса»

Префикс	Статус объекта	Информация об обработке объекта
Префикс отсутствует, стандартный тестовый «вирус».	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Программа идентифицирует данный объект как вирус, не подлежащий лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR-	**Поврежденный**.	Программа получила доступ к объекту, но не смогла 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 программы.
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.	Программа обнаружила 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. Программа не смогла 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 программы.
CURE-	**Зараженный**. Объект содержит код известного вируса. Излечим.	Объект содержит вирус, который может быть вылечен. Программа 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.	Программа идентифицирует данный объект как вирус, не подлежащий 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:*

  попытайтесь загрузить тестовый «вирус» с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

При попытке загрузить тестовый «вирус» Антивирус Касперского 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 выполните следующие действия:

1. Создайте письмо в формате **Обычный текст** с помощью установленного на компьютере почтового клиента.

   Письмо, содержащее в теле 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.

Программа обнаружит объект, идентифицирует его как зараженный и 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, 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 проверки на вирусы

Чтобы проверить, насколько корректно настроена задача проверки на вирусы, 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 проверки на вирусы 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 проверки на вирусы 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 проверки на вирусы 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 программой как спам.

Тестовое сообщение должно содержать в теме письма строку:

```
Spam is bad do not send it
```

После поступления данного сообщения на компьютер Антивирус Касперского проверит его, присвоит сообщению статус спама и выполнит над ним действие, установленное для объекта данного типа.

ВИДЫ УВЕДОМЛЕНИЙ

При возникновении событий в процессе работы Антивируса Касперского 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. 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 обучения Анти-Хакера. Информационные уведомления имеют голубой цвет.

В ЭТОМ РАЗДЕЛЕ

Обнаружен вредоносный объект

При обнаружении Файловым Антивирусом, Почтовым Антивирусом или задачей проверки на вирусы вредоносного объекта на экране открывается специальное уведомление.

Оно содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Лечить** – пытаться лечить вредоносный объект. Перед лечением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок ☑ **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Лечение объекта невозможно

В некоторых случаях лечение вредоносного объекта невозможно. Например, если файл поврежден настолько, что удалить из него вредоносный код и восстановить целостность не удается. Кроме того, процедура лечения не применима к некоторым видам вредоносных объектов, например, троянским программам.

В данных случаях на экран выводится специальное уведомление, которое содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок ☑ **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения

либо перезапуска программы, а также время выполнения задачи проверки на вирусы от момента запуска до завершения.

Требуется специальная процедура лечения

При обнаружении угрозы, которая в данный момент активна в системе (например, вредоносного процесса в оперативной памяти или объектах автозапуска), на экран выводится запрос о проведении специальной расширенной процедуры лечения.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют согласиться с проведением расширенной процедуры лечения. Для этого нажмите на кнопку **ОК**. Однако обратите внимание, что по ее окончании будет произведена перезагрузка компьютера, поэтому перед выполнением процедуры рекомендуется сохранить результаты текущей работы и закрыть все программы.

В процессе выполнения процедуры лечения не разрешается запускать почтовые клиенты и редактировать реестр операционной системы. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы.

Обнаружен подозрительный объект

При обнаружении Файловым Антивирусом, Почтовым Антивирусом или задачей проверки на вирусы объекта, содержащего код неизвестного вируса либо модифицированный код известного вируса, на экране открывается специальное уведомление.

Оно содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Карантин** – поместить объект на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

  При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз – либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  > Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась (не менее чем через три дня) после помещения файла на карантин.

- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта на тот случай, если впоследствии возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок ☑ **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения

либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженный объект не является вредоносным, рекомендуется, во избежание повторных срабатываний программы при работе с этим объектом, добавить его в доверенную зону.

Обнаружен опасный объект на трафике

При обнаружении Веб-Антивирусом опасного объекта на трафике на экране открывается специальное уведомление.

Уведомление содержит:

- Вид угрозы (например, *модификация вируса*) и имя опасного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.

- Полное имя опасного объекта и путь к веб-ресурсу.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Разрешить** – продолжить загрузку объекта.

- **Запретить** – заблокировать загрузку объекта с веб-ресурса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружена опасная активность в системе

При обнаружении Проактивной защитой опасной активности какой-либо программы в системе на экран выводится специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.

- Полное имя файла процесса, инициирующего опасную активность, и путь к нему.

- Набор возможных действий:

  - **Карантин** – завершить процесс и поместить исполняемый файл процесса на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование. Файлы на карантине хранятся в специальном формате и не представляют опасности.

    При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз, либо получить статус *не заражен*, и тогда его можно будет восстановить.

    Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась (не менее чем через три дня) после помещения файла на карантин.

  - **Завершить** – завершить процесс.

- **Разрешить** – разрешить выполнение процесса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженная программа не является опасной, во избежание повторных срабатываний Антивируса Касперского при ее обнаружении, рекомендуется добавить программу в доверенную зону.

Обнаружен процесс внедрения (Invader)

При обнаружении Проактивной защитой попытки внедрения одного процесса в другой на экран выводится специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.
- Полное имя файла процесса, инициирующего попытку внедрения, и путь к нему.
- Набор возможных действий:
  - **Завершить** – полностью завершить процесс, инициирующий попытку внедрения.
  - **Запретить** – запретить внедрение.
  - **Пропустить** – не выполнять никаких действий, лишь зафиксировать информацию в отчете.

Для того чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что подобное действие не является опасным, рекомендуется, во избежание повторных срабатываний Антивируса Касперского при попытке данного процесса внедрится в другой процесс, добавить исключение в доверенную зону.

Например, вы используете программы автоматического переключения раскладки клавиатуры. Антивирус Касперского идентифицирует действия таких программ как опасные, поскольку попытки внедрения в другие процессы, используемые данными программами, характерны для некоторых вредоносных программ (например, перехватчиков ввода паролей и т.д.).

Обнаружен скрытый процесс

При обнаружении Проактивной защитой скрытого процесса в системе на экран выводится специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.
- Полное имя файла скрытого процесса и путь к нему.
- Набор возможных действий:

- **Карантин** – поместить исполняемый файл процесса на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование. Файлы на карантине хранятся в специальном формате и не представляют опасности.

  При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз, либо получить статус *не заражен*, и тогда его можно будет восстановить.

  Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась через некоторое время (не менее трех дней) после помещения файла на карантин.

- **Завершить** – завершить процесс.

- **Разрешить** – разрешить выполнение процесса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженная программа не является опасной, рекомендуется, во избежание повторных срабатываний Антивируса Касперского при ее обнаружении, добавить программу в доверенную зону.

Обнаружена попытка доступа к системному реестру

При обнаружении Проактивной защитой попытки доступа к ключам системного реестра на экран выводится специальное уведомление, в котором содержится:

- Ключ реестра, к которому осуществляется попытка доступа.
- Полное имя файла процесса, инициирующего попытку доступа к ключам реестра, и путь к нему.
- Набор возможных действий:
  - **Разрешить** – однократно разрешить выполнение опасного действия;
  - **Запретить** – однократно запретить выполнение опасного действия.

Чтобы выбранное вами действие выполнялось автоматически каждый раз, когда такая активность будет инициироваться на вашем компьютере, установите флажок **Создать правило**.

Если вы считаете, что любая активность программы, которая инициировала обращение к ключам системного реестра, не является опасной, добавьте эту программу в список доверенных.

Обнаружена попытка переадресации вызова системной функции

При обнаружении Проактивной защитой попытки встраивания некоего кода в ядро операционной системы Microsoft Windows с целью изменения адреса вызова системных функций на экран выводится специальное уведомление.

Цель уведомления – проинформировать пользователя, поскольку такое поведение может быть вызвано наличием в системе скрытых вредоносных программ либо еще не известного вируса.

В данной ситуации рекомендуется обновить базы программы и запустить полную проверку компьютера.

Обнаружена сетевая активность программы

Если включен режим обучения Анти-Хакера, каждый раз при попытке какой-либо программы выполнить сетевое соединение, для которой не сформировано правило, на экран будет выведено специальное уведомление.

Уведомление содержит:

- *Описание активности* – название программы и краткая характеристика соединения, которое оно инициирует. Как правило, указывается тип соединения, локальный порт, с которого оно инициируется, удаленный порт и адрес, с которым выполняется соединение. Для получения подробной информации о соединении, о процессе, который его инициирует, и о компании-производителе программы нажмите на ссылку **Подробно**.

- *Действие* – последовательность операций, которую следует выполнить компоненту Анти-Хакер в отношении обнаруженной сетевой активности.

Внимательно изучите информацию о сетевой активности и только после этого выберите действие Анти-Хакера. Рекомендуем вам воспользоваться следующими советами при принятии решения:

1. Прежде всего определите, разрешить или запретить сетевую активность. Возможно, в данном случае вам поможет набор правил, уже сформированных для данной программы или пакета (при условии, что они созданы).

2. Затем определите, следует ли разово выполнить действие или нужно автоматически выполнять его каждый раз при обнаружении такой активности.

Чтобы выполнить действие один раз

снимите флажок **Создать правило** и выберите необходимое действие – **Разрешить** или **Запретить**.

Чтобы выбранное вами действие выполнялось автоматически каждый раз, когда такая активность будет инициироваться на вашем компьютере, выполните следующие действия:

1. Убедитесь, что флажок **Создать правило** установлен.

2. Выберите тип активности, к которой вы хотите применить действие, из раскрывающегося списка:

   - **Любая активность** – сетевая активность любого характера, инициируемая данной программой.

   - **Выборочно** – отдельная активность, которую вам нужно определить в окне создания правила.

   - **<Шаблон>** – имя шаблона, включающего набор правил, характерных для сетевой активности программы. Такой тип активности появляется в списке в том случае, если для программы, инициировавшего сетевую активность, существует подходящий шаблон, включенный в поставку Антивируса Касперского. В этом случае вам не нужно выборочно определять, какую активность разрешить или запретить в данный момент. Воспользуйтесь шаблоном, и набор правил для программы будет создан автоматически.

3. Выберите необходимое действие – **Разрешить** или **Запретить**.

Помните, что созданное правило будет использоваться только в случае, когда все параметры соединения ему удовлетворяют. Для соединения, выполняемого, например, с другого локального порта, такое правило будет недействительно.

Чтобы отключить получение уведомлений от Анти-Хакера при попытках любой программы установить сетевое соединение, воспользуйтесь ссылкой **Отключить режим обучения**. После этого Анти-Хакер будет переведен в режим **Минимальной защиты**, в рамках которого разрешены любые сетевые соединения, за исключением тех, которые явно запрещены правилами.

Обнаружена сетевая активность измененного исполняемого файла

При обнаружении Анти-Хакером сетевой активности, которую инициирует измененный исполняемый файл запущенной пользователем программы, на экран выводится специальное уведомление. Измененным считается файл, который был либо обновлен либо заражен вредоносной программой.

Уведомление содержит:

- *Информацию о программе, инициировавшей сетевую активность* – имя и ID запущенного процесса, а также производитель программы и номер версии.

- *Действие* – последовательность операций, которую следует выполнить Антивирусу Касперского в отношении обнаруженной сетевой активности.

Вам предлагается выбрать одно из следующих действий:

- **Разрешить** – информация об измененном исполняемом файле будет обновлена в существующем правиле для программы. В дальнейшем ее сетевая активность будет разрешаться автоматически.

- **Запретить** – сетевая активность будет запрещена однократно.

Обнаружена новая сеть

При каждом подключении компьютера к новой зоне (сети) на экран будет выведено специальное уведомление.

В верхней части уведомления приведено краткое описание сети с указанием IP-адреса и маски подсети.

В нижней части окна вам предлагается присвоить обнаруженной зоне статус, на основании которого будет разрешена та или иная сетевая активность:

- **Интернет в режиме невидимости (запретить доступ к компьютеру извне)**. При присвоении этого статуса будет разрешена только сетевая активность, инициатором которой выступил пользователь или программа, которым разрешена такая активность. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на работу в интернете данный режим не оказывает никакого влияния.

- **Интернет (запретить доступ к файлам и принтерам)**. Сеть с высокой степенью риска, при работе в которой компьютер подвержен любым возможным типам угроз. Данный статус также рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами и т. д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне.

- **Локальная сеть (разрешить доступ к файлам и принтерам)**. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети).

- **Доверенная сеть (разрешить любую сетевую активность)**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным.

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, HTTP-сервера). В противном случае компьютеры, обращающиеся к данному серверу, не

будут видеть его в сети.

Обнаружена попытка фишинг-атаки

При обнаружении Антивирусом Касперского попытки открытия фишинг-сайта на экран будет выведено специальное уведомление.

В уведомлении содержится:

- Название угрозы – *фишинг-атака*, выполненная в виде ссылки на Вирусную энциклопедию «Лаборатории Касперского» с подробным описанием угрозы.
- Веб-адрес фишинг-сайта в интернете.
- Набор возможных действий:
  - **Разрешить** – продолжить загрузку фишинг-сайта.
  - **Запретить** – заблокировать загрузку фишинг-сайта.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружена попытка дозвона

При обнаружении Анти-Шпионом попытки дозвона через модем на некоторый телефонный номер на экран будет выведено специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, какого рода угроза обнаружена.
- Полное имя файла процесса, инициирующего попытку дозвона, и путь к нему.
- Информация о телефонном номере, на который осуществляется попытка дозвона.
- Набор возможных действий:
  - **Разрешить** – разрешить дозвон на указанный номер с последующим установлением сетевого соединения;
  - **Запретить** – заблокировать попытку дозвона на указанный номер;
  - **Добавить к доверенным номерам** – добавить номер в список доверенных номеров. Используйте данную возможность, если попытка дозвона на указанный номер была санкционирована вами, во избежание повторных срабатываний программы при наборе данного номера.

Обнаружен некорректный сертификат

Проверка безопасности соединения по протоколу SSL производится с помощью установленного сертификата. При попытке соединения с сервером с использованием некорректного сертификата (например, в случае его подмены злоумышленниками), на экран будет выведено специальное уведомление.

В уведомлении будет приведена информация о возможных причинах ошибки, а также удаленные порт и адрес. Вам будет предложено принять решение о необходимости соединения в условиях использования некорректного сертификата:

- **Принять сертификат** – продолжить соединение с веб-ресурсом;
- **Отклонить сертификат** – разорвать соединение с веб-ресурсом;
- **Просмотреть сертификат** – воспользоваться возможностью просмотреть информацию о сертификате.

РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Антивирусом Касперского посредством командной строки.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Обращение к программе через командную строку должно осуществляться из каталога установки Антивируса Касперского либо с указанием полного пути к avp.com.

В качестве <команды> может использоваться:

- **HELP –** помощь по синтаксису команды, вывод списка команд.
- **SCAN –** проверка объектов на присутствие вредоносных программ.
- **UPDATE –** запуск обновления программы.
- **ROLLBACK –** откат последнего произведенного обновления Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **START –** запуск компонента или задачи.
- **STOP –** остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс Антивируса Касперского).
- **STATUS –** вывод на экран текущего статуса компонента или задачи.
- **STATISTICS –** вывод на экран статистики по работе компонента или задачи.
- **EXPORT –** экспорт параметров защиты программы.
- **IMPORT –** импорт параметров защиты Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **ACTIVATE –** активация Антивируса Касперского через интернет с помощью кода активации.
- **ADDKEY –** активация программы с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **RESTORE –** восстановление файла из карантина.
- **EXIT –** завершение работы с программой (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы).
- **TRACE –** получение файла трассировки.

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента программы.

В этом разделе

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>
```

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>]
[<параметры отчета>] [<дополнительные параметры>]
```

Для проверки объектов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки. При этом задача будет выполнена с параметрами, установленными в интерфейсе Антивируса Касперского.

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 папкам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элемента списка – пробел. Замечания:
  - если имя объекта содержит пробел, оно должно быть заключено в кавычки;
  - если указана конкретная папка, проверяются все файлы, содержащиеся в ней.
- **/ALL** – полная проверка компьютера.
- **/MEMORY** – объекты оперативной памяти.
- **/STARTUP** – объекты автозапуска.
- **/MAIL** – почтовые базы.
- **/REMDRIVES** – все съемные диски.
- **/FIXDRIVES** – все локальные диски.
- **/NETDRIVES** – все сетевые диски.
- **/QUARANTINE** – объекты на карантине.
- **/@:<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 в кавычках, если в нем содержится пробел.

<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i2**. Возможны следующие значения:

- **/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). Данное действие используется по умолчанию.
- **/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. Возможны следующие значения:

- **/fe** – проверять только заражаемые файлы по расширению.
- **/fi** – проверять только заражаемые файлы по содержимому.

- **/fa** – проверять все файлы.

<исключения> – параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.

- **/e:a** – не проверять архивы.
- **/e:b** – не проверять почтовые базы.
- **/e:m** – не проверять почтовые сообщения в формате plain text.
- **/e:<mask>** – не проверять объекты по маске.
- **/e:<seconds>** – пропускать объекты, которые проверяются дольше указанного параметром **<seconds>** времени.

<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:<report_file>** – записывать в указанный файл отчета только важные события.
- **/RA:<report_file>** – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметр, определяющий использование технологий антивирусной проверки и файла настроек параметров:

- **/iChecker=<on|off> –** включить / отключить использование технологии iChecker.
- **/iSwift=<on|off> –** включить / отключить использование технологии iSwift.
- **/C:<имя_конфигурационного_файла> –** определяет путь к конфигурационному файлу, содержащему параметры работы программы при проверке. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Примеры:

- *Запустить проверку оперативной памяти, объектов автозапуска, почтовых баз, а также каталогов My Documents, Program Files и файла test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL «C:\Documents and Settings\All Users\My Documents» «C:\Program Files» «C:\Downloads\test.exe»
```

- *Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_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 ПРОГРАММЫ

Команда для обновления модулей Антивируса Касперского и баз программы имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>] [/APP=<on|off>] [<параметры_отчета>] [<дополнительные_параметры>]
```

Описание параметров:

<источник_обновлений> – HTTP-, FTP-сервер или сетевой каталог для загрузки обновлений. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.

/APP=<on|off> – включить / отключить обновление модулей программы.

<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. Возможны следующие значения:

- **/R:<report_file>** – записывать в указанный файл отчета только важные события.
- **/RA:<report_file>** – записывать в указанный файл отчета все события.

<дополнительные параметры> – параметр, определяющий использование файла настроек параметров.

/C:<имя_конфигурационного_файла> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при проверке. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Примеры:

- *Обновить базы программы, зафиксировав все события в отчете:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Обновить модули Антивируса Касперского, используя параметры конфигурационного файла updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Откат последнего обновления

Синтаксис команды:

```
avp.com ROLLBACK </password=<пароль>> [<параметры_отчета>]
```

Описание параметров:

</password=<пароль>> – пароль, заданный через интерфейс программы. Без ввода пароля команда ROLLBACK выполняться не будет.

<параметры отчета> – параметр, определяющий формат отчета о результатах проверки. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

- **/R:<report_file>** – записывать в указанный файл отчета только важные события.
- **/RA:<report_file>** – записывать в указанный файл отчета все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

Пример:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

Запуск / остановка работы компонента или задачи

Синтаксис команды START:

```
avp.com START <профайл|имя_задачи> [параметры_отчета>]
```

Синтаксис команды STOP:

```
avp.com STOP <профайл|имя_задачи> </password=<пароль>>
```

Описание параметров:

</password=<пароль>> – пароль, заданный через интерфейс программы. Без ввода пароля команда STOP выполняться не будет.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного и относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события. Возможны следующие значения:

- **/R:<report_file>** – записывать в указанный файл отчета только важные события.
- **/RA:<report_file>** – записывать в указанный файл отчета все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

<профайл|имя_задачи> – указывается одно из следующих значений:

- **Protection (RTP)** – все компоненты защиты;
- **Anti-Hacker (AH)** – Анти-Хакер;
- **fw** – Сетевой экран;
- **ids** – Система обнаружения вторжений;
- **Anti-Spam (AS)** – Анти-Спам;
- **Anti-Spy (ASPY)** – Анти-Шпион;
- **AdBlocker** – Анти-Баннер;
- **antidial** – Анти-Дозвон;
- **Behavior_Blocking2** – Проактивная защита;
- **pdm2** – Анализ активности;
- **regguard2** – Мониторинг системного реестра;
- **File_Monitoring (FM)** – Файловый Антивирус;
- **Web_Monitoring** – Веб-Антивирус;
- **Mail_Monitoring (EM)** – Почтовый Антивирус;
- **Lock_Control (LC)** – Контроль доступа;
- **Device_Locker** – Контроль устройств;
- **Scan_My_Computer** – задача полной проверки компьютера;
- **Scan_Objects** – проверка объектов;
- **Scan_Quarantine** – проверка карантина;
- **Scan_Startup (STARTUP)** – проверка объектов автозапуска;
- **Updater** – задача обновления;

- **Rollback** – задача отката обновлений.

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе программы.

Примеры:

- *Чтобы включить Файловый Антивирус, в командной строке введите:*

```
avp.com START FM
```

- *Чтобы остановить задачу полной проверки, в командной строке введите:*

```
avp.com STOP SCAN_MY_COMPUTER /password=<ваш_пароль>
```

Статистика работы компонента или задачи

Синтаксис команды STATUS:

```
avp.com STATUS <профайл|имя_задачи>
```

Синтаксис команды STATISTICS:

```
avp.com STATISTICS <профайл|имя_задачи>
```

Описание параметров:

<профайл|имя_задачи> – указывается одно из значений, перечисленных в команде START / STOP (см. стр. 206).

Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл|имя_задачи> <имя_файла>
```

Описание параметров:

<профайл|имя_задачи> – указывается одно из значений, перечисленных в команде START / STOP (см. стр. 206).

<имя_файла> – путь к файлу, в который экспортируются параметры программы. Может быть указан абсолютный или относительный путь.

Пример:

```
avp.com EXPORT RTP RTP_settings.dat – бинарный формат
avp.com EXPORT FM FM_settings.txt – текстовый формат
```

Импорт параметров защиты

Синтаксис команды:

```
avp.com IMPORT <имя_файла> </password=<ваш_пароль>>
```

Описание параметров:

<имя_файла> – путь к файлу, из которого импортируются параметры программы. Может быть указан абсолютный или относительный путь.

</password=<ваш_пароль>> – пароль, заданный через интерфейс программы.

Пример:

```
avp.com IMPORT settings.dat
```

АКТИВАЦИЯ ПРОГРАММЫ

Активацию Антивируса Касперского возможно произвести двумя способами:

- через интернет с помощью кода активации (команда ACTIVATE);
- с помощью файла ключа (команда ADDKEY).

Синтаксис команды:

```
avp.com ACTIVATE <код_активации> </password=<пароль>>
avp.com ADDKEY <имя_файла> </password=<пароль>>
```

Описание параметров:

<код активации> – код активации: xxxxx-xxxxx-xxxxx-xxxxx.

<имя_файла> – файла ключа к программе с расширением .key: xxxxxxxx.key.

</password=<пароль>> – пароль, заданный через интерфейс программы.

Пример:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<пароль>>
```

ВОССТАНОВЛЕНИЕ ФАЙЛА ИЗ КАРАНТИНА

Синтаксис команды:

```
avp.com RESTORE [/REPLACE] <имя_файла>
```

Описание параметров:

/REPLACE – замена существующего файла.

<имя_файла> – имя файла для восстановления.

Пример:

```
avp.com REPLACE C:\eicar.com
```

ЗАВЕРШЕНИЕ РАБОТЫ ПРОГРАММЫ

Синтаксис команды:

```
avp.com EXIT </password=<пароль>>
```

Описание параметров:

</password=<пароль>> – пароль, заданный через интерфейс программы. Без ввода пароля команда выполняться не будет.

Получение файла трассировки

Создание файла трассировки может потребоваться при наличии проблем в работе Антивируса Касперского 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 параметра допустимо указывать числовое значение в диапазоне от 100 (минимальный уровень, только критические сообщения) до 600 (максимальный уровень, все сообщения).

При обращении в Службу технической поддержки следует указывать необходимый уровень трассировки. Если уровень не был указан, то рекомендуется устанавливать значение 500.

Примеры:

- *Отключить создание файлов трассировки:*

  ```
  avp.com TRACE file off
  ```

- *Создать файл трассировки с уровнем 500:*

  ```
  avp.com TRACE file on 500
  ```

Коды 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 проверки на вирусы:

- 101 – все опасные объекты обработаны;
- 102 – обнаружены опасные объекты.

ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ ИЛИ УДАЛЕНИЕ ПРОГРАММЫ

Удалить программу вы можете следующими способами:

- с помощью мастера установки программы (см. раздел «Изменение, восстановление и удаление программы с помощью мастера установки» на стр. 211);
- из командной строки (см. раздел «Удаление программы из командной строки» на стр. 213);
- через Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
- через доменные групповые политики Microsoft Windows Server 2000/2003 (см. раздел «Удаление программы» на стр. 28).

В ЭТОМ РАЗДЕЛЕ

ИЗМЕНЕНИЕ, ВОССТАНОВЛЕНИЕ И УДАЛЕНИЕ ПРОГРАММЫ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Восстановление программы полезно проводить в том случае, если вы обнаружили в ее работе какие-либо ошибки, возникшие вследствие некорректной настройки или повреждения ее файлов.

Изменение компонентного состава позволяет вам доустановить недостающие компоненты Антивируса Касперского или удалить те из них, которые мешают вам в работе или не требуются.

Чтобы перейти к восстановлению исходного состояния программы, установке компонентов Антивируса Касперского, которые не были установлены изначально, или удалению программы, выполните следующие действия:

1. Вставьте CD-диск с дистрибутивом программы в CD/DVD-ROM-устройство, если установка программы производилась с него. В случае установки Антивируса Касперского из другого источника (папка общего доступа, папка на жестком диске и т. д.) убедитесь, что дистрибутив программы присутствует в данном источнике и у вас есть к нему доступ.

2. Выберите **Пуск → Программы → Kaspersky Anti-Virus 6.0 для Windows Workstations MP4 → Изменение, восстановление или удаление**.

В результате будет запущена программа установки, которая выполнена в виде мастера. Рассмотрим подробнее шаги, необходимые для восстановления, изменения компонентного состава программы и ее удаления.

ШАГ 1. СТАРТОВОЕ ОКНО ПРОГРАММЫ УСТАНОВКИ

Если вы провели все описанные выше действия, необходимые для восстановления или изменения состава программы, на экране будет открыто приветственное окно программы установки Антивируса Касперского. Для продолжения нажмите на кнопку **Далее**.

Шаг 2. Выбор операции

На данном этапе вам нужно определить, какую именно операцию вы хотите выполнить над программой: вам предлагается изменить компонентный состав программы, восстановить исходное состояние установленных компонентов или удалить какие-либо компоненты либо программу полностью. Для выполнения нужной вам операции нажмите на соответствующую кнопку. Дальнейшее действие программы установки зависит от выбранной операции.

Изменение компонентного состава выполняется аналогично выборочной установке программы: можно указать, какие компоненты вы хотите установить, а также выбрать те, которые хотите удалить.

Восстановление программы производится исходя из установленного компонентного состава. Будут обновлены все файлы тех компонентов, которые были установлены, и для каждого из них будет установлен **Рекомендуемый** уровень обеспечиваемой защиты.

При удалении программы вы можете выбрать, какие данные, сформированные и используемые в работе программы, вы хотите сохранить на вашем компьютере. Чтобы удалить все данные Антивируса Касперского, выберите вариант **Удалить программу полностью**. Для сохранения данных нужно выбрать вариант **Сохранить объекты программы** и указать, какие именно объекты не нужно удалять:

- *Информация об активации* – файл ключа, необходимый для работы программы.

Базы программы – полный набор сигнатур опасных программ, вирусов и других угроз, актуальных на дату последнего обновления.

- *База Анти-Спама* – база данных, на основе которой распознается нежелательная электронная корреспонденция. Эта база содержит подробную информацию о том, какая почта является для вас спамом, а какая – полезной почтой.

- *Объекты резервного хранилища* – резервные копии удаленных или вылеченных объектов. Такие объекты рекомендуется сохранить для возможности последующего восстановления.

- *Объекты карантина* – объекты, возможно зараженные вирусами или их модификациями. Такие объекты содержат код, который похож на код известного вируса, но однозначно сделать вывод об их вредоносности нельзя. Рекомендуется их сохранить, поскольку они могут оказаться незараженными или их излечение станет возможным после обновления сигнатур угроз.

- *Параметры работы программы* – значения параметров работы всех компонентов программы.

- *Данные iSwift* – база, содержащая информацию о проверенных объектах файловой системы NTFS. Она позволяет ускорить проверку объектов. Используя данные этой базы, Антивирус Касперского проверяет только те объекты, которые изменились со времени последней проверки.

Если между удалением одной версии Антивируса Касперского и установкой другой прошло достаточно продолжительное время, не рекомендуем вам использовать базу iSwift, сохраненную с предыдущей установки программы. За это время на компьютер может проникнуть опасная программа, вредоносные действия которой не будут выявлены при использовании данной базы, и это может привести к заражению компьютера.

Для запуска выбранной операции нажмите на кнопку **Далее**. Запустится процесс копирования необходимых файлов на ваш компьютер или удаления выбранных компонентов и данных.

Шаг 3. Завершение операции восстановления, изменения или удаления программы

Процесс восстановления, изменения или удаления отображается на экране, после чего вы будете уведомлены о его завершении.

Удаление, как правило, требует последующей перезагрузки компьютера, поскольку это необходимо для учета изменений в системе. Запрос на перезагрузку компьютера будет выведен на экран. Нажмите на кнопку **Да**, чтобы выполнить перезагрузку немедленно. Чтобы перезагрузить компьютер позже вручную, нажмите на кнопку **Нет**.

Удаление программы из командной строки

- *Чтобы удалить Антивирус Касперского 6.0 для Windows Workstations MP4 из командной строки, выполните команду:*

  `msiexec /x <имя_пакета>`

  Будет запущен мастер установки, с помощью которого вы сможете провести процедуру удаления программы.

- *Чтобы удалить программу в неинтерактивном режиме без перезагрузки компьютера (перезагрузку следует произвести вручную после удаления), наберите:*

  `msiexec /x <имя_пакета> /qn`

- *Чтобы удалить программу в неинтерактивном режиме с последующей перезагрузкой компьютера, наберите:*

  `msiexec /x <имя_пакета> ALLOWREBOOT=1 /qn`

Если при установке программы был задан пароль на запрет удаления программы, при удалении продукта необходимо указать данный пароль, иначе процедура удаления не будет осуществлена.

- *Чтобы удалить программу с вводом пароля, подтверждающего право на удаление программы, наберите:*

  `msiexec /x <имя_пакета> KLUNINSTPASSWD=******` – для удаления программы в интерактивном режиме;

  `msiexec /x <имя_пакета> KLUNINSTPASSWD=****** /qn` – для удаления программы в неинтерактивном режиме.

УПРАВЛЕНИЕ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit – это система централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе программ, входящих в состав продуктов Kaspersky Open Space Security. Kaspersky Administration Kit поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP / IP.

Программа адресована администраторам корпоративных компьютерных сетей, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях.

Антивирус Касперского 6.0 для Windows Workstations MP4 – один из продуктов «Лаборатории Касперского», управление которым возможно через собственный интерфейс программы, командную строку (эти способы описаны выше в данной документации) либо посредством программы Kaspersky Administration Kit (если компьютер включен в состав системы удаленного централизованного управления).

Для управления Антивирусом Касперского через Kaspersky Administration Kit выполните следующие действия:

- разверните в сети *Сервер администрирования*;
- установите *Консоль администрирования* на рабочее место администратора (подробнее смотрите Руководство по развертыванию Kaspersky Administration Kit);
- на компьютерах сети установите Антивирус Касперского и *Агент администрирования* (входящий в состав Kaspersky Administration Kit). Подробнее об удаленной установке инсталляционного пакета Антивируса Касперского на компьютеры сети смотрите Руководство по развертыванию «Kaspersky Administration Kit».

Обратите внимание, что если на компьютерах сети развернут Антивирус Касперского предыдущей версии, при обновлении до новой версии через Kaspersky Administration Kit необходимо выполнить следующие действия:

- предварительно остановить предыдущую версию программы (это можно сделать удаленно через Kaspersky Administration Kit);
- перед началом установки закрыть все работающие программы;
- по завершении установки перезагрузить операционную систему на удаленном компьютере.

Перед обновлением версии плагина управления Антивирусом Касперского через Kaspersky Administration Kit необходимо завершить работу Консоли администрирования.

Доступ к управлению программой через Kaspersky Administration Kit обеспечивает Консоль администрирования (см. рис. ниже). Она представляет собой стандартный интерфейс, интегрированный в MMC, и позволяет администратору выполнять следующие функции:

- удаленно устанавливать и удалять Антивирус Касперского и *Агент администрирования* на компьютеры сети;
- удаленно настраивать Антивирус Касперского на компьютерах сети;
- обновлять базы и модули Антивируса Касперского;
- осуществлять управление лицензиями для Антивируса Касперского на компьютерах сети;

- просматривать информацию о работе программы на клиентских компьютерах.

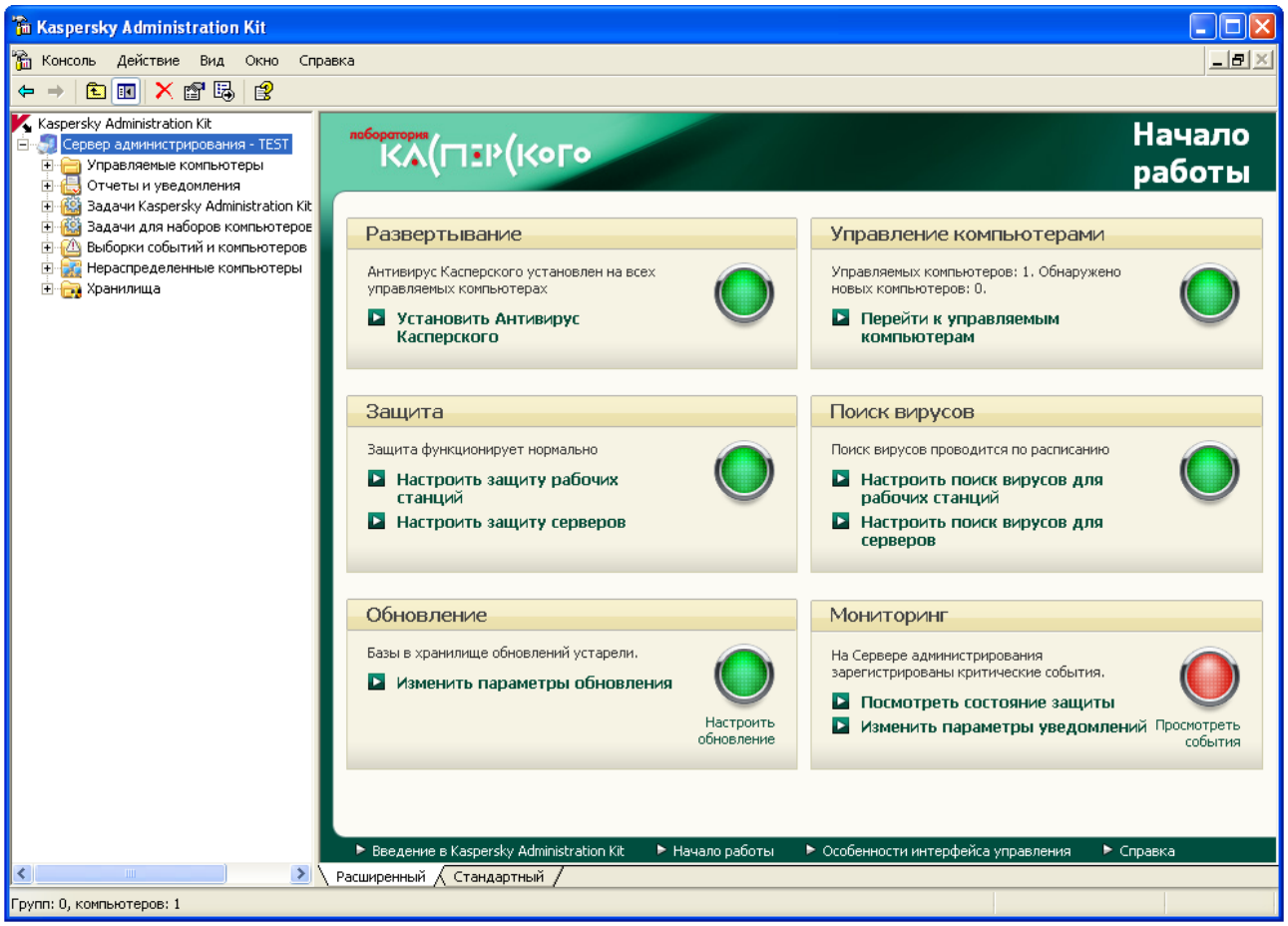


Рисунок 12. Консоль администрирования Kaspersky Administration Kit

Вид главного окна Kaspersky Administration Kit зависит от используемой на компьютере операционной системы.

При работе через Kaspersky Administration Kit управление осуществляется через определение администратором параметров программы, политик и задач.

Именованное действие, выполняемое программой называется *задачей*. В соответствии с выполняемыми функциями задачи разделяют по *типам*: задача проверки на вирусы, задача обновления программы, отката обновлений, задача установки файла ключа.

Каждой задаче соответствует набор параметров работы программы при ее выполнении. Набор параметров работы программы, общий для всех типов задач, составляет *параметры программы*. Параметры работы программы, специфичные для каждого типа задач, образуют *параметры задачи*. Параметры программы и параметры задач не пересекаются.

Особенностью централизованного управления является организация удаленных компьютеров сети в группы и управление ими через создание и определение групповых политик.

Политика – это набор параметров работы программы в группе, а также набор ограничений на переопределение данных параметров при настройке программы или настройке задачи на отдельном клиентском компьютере. Политика включает в себя параметры полной настройки всей функциональности программы, за исключением параметров, индивидуальных для конкретных экземпляров задач. Примером таких параметров могут служить параметры расписания.

Таким образом, в политику входят параметры:

- общие для всех типов задач – параметры программы;

- общие для всех экземпляров задач каждого типа – большая часть параметров задач.

Это означает, что политика для Антивируса Касперского, в число задач которого входят задачи защиты и проверки на вирусы, включает все необходимые параметры настройки программы при выполнении обоих типов задач, но не включает, например, расписание запуска этих задач и параметры, определяющие область проверки.

В этом разделе

Управление программой

Kaspersky Administration Kit предоставляет возможность удаленного управления запуском и остановкой Антивируса Касперского на отдельном клиентском компьютере, а также настройки общих параметров работы программы: включения и отключения защиты компьютера, настройки параметров отчетов и хранилищ.

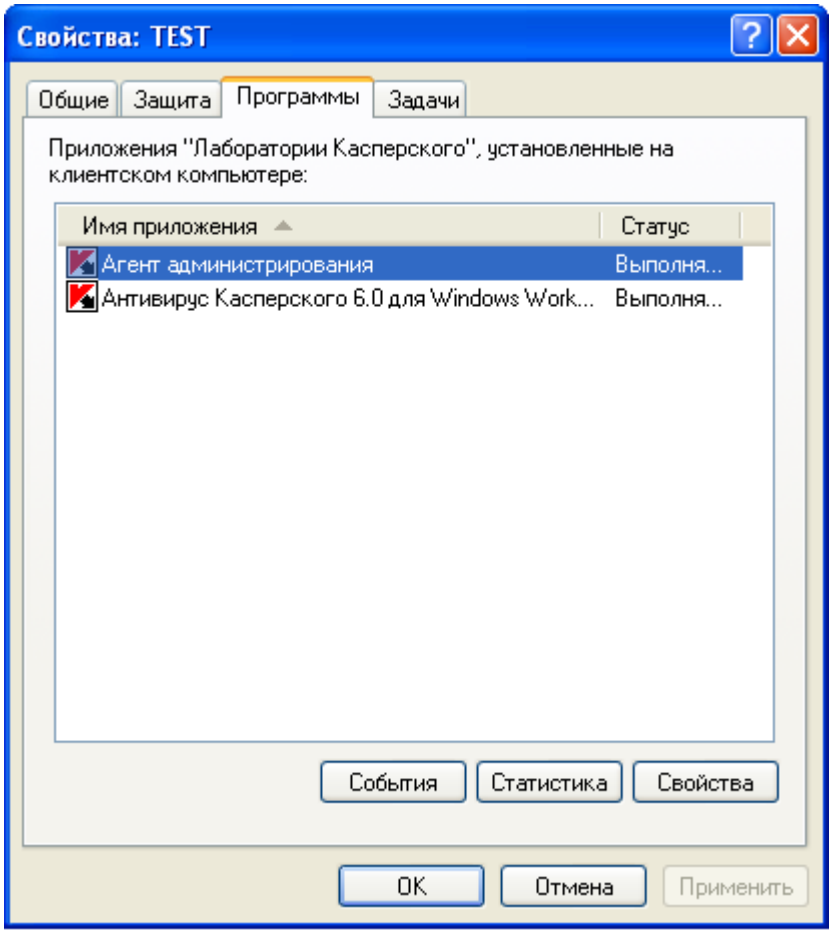


*Рисунок 13. Окно свойств клиентского компьютера. Закладка **Программы***

Чтобы перейти к управлению параметрами программы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.

2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.

3. В выбранной группе откройте вложенную папку **Клиентские компьютеры** и в панели результатов выберите компьютер, для которого вам необходимо изменить параметры программы.

4. Воспользовавшись командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**, откройте окно свойств клиентского компьютера.

5. В окне свойств клиентского компьютера на закладке **Программы** представлен полный список всех программ «Лаборатории Касперского», установленных на клиентском компьютере. Выберите программу **Антивирус Касперского 6.0 для Windows Workstations MP4**.

   Под списком программ расположены кнопки управления, с помощью которых вы можете выполнить следующие действия:

   - просмотреть список событий в работе программы, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования;

   - просмотреть текущую статистическую информацию о работе программы;

   - настроить параметры программы (см. стр. 219).

Запуск и остановка программы

Управление запуском и остановкой Антивируса Касперского 6.0 на удаленном клиентском компьютере осуществляется из окна свойств программы (см. рис. ниже).

В верхней части окна приведены название установленной программы, информация о версии, дата установки, ее статус (запущена или остановлена программа на локальном компьютере), а также информация о состоянии баз программы.

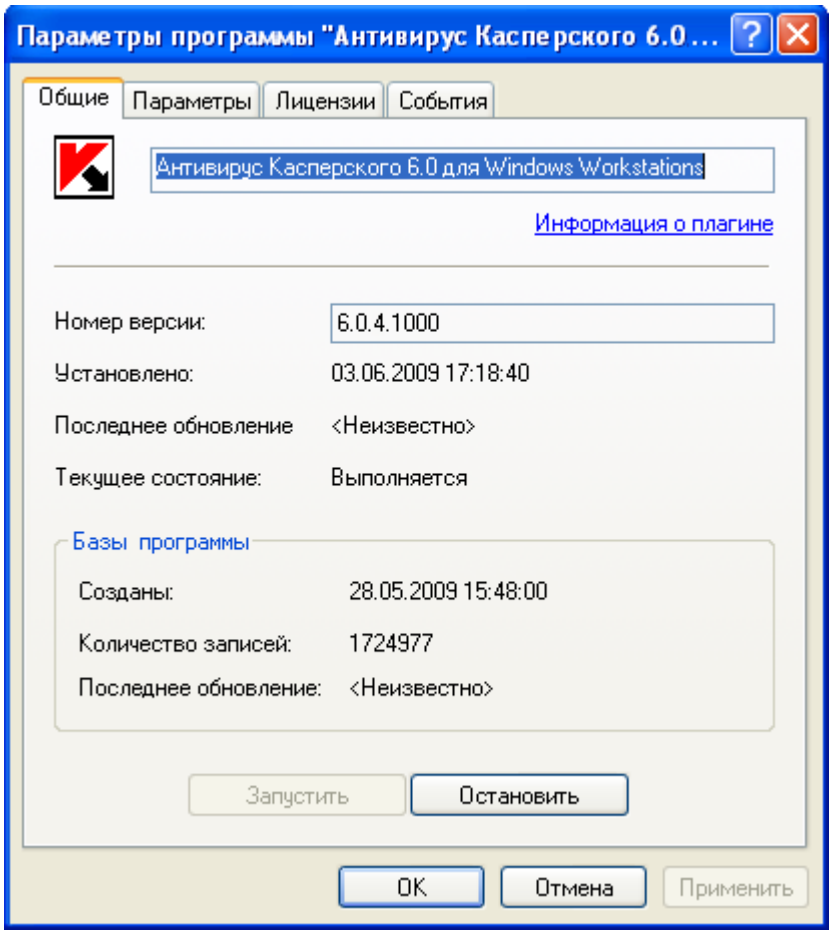


*Рисунок 14. Окно свойств программы. Закладка **Общие***

- *Чтобы остановить или запустить программу на удаленном компьютере, выполните следующие действия:*

1. Откройте окно свойств клиентского компьютера (см. стр. 216) на закладке **Программы**.

2. Выберите программу **Антивирус Касперского 6.0 для Windows Workstations MP4** и нажмите на кнопку **Свойства**.

3. В открывшемся окне свойств программы на закладке **Общие** нажмите на кнопку **Остановить** для остановки программы или **Запустить** для ее запуска.

НАСТРОЙКА ПАРАМЕТРОВ ПРОГРАММЫ

Просмотреть и изменить параметры работы программы вы можете в окне свойств программы на закладке **Параметры** (см. рис. ниже). Остальные закладки стандартны для программы Kaspersky Administration Kit, их подробное описание смотрите в одноименном Справочном руководстве.

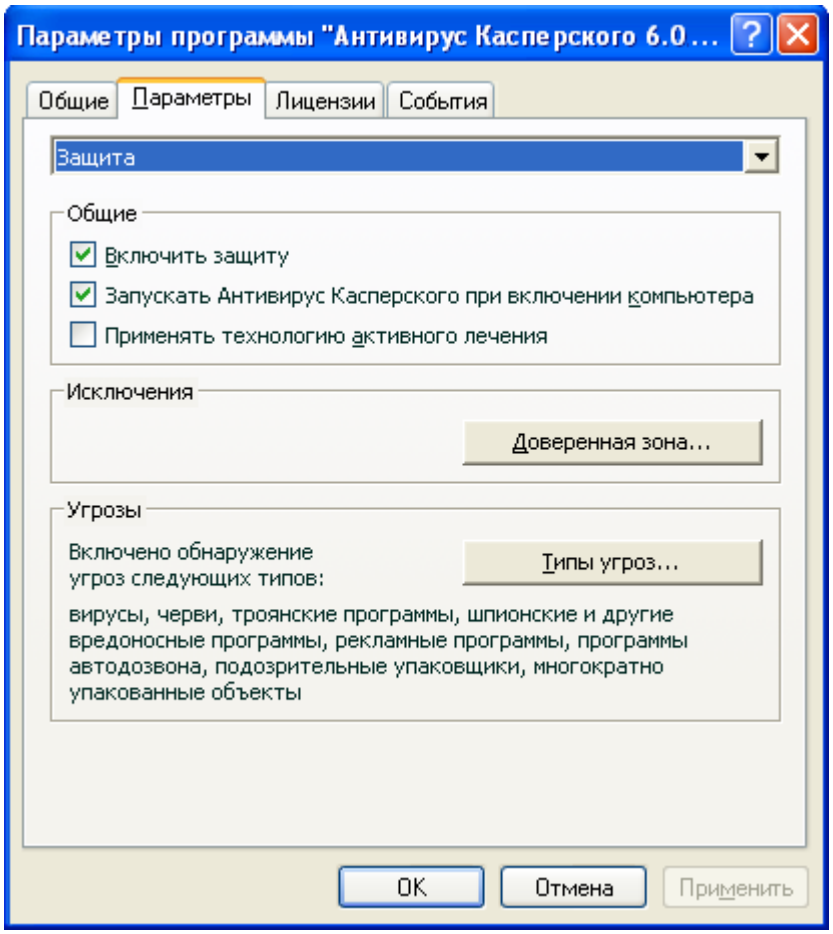


*Рисунок 15. Окно свойств программы. Закладка **Параметры***

Если для программы создана политика (см. стр. 229), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров программы будет недоступно.

Чтобы перейти к просмотру и изменению параметров работы программы, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. 216) на закладке **Программы**.

2. Выберите программу **Антивирус Касперского 6.0 для Windows Workstations MP4** и нажмите на кнопку **Свойства**.

3. В открывшемся окне свойств программы на закладке **Параметры** вы можете настраивать общие параметры работы Антивируса Касперского, параметры отчетов и хранилищ, а также параметры сети. Для этого из раскрывающегося списка в верхней части окна выберите нужное значение и произведите настройку параметров.

См. также

НАСТРОЙКА СПЕЦИФИЧЕСКИХ ПАРАМЕТРОВ

При управлении Антивирусом Касперского через Kaspersky Administration Kit вы можете включать или отключать режим взаимодействия программы с пользователем, настраивать внешний вид программы, а также редактировать информацию о технической поддержке. Настройка этих параметров производится в окне свойств программы (см. рис. ниже).

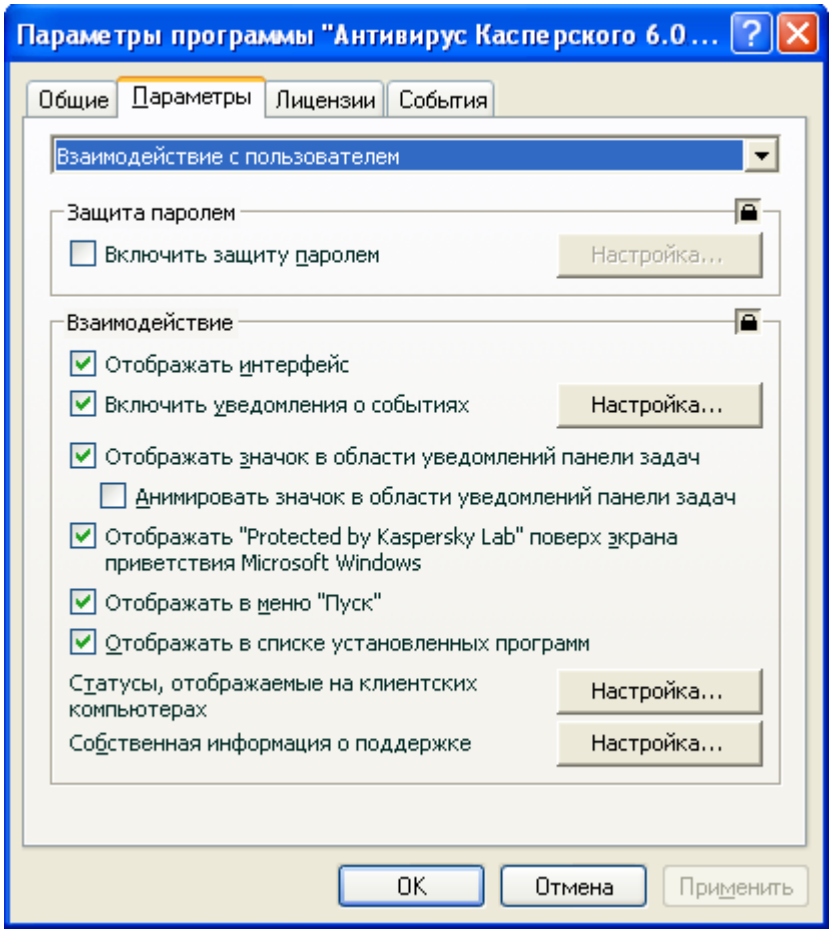


Рисунок 16. Окно свойств программы. Настройка специфических параметров

В блоке **Взаимодействие** вы можете указать параметры взаимодействия пользователя с интерфейсом Антивируса Касперского:

- *Отображение интерфейса программы на удаленном компьютере*. Если флажок **Отображать интерфейс** установлен, пользователь, работающий на удаленном компьютере, увидит значок Антивируса Касперского, всплывающие сообщения, а также будет иметь возможность принимать решение о дальнейших действиях в окнах, уведомляющих о наступлении какого-либо события. Для отключения интерактивного режима работы программы необходимо снять флажок.

- *Уведомление пользователя о событиях*. Вы можете настраивать параметры уведомлений о возникновении событий в работе программы (например, обнаружение опасного объекта). Для этого установите флажок **Включить уведомления о событиях** и нажмите на кнопку **Настройка**.

- *Отображение значка программы в области уведомлений панели задач и его анимация*. Если флажок **Отображать значок в области уведомлений панели задач** установлен, пользователь, работающий на удаленном компьютере, будет видеть значок Антивируса Касперского. В зависимости от операции, выполняемой программой, значок в системной панели меняется. По умолчанию анимация значка программы используется. В этом случае он будет отражать только статус защиты вашего компьютера: если защита включена, значок будет цветным, если она приостановлена или выключена, значок приобретет серый цвет.

- *Отображение «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows*. Если одноименный флажок установлен, то по умолчанию такой индикатор появляется в правом верхнем углу экрана в момент запуска Антивируса Касперского. Он информирует вас о том, что защита вашего компьютера от любого рода угроз включена.

  Если программа установлена на компьютере, работающем под управлением операционной системы семейства Microsoft Windows Vista, данная возможность недоступна.

- *Отображение программы в меню «Пуск»*. Если флажок ☑ **Отображать в меню «Пуск»** снят, пользователь, работающий на удаленном компьютере, не будет видеть программу в меню **Пуск**.

- *Отображение в списке установленных программ*. Если флажок ☑ **Отображать в списке установленных программ** снят, пользователь, работающий на удаленном компьютере, не будет видеть программу в списке установленных программ.

Кроме того, вы можете указать статусы программы, которые не должны отображаться в главном окне Антивируса Касперского. Для этого в поле **Статусы, отображаемые на клиентских компьютерах** нажмите на кнопку **Настройка** и в открывшемся окне установите флажки ☑ рядом с названиями нужных статусов безопасности. В этом же окне вы можете указать контрольные периоды устаревания баз программы.

Можно также редактировать информацию о технической поддержке пользователей, которая представлена в разделе **Информация о поддержке** окна **Поддержка** Антивируса Касперского на удаленном компьютере. Для доступа к окну нажмите на кнопку **Настройка** в поле **Собственная информация о поддержке**.

Если для программы создана политика (см. стр. 229), в которой запрещено переопределение некоторых параметров, то их изменение при настройке параметров программы будет недоступно.

➡ *Чтобы перейти к просмотру и изменению специфических параметров работы программы, выполните следующие действия:*

1. Откройте окно свойств клиентского компьютера (см. стр. 216) на закладке **Программы**.
2. Выберите программу **Антивирус Касперского 6.0 для Windows Workstations MP4** и нажмите на кнопку **Свойства**.
3. В открывшемся окне свойств программы на закладке **Параметры** в раскрывающемся списке выберите пункт **Взаимодействие с пользователем** и произведите настройку параметров.

Управление задачами

В данном разделе приведена информация об управлении задачами для Антивируса Касперского. Подробнее о концепции управления задачами через Kaspersky Administration Kit смотрите в одноименном Руководстве администратора.

При установке программы для каждого компьютера сети формируется набор системных задач. В этот список входят задачи защиты (Файловый Антивирус, Веб-Антивирус, Почтовый Антивирус, Проактивная защита, Анти-Шпион, Анти-Хакер, Анти-Спам, Контроль устройств), ряд задач проверки на вирусы (Полная проверка, Быстрая проверка) и задачи обновления (обновление баз и модулей программы, откат обновления).

Вы можете управлять запуском системных задач, настраивать их параметры. Удаление системных задач невозможно.

Можно также создавать собственные задачи (см. стр. 224), например, задачи проверки, обновления программы и отката обновления, задачу установки файла ключа.

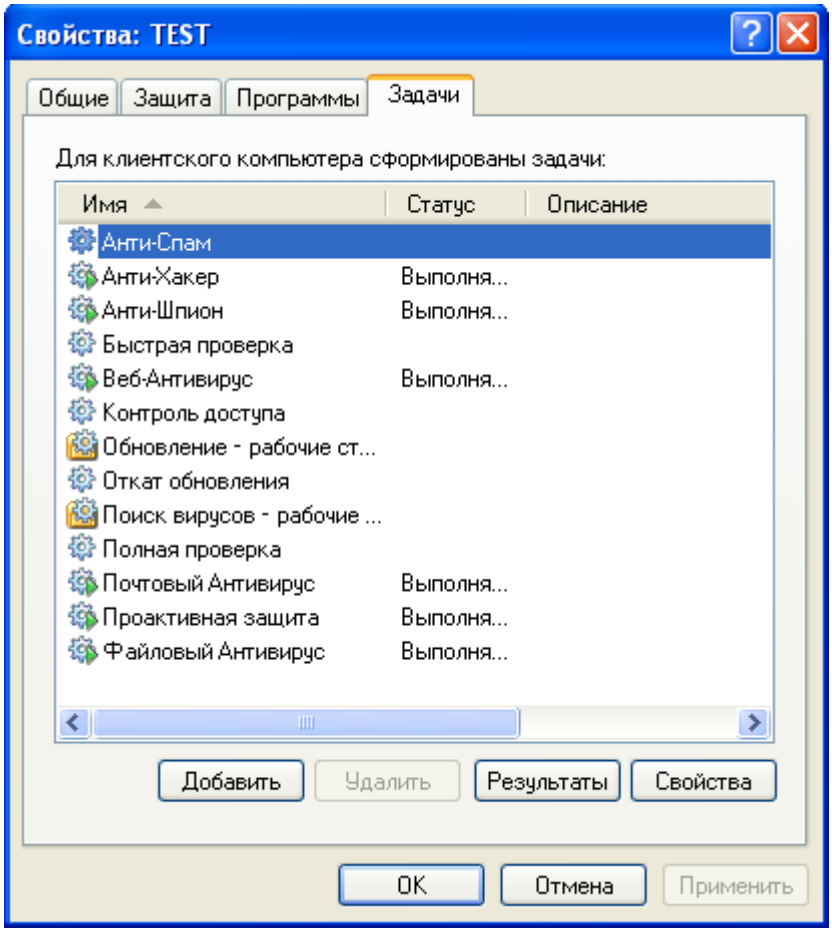


*Рисунок 17. Окно свойств клиентского компьютера. Закладка **Задачи***

Чтобы открыть список задач, сформированных для клиентского компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.
3. В выбранной группе откройте вложенную папку **Клиентские компьютеры** и в панели результатов выберите компьютер, для которого вам необходимо изменить параметры программы.
4. Воспользовавшись командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**, откройте окно свойств клиентского компьютера.
5. В открывшемся окне свойств клиентского компьютера откройте закладку **Задачи**, на которой представлен полный перечень задач, сформированных для данного клиентского компьютера.

Запуск и остановка задач

Запуск задач на компьютере выполняется только в том случае, если запущена соответствующая программа (см. стр. 217). При остановке программы выполнение запущенных задач прекращается.

Запуск и остановка задач осуществляется автоматически (в соответствии с расписанием) или вручную (при помощи команд контекстного меню), а также из окна просмотра свойств задачи. Вы можете приостановить процесс выполнения запущенной задачи и возобновить его.

Чтобы запустить, остановить, приостановить или возобновить действие задачи вручную, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. 222) на закладке **Задачи**.

2. Выберите нужную задачу и откройте ее контекстное меню. Выберите пункт **Запустить** для запуска задачи или пункт **Остановить** – для ее остановки. Можно также воспользоваться аналогичными пунктами в меню **Действие**.

   Приостановка и возобновление задачи из контекстного меню невозможно.

   или

   Выберите в списке нужную задачу и нажмите на кнопку **Свойства**. В открывшемся окне свойств задачи на закладке **Общие** при помощи одноименных кнопок запустите, остановите, приостановите или возобновите действие задачи.

Создание задачи

При работе с Антивирусом Касперского через Kaspersky Administration Kit вы можете создавать следующие типы задач:

- локальные задачи, определяемые для отдельного клиентского компьютера;
- групповые задачи, определяемые для клиентских компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, определяемые для компьютеров вне групп администрирования;
- задачи Kaspersky Administration Kit – специфические задачи Сервера обновления: задачи получения обновлений, задачи резервного копирования и задачи отправки отчетов.

Задачи для наборов компьютеров выполняются только для заданного набора компьютеров. Если в состав группы, для компьютеров которой сформирована задача удаленной установки, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести в настройки параметров уже существующей соответствующие изменения.

Над задачами можно выполнять следующие действия:

- настройку параметров задачи;
- мониторинг выполнения задачи;
- копирование и перенос задачи из одной группы в другую, а также удаление при помощи стандартных команд контекстного меню **Копировать / Вставить, Вырезать / Вставить и Удалить**, аналогичных пунктов в меню **Действие**.
- импорт и экспорт задач.

Подробные сведения о работе с задачами представлены в Справочном руководстве Kaspersky Administration Kit.

Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте окно свойств нужного клиентского компьютера (см. стр. 222) на закладке **Задачи**.

2. Нажмите на кнопку **Добавить**.

3. В результате будет запущен мастер создания новой задачи (см. стр. 225), следуйте его указаниям.

Чтобы создать групповую задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Групповые задачи**, в которой буду представлены все созданные для группы задачи.
4. С помощью ссылки **Создать новую задачу** в панели задач запустите мастер создания новой задачи. Информация об особенностях создания групповых задач представлена в Справочном руководстве Kaspersky Administration Kit.

Чтобы создать задачу для наборов компьютеров (задачу Kaspersky Administration Kit), выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. Выберите папку **Задачи для наборов компьютеров** (**Задачи Kaspersky Administration Kit**).
3. С помощью ссылки **Создать новую задачу** в панели задач запустите мастер создания новой задачи. Информация об особенностях создания задач Kaspersky Administration Kit и для наборов компьютеров представлена в Справочном руководстве Kaspersky Administration Kit.

Мастер создания локальной задачи

Мастер создания локальной задачи запускается при выборе соответствующего действия в контекстном меню клиентского компьютера или окне его свойств.

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

Шаг 1. Ввод общих данных о задаче

Первое окно мастера является вводным: здесь необходимо указать имя задачи (поле **Имя**).

Шаг 2. Выбор программы и типа задачи

На данном этапе следует указать программу, для которой создается задача, – Антивирус Касперского 6.0 для Windows Workstations MP4 или Агент администрирования. Кроме того, нужно выбрать тип задачи. Для Антивируса Касперского 6.0 возможно создание следующих задач:

- *Поиск вирусов* – задача проверки на вирусы указанных пользователем областей.
- *Обновление* – задача получения и применения пакета обновлений для программы.
- *Откат обновления* – задача отката последнего произведенного обновления программы.
- *Установка файла ключа* – задача установки файла ключа новой лицензии, необходимой для работы программы.

Шаг 3. Настройка параметров выбранного типа задачи

В зависимости от выбранного на предыдущем шаге типа задачи содержимое окна настройки параметров варьируется.

Для задачи проверки на вирусы требуется указать действие (см. стр. 130), которое будет выполнять Антивирус Касперского при обнаружении опасного объекта, а также сформировать список объектов проверки (см. стр. 129).

Для задачи обновления баз и модулей программы требуется указать источник, из которого будут загружены обновления (см. стр. 140). По умолчанию обновление выполняется с сервера обновлений программы Kaspersky Administration Kit.

Задача отката обновлений не имеет специфических настроек.

Для задачи установки файла ключа с помощью кнопки **Обзор** следует указать путь к файлу ключа. Чтобы добавить файл в качестве файла ключа для дополнительной лицензии, установите одноименный флажок ☑. Дополнительная лицензия вступает в силу по окончании срока действия активной лицензии.

Информация о указанной лицензии (номер лицензии, тип и дата окончания) представлена в поле ниже.

Шаг 4. Настройка расписания

По завершении настройки параметров задач вам предлагается настроить расписание автоматического запуска задачи.

Для этого в окне настройки расписания выберите из раскрывающегося списка периодичность запуска задачи и в нижней части окна уточните параметры расписания.

Шаг 5. Завершение создания задачи

В последнем окне мастер проинформирует вас об успешном завершении процесса создания задачи.

Настройка параметров задач

Настройка параметров задач программы через интерфейс Kaspersky Administration Kit аналогична настройке через локальный интерфейс Антивируса Касперского. Исключение составляют параметры, которые настраиваются индивидуально для каждого пользователя, например, «черные» и «белые» списки Анти-Спама, а также параметры, специфичные для Kaspersky Administration Kit: например, параметры, разрешающие (запрещающие) пользователю управлять локальной задачей проверки.

Если для программы создана политика (см. стр. 229), в которой запрещено переопределение некоторых параметров, их изменение при настройке задач будет недоступно.

Все закладки окна свойств задачи, кроме закладки **Параметры** (см. рис. ниже), стандартны для программы Kaspersky Administration Kit. Их подробное описание смотрите в одноименном справочном руководстве. Закладка **Параметры** содержит специфические параметры Антивируса Касперского; содержимое данной закладки варьируется в зависимости от выбранного типа задачи.

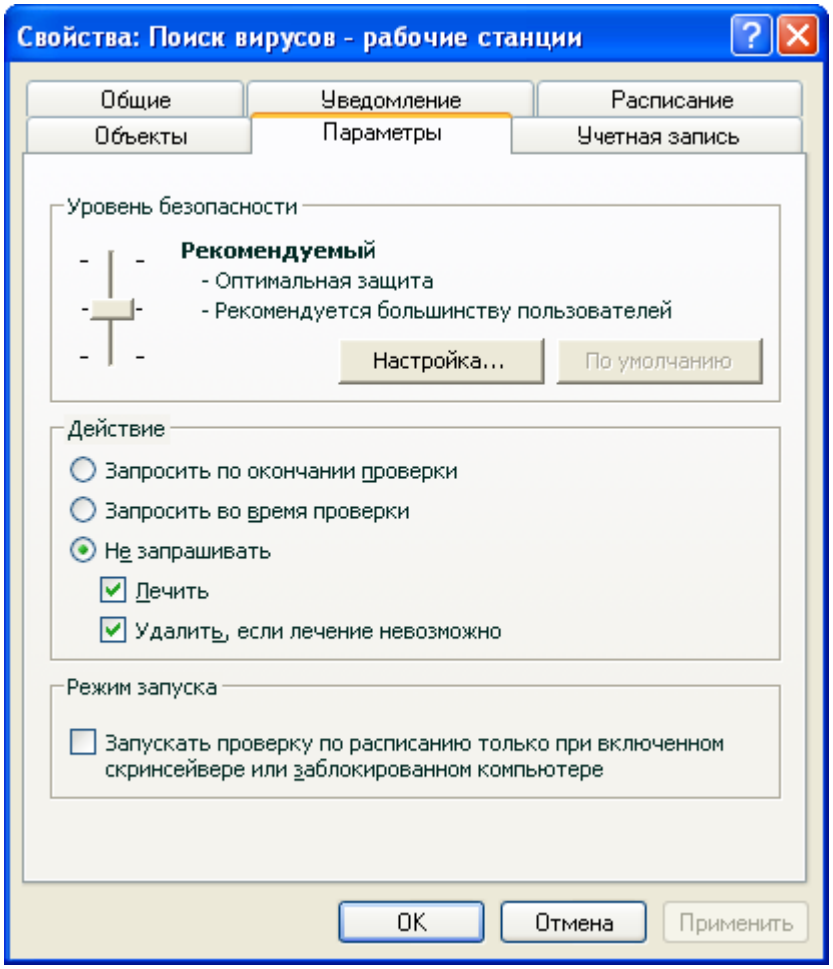


*Рисунок 18. Окно свойств задачи. Закладка **Параметры***

Чтобы перейти к просмотру и редактированию локальной задачи, выполните следующие действия:

1. Откройте окно свойств клиентского компьютера (см. стр. 222) на закладке **Задачи**.

2. Выберите задачу в списке и воспользуйтесь кнопкой **Свойства**. В результате будет открыто окно настройки параметров задачи.

Чтобы перейти к групповым задачам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.

2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.

3. В выбранной группе откройте вложенную папку **Групповые задачи**, в которой буду представлены все созданные для группы задачи.

4. Выберите в дереве консоли нужную задачу для перехода к просмотру и редактированию ее свойств.

   В панели задач будет представлена сводная информация о задаче, а также ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях групповых задач содержится в Справочном руководстве Kaspersky Administration Kit.

Чтобы перейти к задачам для наборов компьютеров (задачам Kaspersky Administration Kit), выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. Выберите папку **Задачи для наборов компьютеров** (**Задачи Kaspersky Administration Kit**).
3. Выберите дереве консоли нужную задачу для перехода к просмотру и редактированию ее свойств.

   В панели задач будет представлена сводная информация о задаче, а также ссылки для управления выполнением задачи и редактирования ее параметров. Информация об особенностях задач Kaspersky Administration Kit и для наборов компьютеров содержится в Справочном руководстве Kaspersky Administration Kit.

Управление политиками

Определение политик позволяет распространять единые настройки параметров программы и задач на клиентские компьютеры, входящие в состав одной группы администрирования.

В данном разделе приведена информация о создании и настройке политики для Антивируса Касперского 6.0 для Windows Workstations MP4. Более подробную информацию о концепции управления политиками через Kaspersky Administration Kit смотрите в Руководстве администратора к данному продукту.

При создании и настройке политики вы можете налагать запрет на полное или частичное изменение ее параметров в политиках вложенных групп, параметрах задач и параметрах программы. Для этого нажмите на кнопку  . Для параметров, запрещенных к изменению, она должна принять вид  .

Чтобы открыть список политик, сформированных для Антивируса Касперского, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием группы, в состав которой входит клиентский компьютер.
3. В выбранной группе откройте вложенную папку **Политики**: в дереве консоли буду представлены все созданные для группы политики.

Создание политики

При работе с Антивирусом Касперского через Kaspersky Administration Kit вы можете создавать для него политики.

Над политиками можно выполнять следующие действия:

- настройку параметров политики;
- копирование и перенос политики из одной группы в другую, а также удаление при помощи стандартных команд контекстного меню **Копировать / Вставить, Вырезать / Вставить и Удалить**, а также аналогичных пунктов в меню **Действие**.
- импорт и экспорт параметров политики.

Более подробная информация о работе с политиками представлена в Справочном руководстве Kaspersky Administration Kit.

Чтобы создать политику, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Политики**, в которой буду представлены все созданные для группы политики.
4. С помощью ссылки **Создать новую политику** в панели задач запустите мастер создания новой задачи.
5. В открывшемся окне будет запущен мастер создания новой политики (см. стр. 229): следуйте его указаниям.

Мастер создания политики

Мастер создания политики запускается при выборе соответствующего действия в контекстном меню папки **Политики** нужной группы администрирования или ссылки в панели результатов (для папки **Политики**).

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

Шаг 1. Ввод общих данных о политике

Первые окна мастера являются вводными. Здесь необходимо указать имя политики (поле **Имя**) и выбрать программу **Антивирус Касперского 6.0 для Windows Workstations MP4** из раскрывающегося списка **Имя программы**.

Если мастер создания политики был запущен из панели задач узла **Политики** (с помощью ссылки **Создать политику для Антивируса Касперского для Windows Workstations MP4**), выбор программы отсутствует.

Если вы хотите создать политику на основании параметров существующей политики для предыдущей версии программы, установите флажок **Взять параметры из существующей политики** и выберите политику, параметры которой будут использованы в новой политике. Чтобы определить политику, нажмите на кнопку **Выбрать**. В результате будет представлен список существующих политик, которые могут быть использованы при создании политики.

Шаг 2. Выбор статуса политики

В данном окне вам предлагается указать статус политики после ее создания, выбрав для этого один из вариантов: активная политика, неактивная политика, политика для мобильного пользователя. Подробнее о статусах политик смотрите в Справочном руководстве Kaspersky Administration Kit.

В группе для одной программы может быть создано несколько политик, но действующей (активной) может быть только одна из них.

Шаг 3. Импорт параметров программы

Если у вас имеется ранее сохраненный файл с параметрами программы, можно указать его на этом шаге мастера с помощью кнопки **Загрузить.** При этом в следующих окнах мастера будут уже отображать импортированные параметры.

Шаг 4. Настройка параметров защиты

На данном этапе вы можете включать (отключать), а также настраивать компоненты защиты, которые будут использоваться в политике.

По умолчанию все компоненты защиты включены. Чтобы отключить какой-либо из них, снимите флажок рядом с его названием. Для детальной настройки компонента защиты выберите его в списке и нажмите на кнопку **Настройка**.

Шаг 5. Настройка защиты паролем

В этом окне мастера (см. рис. ниже) вам предлагается настроить общие параметры работы программы: включить (отключить) самозащиту, включить (отключить) возможность внешнего управления системной службой, установить защиту паролем на работу с программой и ее удаление.

Шаг 6. Настройка доверенной зоны

В этом окне мастера вам предлагается настроить параметры доверенной зоны: добавить в список доверенных программ программное обеспечение, используемое для администрирования сети, и исключить из области проверки некоторые типы файлов.

Шаг 7. Настройка параметров взаимодействия с пользователем

На данном шаге вы можете указать параметры взаимодействия пользователя с Антивирусом Касперского:

- отображение интерфейса программы на удаленном компьютере;
- уведомление пользователя о событиях;
- отображение значка программы в области уведомлений панели задач и его анимация;
- отображение «Protected by Kaspersky Lab» поверх экрана приветствия Microsoft Windows;
- отображение программы в меню «Пуск»;
- отображение в списке установленных программ.

Шаг 8. Завершение создания политики

Последнее окно мастера проинформирует вас об успешном завершении процесса создания политики.

По окончании работы мастера политика для заданной программы будет добавлена в папку **Политики** соответствующей группы администрирования и представлена в дереве консоли.

Для созданной политики вы можете отредактировать ее параметры и установить ограничения на изменения ее параметров с помощью кнопок  и  для каждой группы настроек. При значке  пользователь на клиентском компьютере не сможет изменить настройки. При значке  пользователю доступно редактирование параметров. Распространение политики на клиентские компьютеры будет осуществлено при первой синхронизации клиентов с сервером.

Настройка параметров политики

На этапе редактирования вы можете вносить изменения в политику, налагать запрет на изменение параметров в политиках вложенных групп, в параметрах программы и параметрах задач. Параметры политики можно изменять в окне свойств политики (см. рис. ниже).

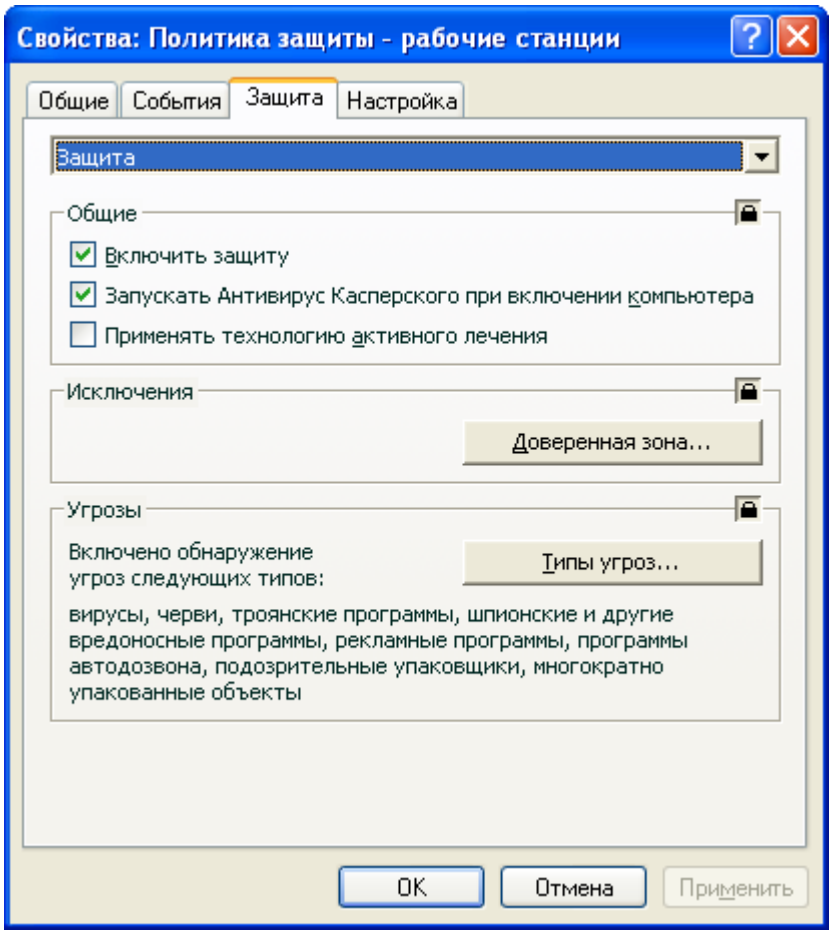


*Рисунок 19. Окно свойств политики. Закладка **Защита***

Все закладки (кроме **Защита** и **Настройка**) стандартны для программы Kaspersky Administration Kit. Их подробное описание смотрите в одноименном Руководстве администратора.

Параметры политики для Антивируса Касперского 6.0 включают в себя параметры программы (см. стр. 219) и параметры задач (см. стр. 226). На закладке **Настройка** представлены параметры программы, а на закладке **Защита** – параметры задач.

Для настройки параметров выберите из раскрывающегося списка в верхней части окна нужное значение и произведите настройку.

Чтобы перейти к просмотру и настройке параметров политики, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Administration Kit.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы.
3. В выбранной группе откройте вложенную папку **Политики**, в которой буду представлены все созданные для группы политики.
4. Выберите в дереве консоли нужную политику для перехода к просмотру и редактированию ее свойств.

5. В панели задач будет представлена сводная информация о политике и ссылки для управления статусом политики и редактирования ее параметров.

   или

   Откройте контекстное меню выбранной политики и с помощью пункта **Свойства** откройте окно настройки политики для Антивируса Касперского.

   Информация об особенностях работы с политиками содержится в Справочном руководстве Kaspersky Administration Kit.

ИСПОЛЬЗОВАНИЕ СТОРОННЕГО КОДА

При создании Антивируса Касперского использовался код сторонних производителей.

В этом разделе

Библиотека Boost-1.30.0

При создании программы использовалась библиотека Boost-1.30.0.

Copyright (C) 2003, Christof Meerwald

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the «Software») to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Библиотека LZMA SDK 4.40, 4.43

При создании программы использовалась библиотека LZMA SDK 4.40, 4.43.

Библиотека OPENSSL-0.9.8D

При создании программы использовалась библиотека OpenSSL-0.9.8d.

Copyright (C) 1998-2007, The OpenSSL Project

LICENSE

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL

please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

«This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)»

4. The names «OpenSSL Toolkit» and «OpenSSL Project» must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called «OpenSSL» nor may «OpenSSL» appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

«This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)»

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA,

lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution

as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

«This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)»

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

«This product includes software written by Tim Hudson (tjh@cryptsoft.com)»

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

Библиотека Windows Template Library 7.5

При создании программы использовалась библиотека Windows Template Library 7.5.

Библиотека Windows Installer XML (WiX) toolset 2.0

При создании программы использовалась библиотека Windows Installer XML (WiX) toolset 2.0.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE («AGREEMENT»). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

«Contribution» means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

«Contributor» means any person or entity that distributes the Program.

«Licensed Patents» mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

«Program» means the Contributions distributed in accordance with this Agreement.

«Recipient» means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor («Commercial Contributor») hereby agrees to defend and indemnify every other Contributor («Indemnified Contributor») against any losses, damages and costs (collectively «Losses») arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN «AS IS» BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Библиотека ZIP-2.31

При создании программы использовалась библиотека Zip-2.31.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, «Info-ZIP» is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens,

George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided «as is,» without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip,» «UnZipSFX,» «WiZ,» «Pocket UnZip,» «Pocket Zip,» and «MacZip» for its own source and binary releases.

Библиотека ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3

При создании программы использовалась библиотека Zlib-1.0.4, ZLIB-1.0.8, Zlib-1.1.3, Zlib-1.2.3.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Библиотека UNZIP-5.51

При создании программы использовалась библиотека UnZip-5.51.

Copyright (c) 1990-2004, Info-ZIP

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, «Info-ZIP» is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided «as is,» without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered

versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip,» «UnZipSFX,» «WiZ,» «Pocket UnZip,» «Pocket Zip,» and «MacZip» for its own source and binary releases.

Библиотека LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

При создании программы использовалась библиотека libpng-1.0.1, libpng-1.2.8, libpng-1.2.12.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following

this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, «Contributing Authors» is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied «AS IS». The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A «png_get_copyright» function is available, for convenient use in «about» boxes and the like:

printf(«%s»,png_get_copyright(NULL));

Also, the PNG logo (in PNG format, of course) is supplied in the files «pngbar.png» and «pngbar.jpg» (88x31) and «pngnow.png» (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a

certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

Библиотека LIBJPEG-6B

При создании программы использовалась библиотека libjpeg-6b.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided «AS IS», and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that «this software is based in part on the work of the Independent JPEG Group».

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code,

not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name

in advertising or publicity relating to this software or products derived from

it. This software may be referred to only as «the Independent JPEG Group's

software».

We specifically permit and encourage the use of this software as the basis of

commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than

the foregoing paragraphs do.

The Unix configuration script «configure» was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has

been removed altogether, and the GIF writer has been simplified to produce

«uncompressed GIFs». This technique does not use the LZW algorithm; the

resulting GIF files are larger than usual, but are readable by all standard

GIF decoders.

We are required to state that

«The Graphics Interchange Format(c) is the Copyright property of

CompuServe Incorporated. GIF(sm) is a Service Mark property of

CompuServe Incorporated.»

Библиотека LIBUNGIF-4.1.4

При создании программы использовалась библиотека libungif-4.1.4.

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Библиотека PCRE-3.0

При создании программы использовалась библиотека PCRE-3.0.

Copyright (C) 1997-1999, University of Cambridge

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2000 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose Licence (GPL), then the terms of that licence shall supersede any condition above with which it is incompatible.

End

Библиотека REGEX-3.4A

При создании программы использовалась библиотека regex-3.4a.

Copyright (C) 1992, 1993, 1994, 1997, Henry Spencer

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

Библиотека MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

При создании программы использовалась библиотека MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.

Библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

При создании программы использовалась библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

Библиотека INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

При создании программы использовалась библиотека Independent implementation of MD5 (RFC 1321)-v. 04.11.1999.

Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the «RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as «derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm» in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided «as is» without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Библиотека CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

При создании программы использовалась библиотека Conversion routines between UTF32, UTF-16, and UTF-8-v. 02.11.2004.

Copyright 2001-2004 Unicode, Inc.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Библиотека COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum

При создании программы использовалась библиотека Cool Owner Drawn Menus-v. 2.4, 2.63 By Brent Corkum.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware,Shareware,Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

Библиотека FMT-2002

При создании программы использовалась библиотека Fmt-2002.

Copyright (C) 2002, Lucent Technologies

The authors of this software are Rob Pike and Ken Thompson.Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED «AS IS», WITHOUT ANY EXPRESS OR IMPLIED

WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

Библиотека EXPAT-1.95.2

При создании программы использовалась библиотека expat-1.95.2.

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY

CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,

TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE

SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Библиотека LIBNKFM-0.1

При создании программы использовалась библиотека libnkfm-0.1.

Copyright (C) 1987, Fujitsu LTD (Itaru ICHIKAWA)

Everyone is permitted to do anything on this program including copying, modifying, improving, as long as you don't try to pretend that you wrote it. i.e., the above copyright notice has to appear in all copies. Binary distribution requires original version messages. You don't have to ask before copying, redistribution or publishing.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE.

Библиотека PLATFORM INDEPENDENT IMAGE CLASS

При создании программы использовалась библиотека Platform Independent Image Class.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

Covered code is provided under this license on an «as is» basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Библиотека NETWORK KANJI FILTER (PDS VERSION)-2.0.5

При создании программы использовалась библиотека Network Kanji Filter (PDS Version)-2.0.5.

Библиотека DB-1.85

При создании программы использовалась библиотека db-1.85.

Библиотека LIBNET-1991, 1993

При создании программы использовалась библиотека libnet-1991, 1993.

This code is derived from software contributed to Berkeley by Berkeley Software Design, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Библиотека GETOPT-1987, 1993, 1994

При создании программы использовалась библиотека getopt-1987, 1993, 1994.

Copyright (C) 1987, 1993, 1994, The Regents of the University of California

---

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Библиотека MERGE-1992, 1993

При создании программы использовалась библиотека merge-1992, 1993.

Библиотека FLEX PARSER (FLEXLEXER)-V. 1993

При создании программы использовалась библиотека Flex parser (FlexLexer)-v. 1993.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

Библиотека STRPTIME-1.0

При создании программы использовалась библиотека strptime-1.0.

Библиотека EnsureCleanup, SWMRG, Layout-v. 2000

При создании программы использовалась библиотека EnsureCleanup, SWMRG, Layout-v. 2000.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities («U.S. Government»), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

Библиотека OUTLOOK2K ADDIN-2002

При создании программы использовалась библиотека Outlook2K Addin-2002.

Copyright (C) 2002, Amit Dey email :amitdey@joymail.com

This code may be used in compiled form in any way you desire. This file may be redistributed unmodified by any means PROVIDING it is not sold for profit without the authors written consent, and providing that this notice and the authors name is included.

This file is provided 'as is' with no expressed or implied warranty. The author accepts no liability if it causes any damage to your computer.

Do expect bugs.

Please let me know of any bugs/mods/improvements.

and I will try to fix/incorporate them into this file.

Enjoy!

Библиотека STDSTRING- V. 1999

При создании программы использовалась библиотека StdString- v. 1999.

Copyright (C) 1999, Joseph M. O'Leary

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your $30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

Библиотека T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

При создании программы использовалась библиотека T-Rex (tiny regular expression library)- v. 2003-2006.

Библиотека NTSERVICE- V. 1997

При создании программы использовалась библиотека NTService- v. 1997.

Библиотека SHA-1-1.2

При создании программы использовалась библиотека SHA-1-1.2.

Библиотека COCOA SAMPLE CODE- V. 18.07.2007

При создании программы использовалась библиотека Cocoa sample code- v. 18.07.2007.

Библиотека PUTTY SOURCES-25.09.2008

При создании программы использовалась библиотека PUTTY SOURCES-25.09.2008. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified http://www.opensource.org/licenses/ and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

Другая информация

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) «Крипто-Си», разработанная ООО «КриптоЭкс», http://www.cryptoex.ru.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) «Агава-С», разработанная ООО «Р-Альфа».

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают Пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода Пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом.

ГЛОССАРИЙ ТЕРМИНОВ

Б

«Белый» список адресов

Список электронных адресов, входящие сообщения с которых не проверяются программой «Лаборатории Касперского».

Ч

«Черный» список адресов

Список электронных адресов, входящие сообщения с которых блокируются программой «Лаборатории Касперского» независимо от их содержания.

«Черный» список файлов ключей

База данных, содержащая информацию о заблокированных «Лабораторией Касперского» файлах ключей, владельцы которых нарушили условия лицензионного соглашения, и о файлах ключей, которые были выписаны, но по какой-либо причине не были проданы либо были заменены. Файл «черного» списка необходим для работы программ «Лаборатории Касперского». Содержимое файла обновляется вместе с базами.

В

Boot-вирус (загрузочный)

Вирус, поражающий загрузочные секторы дисков компьютера. Вирус «заставляет» систему при ее перезапуске считывать в память и отдавать управление не оригинальному коду загрузчика, а коду вируса.

O

OLE-объект

Присоединенный или встроенный в другой файл объект. Программа «Лаборатории Касперского» позволяет проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

S

SOCKS

Протокол прокси-сервера, позволяющий реализовать двухточечное соединение между компьютерами внутренней и внешней сетей.

А

Агент администрирования

Компонент программы Антивируса Касперского, осуществляющий взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-программ из состава продуктов компании. Для Novell- и Unix-программ «Лаборатории Касперского» существуют отдельные версии Агента администрирования.

Администратор Антивируса Касперского

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Антивируса Касперского.

Активная лицензия

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

Архив

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

Б

Базы

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз. Для повышения качества обнаружения угроз мы рекомендуем регулярно копировать обновления баз с серверов обновлений «Лаборатории Касперского».

Базы контентной фильтрации

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие письма-образцы спама и характерные для спама термины (слова и словосочетания). На их основании выполняется лингвистический анализ содержания сообщений и вложений. Базы постоянно обновляются в «Лаборатории Касперского». Это требует от администратора проведения регулярного обновления баз, используемых программой.

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

В

Вирусная атака

Ряд целенаправленных попыток заразить компьютер вирусом.

Возможно зараженный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Д

Доверенный процесс

Программный процесс, файловые операции которого не контролируется программой «Лаборатории Касперского» в режиме постоянной защиты. То есть все объекты, запускаемые, открываемые и сохраняемые доверенным процессом, не проверяются.

Дополнительная лицензия

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

З

Заголовок

Информация, которая содержится в начале файла или сообщения и состоит из низкоуровневых данных о статусе и обработке файла (сообщения). В частности, заголовок сообщения электронной почты содержит такие сведения, как данные об отправителе, получателе и дату.

Загрузочный сектор диска

Загрузочный сектор — это особый сектор на жёстком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа «Лаборатории Касперского» позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

Зараженный объект

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

И

Исключение

Исключение - объект исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

К

Карантин

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

Клиент

Программа, которая связывается по сети с сервером для использования определенной службы. Например, **Netscape** является клиентом **WWW** и связывается с веб-серверами для загрузки веб-страниц.

Контролируемый объект

Файл, перемещаемый по протоколам HTTP, FTP или SMTP через межсетевой экран и направляемый на проверку программе «Лаборатории Касперского».

Л

Лечение объектов

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных, либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В случае, если лечение является первичным действием над объектом (самое первое действие над объектом сразу после его обнаружения), то перед его выполнением создается резервная копия объекта. В процессе лечения часть данных может быть потеряна. Вы можете использовать эту копию для восстановления объекта до предшествующего лечению состояния.

Лечение объектов при перезагрузке

Способ обработки зараженных объектов, используемых в момент лечения другими программами. Заключается в создании копии зараженного объекта, лечении созданной копии и замене при следующей перезагрузке исходного зараженного объекта его вылеченной копией.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

M

Максимальная защита

Уровень безопасности вашего компьютера, соответствующий максимально полной защите, которую может обеспечить программа. При таком уровне защиты на присутствие вирусов проверяются все файлы компьютера, сменных носителей и сетевых дисков, если таковые подключены к компьютеру.

Маска подсети

Маска подсети (также именуемая сетевой маской) и сетевой адрес определяют адреса входящих в состав сети компьютеров.

Маска файла

Представление имени и расширения файла общими символами. Двумя основными символами, используемыми в масках файлов, являются ***** и **?** (где ***** – любое число символов, а **?** – любой один символ). При помощи данных знаков можно представить любой файл. Обратите внимание, что имя и расширение файла всегда пишутся через точку.

H

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Антивирус Касперского.

Нецензурное сообщение

Электронное сообщение, содержащее ненормативную лексику.

O

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Обновление баз

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование баз с серверов обновлений «Лаборатории Касперского» на компьютер и автоматическое подключение их к программе.

Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Опасный объект

Объект, внутри которого содержится вирус. Не рекомендуется работать с такими объектами, поскольку это может привести к заражению компьютера. При обнаружении зараженного объекта рекомендуется лечить его с помощью программы «Лаборатории Касперского» или удалить, если лечение невозможно.

П

Пакет обновлений

Пакет файлов для обновления программного обеспечения, который копируется из интернета и устанавливается на вашем компьютере.

Папка данных

Папка размещения необходимых для работы программы служебных папок и баз данных. В случае смены папки данных, вся входящая в ее состав информация должна быть сохранена по новому адресу.

Перехватчик

Подкомпонент программы, отвечающий за проверку определенных типов почтовых сообщений. Набор подлежащих установке перехватчиков зависит от того, в какой роли или в какой комбинации ролей развернута программа.

Подозрительное сообщение

Сообщение, которое нельзя однозначно классифицировать как спам, но при проверке оно вызвало подозрение (например, некоторые виды рассылок и рекламных сообщений).

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Подозрительные объекты обнаруживаются при помощи эвристического анализатора.

Помещение объектов на карантин

Способ обработки возможно зараженного объекта, при котором доступ к объекту блокируется, и он перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения. Помещенные на карантин объекты могут быть проверены с использованием обновленных баз Антивируса, проанализированы администратором или отправлены в «Лабораторию Касперского».

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера», для размещения и распространения вредоносного объекта. Как правило, это исполняемые файлы, например, с расширением **com**, **exe**, **dll** и др. Риск внедрения в такие файлы вредоносного кода достаточно.

Почтовые базы

Базы, включающие почтовые сообщения, хранящиеся на вашем компьютере и имеющие специальный формат. Каждое входящее / исходящее письмо помещается в почтовую базу после его получения / отправки. Такие базы проверяются во время полной проверки компьютера.

Входящие и исходящие почтовые сообщения в момент их получения и отправки анализируются на присутствие вирусов в реальном времени, если включена постоянная защита.

Проверка по требованию

Режим работы программы «Лаборатории Касперского», который инициируется пользователем и направлен на проверку любых файлов.

Проверка трафика

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и пр.).

Проверка хранилищ

Проверка хранящихся на почтовом сервере сообщений и содержимого общих папок с использованием последней версии баз. Проверка осуществляется в фоновом режиме и может запускаться как по расписанию, так и вручную. Проверяются все общие папки и почтовые хранилища (mailbox storage). При проверке могут быть обнаружены новые вирусы, информация о которых отсутствовала в базах на момент предыдущих проверок.

Пропуск объекта

Способ обработки, при котором объект пропускается пользователю без каких-либо изменений. Если параметрами отчета задано протоколирование событий данного типа, информация об обнаруженном объекте заносится в отчет.

Простой объект

Тело письма или простое вложение, например, в виде исполняемого файла. См. также объект-контейнер.

Протокол

Четко определенный и стандартизованный набор правил, регулирующих взаимодействие между клиентом и сервером. К ряду хорошо известных протоколов и связанных с ними служб относятся: HTTP (WWW), FTP и NNTP (новости).

Протокол интернета (IP)

Базовый протокол сети интернет, используемый без изменений со времени его разработки в 1974 г. Он осуществляет основные операции передачи данных с одного компьютера на другой и служит в качестве основы для протоколов более высокого уровня, таких как TCP и UDP. Он управляет соединением и обработкой ошибок. Такие технологии как NAT и маскарад делают возможным скрытие больших частных сетей за небольшим числом IP-адресов (или даже одним адресом), что позволяет удовлетворить запросы постоянно растущего интернета, используя относительно ограниченное адресное пространство IPv4.

Р

Резервное копирование

Создание резервной копии файла перед его лечением или удалением и размещение этой копии в резервном хранилище с возможностью последующего восстановления файла, например, для его проверки с помощью обновленных баз.

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением.

Рекомендуемый уровень

Уровень безопасности, базирующийся на параметрах работы программы, рекомендуемых экспертами «Лаборатории Касперского» и обеспечивающих оптимальную защиту вашего компьютера. Данный уровень установлен для использования по умолчанию.

С

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей на ваш компьютер.

Сетевой порт

Параметр протоколов TCP и UDP, определяющий назначение пакетов данных в IP-формате, передаваемых на хост по сети и позволяющий различным программам, выполняемым на одном хосте, получать данные независимо друг от друга. Каждая программа обрабатывает данные, поступающие на определённый порт (иногда говорят, что программа «слушает» этот номер порта).

Обычно за некоторыми распространёнными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу HTTP на TCP-порт 80), хотя в общем случае программа может использовать любой протокол на любом порте. Возможные значения: от 1 до 65535.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения небольшой конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторый веб-сайт.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

Спам

Несанкционированная массовая рассылка электронных сообщений, чаще всего рекламного характера.

Срок действия лицензии

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». Срок действия лицензии, как правило, составляет календарный год со дня ее установки. После окончания срока действия лицензии функциональность программы сокращается: вы не сможете обновлять базы программы.

Срочное обновление

Критическое обновление модулей программы «Лаборатории Касперского».

Статус защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Т

Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что параметры проверки (антивирусные базы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой «Лаборатории Касперского» и 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 антивирусные базы, архив будет проверен повторно.

Ограничения технологии **iChecker**:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять был ли он изменен с момента последней проверки;

- технология поддерживает ограниченное число форматов (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

У

Удаление объекта

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

Удаление сообщения

Способ обработки электронного сообщения, содержащего признаки спама, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам. Перед удалением сообщения его копия сохраняется в резервном хранилище (если данная функциональность не отключен).

Упакованный файл

Файл архива, который содержит в себе некоторую программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень важности события

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

- **Критическое событие**.
- **Отказ функционирования**.
- **Предупреждение**.
- **Информационное сообщение**.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Ф

Файл ключа

Файл с расширением .key, который является вашим личным «ключом», необходимым для работы с программой «Лаборатории Касперского». Файл ключа входит в комплект поставки продукта, если вы приобрели его у дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

Х

Хост

Компьютер, на котором работает серверное программное обеспечение. Один хост может выполнять множество серверных программ: т.е., FTP-сервер, почтовый сервер и веб-сервер могут работать на одном хосте. Пользователь использует клиентскую программу, например, браузер, для доступа на хост. Термин сервер также часто применяется для обозначения компьютера, на котором работает серверное ПО, что размывает практическое различие между сервером и хостом.

В области телекоммуникаций хост - это компьютер, с которого поступает информация (такая как FTP-файлы, новости или веб-страницы). В интернете хосты часто также называют **узлами**.

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Э

Эвристический анализатор

Технология обнаружения угроз, неопределяемых с помощью баз Антивируса. Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. 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 тысячи 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 мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), 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 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.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.viruslist.ru
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

I

A

B

Г

Д

З

И

К

Л

М

О

П

Р

С

У

Ф

Х

Э