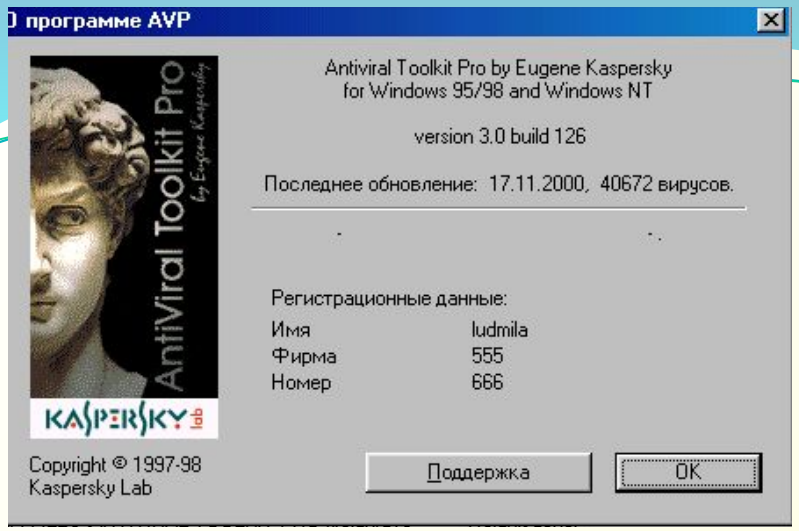
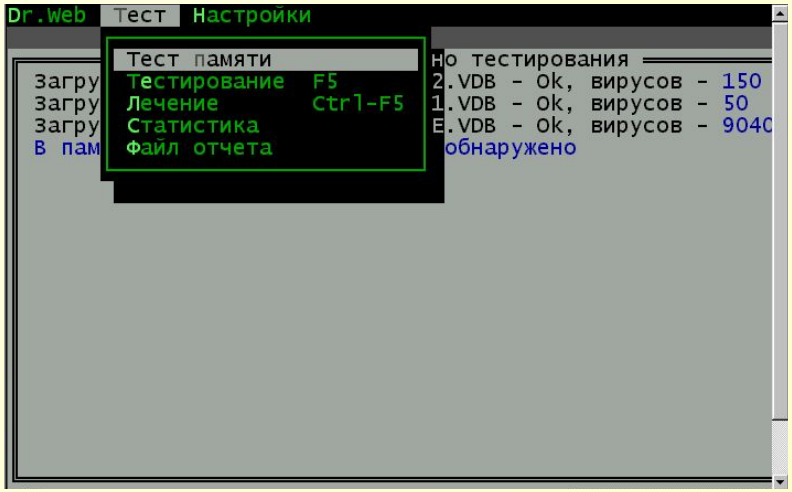


Компьютерные вирусы Антивирусные программы



Компьютерный вирус - специально написанная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью порчи файлов и каталогов, создания помех в работе.

Обязательным свойством компьютерного вируса является способность к размножению (самокопированию). Вирусы могут также незаметно для пользователя внедряться в исполняемые файлы, загрузочные секторы дисков и документы.

Активизация вируса может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программы, открытием документа и т. д.).

Виды (по степени воздействия):

- ✔***неопасные (не мешают работе, не уменьшают объём оперативной памяти и дисковой памяти)***
- ✔***опасные (могут привести к сбоям в работе)***
- ✔***очень опасные (приводят к потере программ, уничтожению данных)***

Признаки проявления вирусов:

- неправильная работа нормально работавших программ
- произвольный запуск на компьютере каких-либо программ;
- медленная работа компьютера
- неожиданное открытие и закрытие лотка CD/DVD дисковода;
- невозможность загрузки ОС
- частые «зависания» и сбои в работе компьютера;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке)
- исчезновение файлов и каталогов
- изменение размеров файлов
- неожиданное увеличение количества файлов на диске
- уменьшение размеров свободной ОП
- вывод на экран неожиданных сообщений и изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

Антивирусные программы

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.

Для поиска известных вирусов используются сигнатуры, т. е. некоторые постоянные последовательности двоичного кода, специфичные для этого конкретного вируса. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т. е. анализ последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

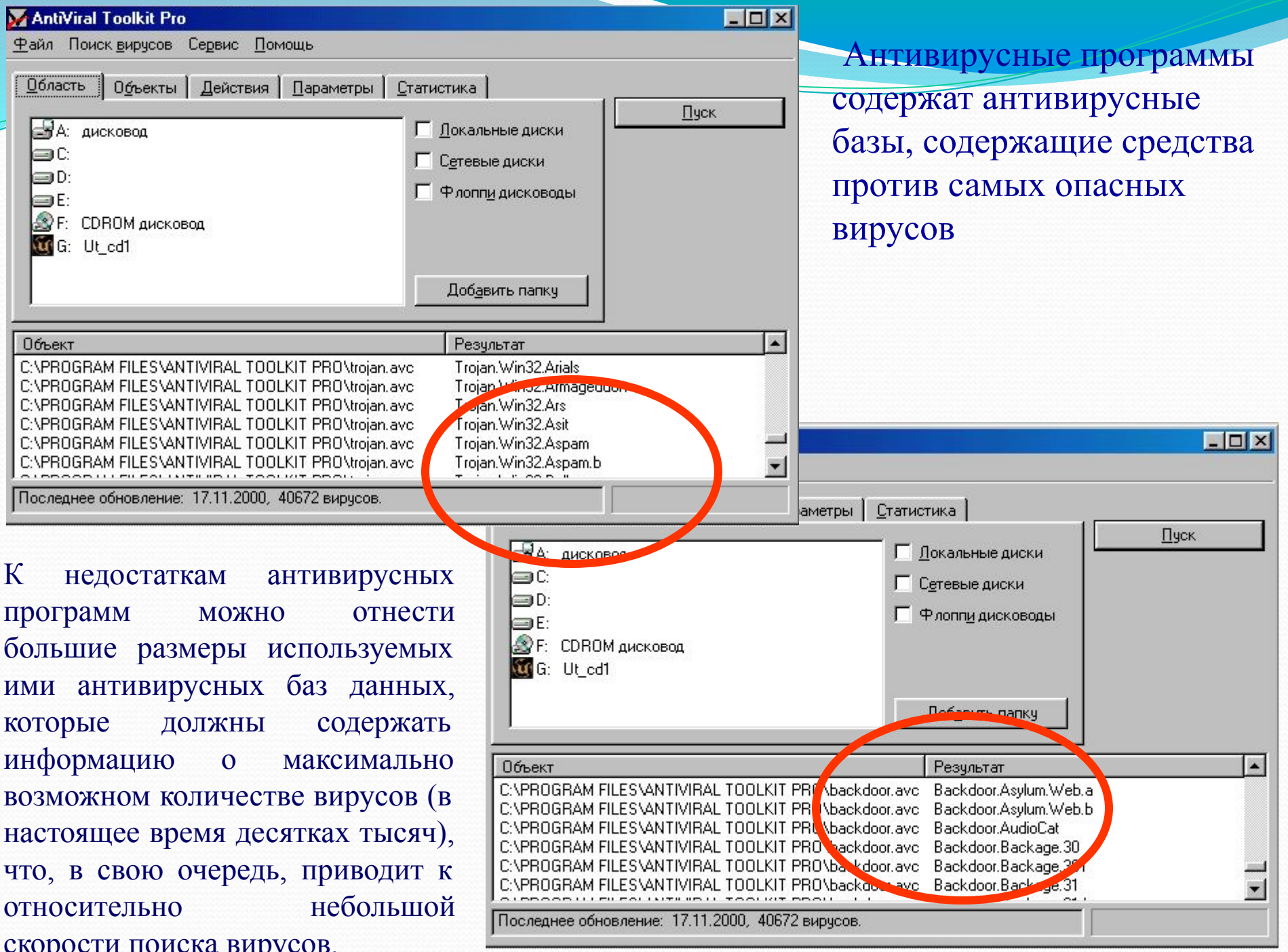
Антивирусный монитор

Антивирусный монитор запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия. Основная задача антивирусного монитора состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

Антивирусный сканер

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольный момент пользователем. Антивирусный сканер производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

Антивирусные программы содержат антивирусные базы, содержащие средства против самых опасных вирусов



К недостаткам антивирусных программ можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов (в настоящее время десятках тысяч), что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

Антивирусные программы:

- программы - доктора

(Norton AntiVirus, DoctorWeb, Aidstest

AntiViral ToolkitPro сканер...)

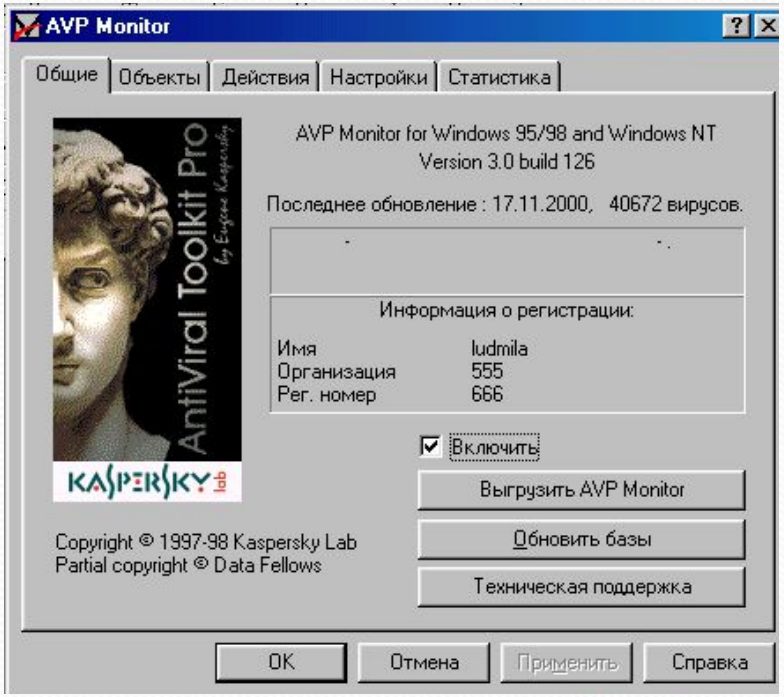
- программы - сторожа

(Anti AntiViral Toolkit Pro r...)

- программы - детекторы

- программы - ревизоры

Adinf (фирмы «Диалог-Наука»)



Доктора и вакцины могут обнаруживать и «лечить» заражённые файлы,
удаляя из файла тело вируса

Сторожа - небольшие резидентные программы, подающие сигнал тревоги, но лечить неспособны.

Детекторы производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы.

Ревизоры запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение (проверяется контрольная сумма файла).

Компьютерные вирусы

«Вирусы - черви» распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

К самым опасным вирусам относятся, например, ***«троянские»,*** т.к. они, маскируясь под полезную программу разрушают загрузочный сектор и файловую систему дисков.

«Вирусы-невидимки» или ***«стелс-вирусы»*** перехватывают обращения операционной системы к поражённым файлам и подставляют вместо своего тела незаражённые участки.

«Паразитические вирусы» изменяют содержимое файлов и секторов диска, легко обнаруживаются и уничтожаются.

Вирусы ***«резидентные»*** записывают в оперативную память свою часть. Они активны до выключения или перезагрузки компьютера.

Вирусы ***«нерезидентные»*** не заражают память компьютера, активны ограниченное время.

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска при включении или перезагрузке компьютера. После необходимых тестов установленного оборудования программа системной загрузки считывает первый физический сектор загрузочного диска (гибкого, жесткого, оптического или флэш-диска в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса. При инфицировании диска вирус в большинстве случаев переносит оригинальный загрузочный сектор в какой-либо другой сектор диска (например, в первый свободный).

Профилактическая защита от таких вирусов состоит **в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.** С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

Файловые вирусы

Файловые вирусы различными способами внедряются в исполнимые файлы (командные файлы *.bat, программы *.exe, системные файлы *.corn и *.sys, программные библиотеки *.dll и др.) и обычно активизируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т. е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

Лечение от файловых вирусов затруднено, так как даже после удаления зараженных файлов с дисков вирус остается в оперативной памяти и возможно повторное заражение файлов.

Профилактическая защита от файловых вирусов:

не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

Макро-вирусы. Наибольшее распространение получили макро-вирусы для программного пакета Microsoft Office (Word, Excel, PowerPoint и Access). Макро-вирусы фактически являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

При работе с документом пользователь выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и т. д. При этом приложение ищет и выполняет соответствующие стандартные макросы. Макро-вирусы содержат стандартные макросы, вызываются вместо них и заражают каждый открываемый или сохраняемый документ. Вредные действия макро-вирусов реализуются с помощью встроенных макросов (вставки текстов, запрета выполнения команд меню приложения и т. д.).

Макро-вирусы находятся в оперативной памяти и заражают документы, пока открыто приложение. Кроме того, макро-вирусы заражают шаблоны документов и поэтому активизируются уже при запуске зараженного приложения.

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Microsoft Office сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. **Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макро-вирусами, однако отключит и полезные макросы, содержащиеся в документе.**

Скрипт-вирусы

Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц. Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.
Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

«Вирусы - черви»

«Вирусы - черви» распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Для своего распространения сетевые черви используют разнообразные сервисы глобальных и локальных компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т. д.

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников. Рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

Сетевые черви кроме вредоносных действий, которыми обладают и классические компьютерные вирусы, могут выполнять шпионскую функцию троянских программ.

Троянские программы

Троянские программы осуществляют не санкционированные пользователем действия по сбору и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию. Троянские программы могут вызывать нарушение работоспособности компьютера или незаметно для пользователя использовать ресурсы компьютера в целях злоумышленника.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе.

Троянские программы данного типа могут быть использованы для обнаружения и передачи конфиденциальной информации.

(банковские реквизиты, пароли доступа к Интернету и др.) и отсылают ее по указанному в коде троянца электронному адресу или адресам.

Троянцы данного типа также сообщают информацию о зараженном компьютере (размер памяти и дискового пространства, версию операционной системы, IP-адрес и т. п.). Некоторые троянцы воруют регистрационную информацию к программному обеспечению.

Троянские программы часто изменяют записи системного реестра операционной системы, поэтому для их удаления необходимо в том числе восстановление системного реестра (например, с помощью программы CCleaner можно исправить ошибки системного реестра).

Куки

Куки (от англ. cookies — домашнее печенье) — небольшой текстовый файл, помещаемый Web-сервером на локальный компьютер пользователя. Файлы cookies могут храниться в оперативной памяти (сеансовые файлы cookies) или записываться на жесткий диск (постоянные файлы cookies). Файлы cookies не могут быть использованы для запуска программного кода (запуска программ) или для заражения компьютера вирусами.

Cookies применяются для сохранения данных, специфичных для данного пользователя. При вводе регистрационных данных файлы cookies помогают серверу упростить процесс сохранения персональных данных, связанных с текущим пользователем. Если пользователь Интернет-магазина ранее указывал адрес для доставки счетов или товара, вместо повторного ввода этих данных можно указать пароль, позволяющий автоматически заполнить соответствующие поля в форме заказа.

Браузеры позволяют включать и отключать использование файлов cookies, а также выполнять прием файлов cookies только после подтверждения со стороны пользователя. Для защиты от файлов **cookies** можно запустить браузер Internet Explorer, открыть меню *Свойства обозревателя/Конфиденциальность* и установить уровень конфиденциальности «Блокировать все cookies»

Спам

Спам — массово рассылаемая корреспонденция рекламного или иного характера, отправляемая людям, не выразившим желание ее получать. В первую очередь термин «спам» относится к рекламным электронным письмам.

Спам приходит потому, что электронный адрес получателя стал известен спамерам (рассыльщикам спама). Чаще всего владелец почтового ящика сам указывает электронный почтовый адрес при регистрации на каком-либо сайте и его обнаруживает специальный робот, «бродящий» по сайтам наподобие индексирующего робота поисковых систем.

«Нигерийские письма». Иногда спам используется для того, чтобы выманить деньги у получателя письма. Наиболее распространенный способ получил название «нигерийские письма», потому что большое количество таких писем приходило из Нигерии. Такое письмо содержит сообщение о том, что получатель письма может получить большую сумму денег, а отправитель может ему в этом помочь. Затем отправитель письма просит перевести ему немного денег под предлогом, например, оформления документов или открытия счета. Выманивание этой суммы и является целью мошенников.

Фишинг

Фишинг (от англ. fishing — рыбалка) — еще один способ мошенничества путем обмана пользователей. Он представляет собой попытку выманить у получателя письма данные, которые можно использовать для получения выгоды: номера его кредитных карточек или пароли доступа к системам онлайновых платежей. Такое письмо обычно маскируется под официальное сообщение от администрации банка. В нем говорится, что получатель должен подтвердить сведения о себе, иначе его счет будет заблокирован, и приводится адрес сайта (принадлежащего спамерам) с формой, которую надо заполнить. Среди данных, которые требуется сообщить, присутствуют и те, которые нужны мошенникам. Для того чтобы жертва не догадалась об обмане, оформление этого сайта имитирует оформление официального сайта банка.

Хакерские утилиты

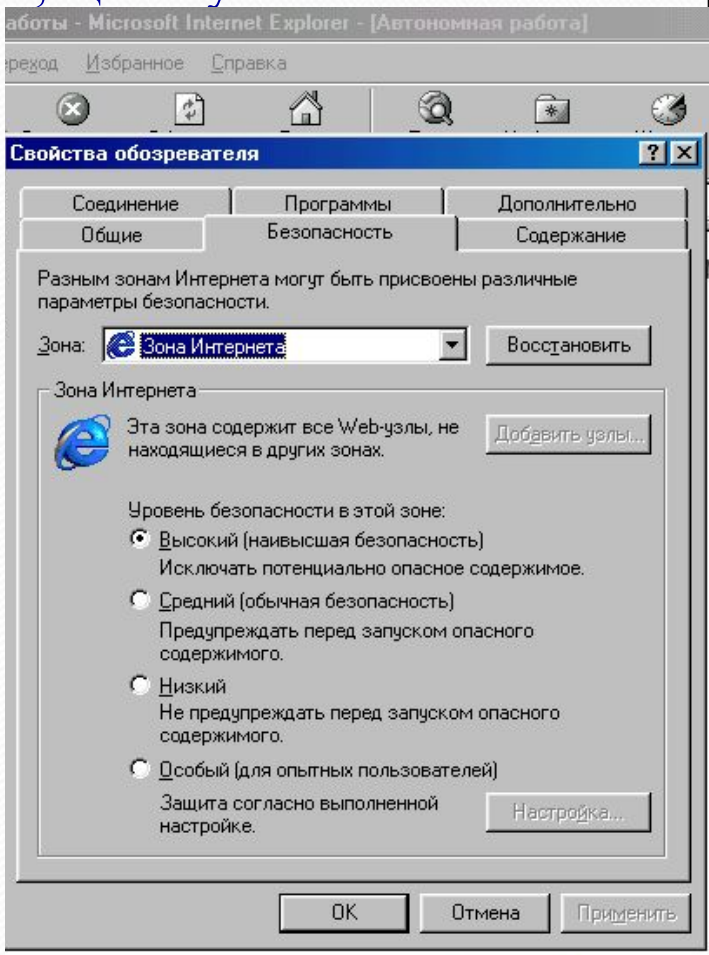
Сетевые атаки. Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них специфические запросы. Это приводит к отказу в обслуживании («зависанию» сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Меры предосторожности:

- периодически проверяйте на наличие вирусов жёсткие диски компьютера
- вовремя обновляйте антивирусные базы
- делайте архивные копии ценной информации
- не оставляйте в дисководе гибкую дискету во время загрузки и перезагрузки, чтобы не заразить компьютер загрузочными вирусами
- при работе на других компьютерах защищайте свои дискеты от записи
- добавьте в Автозагрузку антивирусную программу - сторож

- принимая электронную почту не вскрывайте вложения, если отправитель вам неизвестен

- подключаясь к Internet, настройте свой обозреватель, щёлкнув в Главном меню Internet Explorer команду ***Вид***, ***Свойства обозревателя*** выбрав высокий уровень безопасности



- Чужую дискету или флэшку, вставив в дисковод, сначала проверьте антивирусной пр