Компьютерные вирусы. Антивирусные программы.

Зайцева Ирина
Самарская область
ГБОУСОШ
с. Красноармейское

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Содержание:

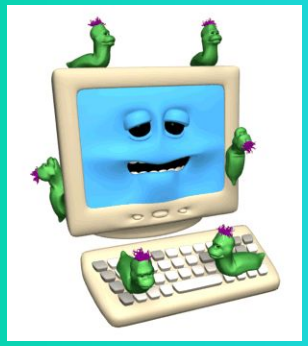
Компьютерные вирусы

Компьютерные вирусы – это одна из наиболее широко известных опасное для сетей. Подобно живым микроорганизмам, они распространяются, заражая здоровые программы. Заразив систему, они проникают в каждый исполняемый или объектный файл, размещенный на машине. Более того, некоторые вирусы заражают загрузочные сектора дисков, а это значит, что вирус проникнет и в машины, загружающиеся с зараженного диска.

История компьютерного вируса

Существует много разных версий относительно даты рождения первого компьютерного вируса. Однако большинство специалистов сходятся на мысли, что компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов". В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе за создание и распространение вирусов.

ann-testsite.ucoz.ua



Основные источники вирусов

- дискета, на которой находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Internet;
- жесткий диск, на который попал вирус в результате работы с зараженными программами;
- вирус, оставшийся в оперативной памяти после предшествующего

Вирусы действуют только программным путем. Они, как правило, присоединяются к файлу или проникают в тело файла. В этом случае говорят, что файл заражен вирусом. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно.

Ранние признаки заражения компьютера вирусом

- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д
- исчезновение файлов;
- форматирование жесткого диска;
- невозможность загрузки файлов или операционной системы.
- уменьшение объема свободной оперативной памяти;

Троянские Кони

Троянскими конями называются вирусы, прячущиеся в файлах данных (например, сжатых файлах или документах). Чтобы избежать обнаружения, некоторые разновидности троянских коней прячутся и в исполняемых файлах. Таким образом, эта программа может располагаться и в программных файлах, и в файлах библиотек, пришедших в сжатом виде. Однако зачастую троянские кони содержат только подпрограммы вируса. Возможно, самое лучшее определение троянских коней дал Дэн Эдварде — бывший хакер, занимающийся теперь разработкой антивирусного программного обеспечения для NSA (National Security Administration).

Одной из наиболее известных «троянских лошадок» стала программа Crackerjack. Как и все другие средства для взлома паролей, доступные в Internet, эта программа тестировала относительную мощность паролей, расположенных в выбранном файле. После своего запуска она выдавала список взломанных паролей и предлагала пользователю удалить этот файл. Первая версия программы не только взламывала пароли, но также и передавала их автору троянского коня. Crackerjack оказался достаточно полезным средством, в чем вы можете убедиться сами. Для этого достаточно загрузить программу из Internet.

ПОЛИМОРФНЫЕ ВИРУСЫ

Полиморфные вирусы — это вирусы, которые зашифровывают свое тело и благодаря этому могут избежать обнаружения путем проверки сигнатуры вируса. Прежде чем приступить к работе, такой вирус расшифровывает себя с помощью специальной процедуры расшифровки. Чтобы расшифровать тело вируса, процедура расшифровки захватывает управление машиной. После расшифровки управление компьютером передается расшифрованному вирусу. Первые шифрующиеся вирусы были неполиморфными. Поэтому антивирусные программы могли обнаружить вирус по сигнатуре, присущей процедуре расшифровки. Полиморфные вирусы обнаружить очень трудно. Дело в том, что они генерируют абсолютно новые процедуры расшифровки при каждом новом заражении. Благодаря этому сигнатура вируса изменяется от файла к файлу. Для изменения процедуры шифрования используется достаточно простой генератор машинного кода, называющийся генератором мутаций. Он использует генератор случайных чисел и достаточно простой алгоритм изменения сигнатуры вируса. С его помощью программист может превратить любой вирус в полиморфный. Для этого о должен изменить текст вируса так, чтобы перед каждым созданием своей копии он вызывал генератор мутаций.

Несмотря на то что полиморфные вирусы нельзя обнаружить с помощью обычных методов проверки (вроде сравнения строк кода), они все же детектируются специальными антивирусными программами. Итак, полиморфные вирусы можно обнаружить. Однако этот процесс занимает огромное количество времени, а на создание антивирусной программы уходит гораздо больше сил. Наиболее свежие обновления антивирусного программного обеспечения производят поиск процедур шифрования,, с помощью которой обнаруживают полиморфные вирусы.

Полиморфный вирус изменяет свою сигнатуру при создании очередной копии, от файла к файлу.

СТЕЛС-ВИРУСЫ

Стелс-вирусы — это вирусы, которые прячут изменения, созданные в зараженном файле. Для этого они отслеживают системные функции чтения файлов или секторов на носителях информации. Если происходит вызов такой функции, то вирус старается изменить полученные ею результаты: вместо настоящей информации вирус передает функции данные незараженного файла. Таким образом, антивирусная программа не может обнаружить никаких изменений в файле. Но, для того чтобы перехватывать системные вызовы, вирус должен находиться в памяти машины. Все достаточно хорошие антивирусные программы могут обнаружить подобные вирусы во время загрузки зараженной программы. Хорошим примером стелс-вируса является один из первых задокументированных вирусов DOS — Brain. Этот загрузочный вирус просматривал все дисковые системные операции ввода/вывода и перенаправлял вызов всякий раз, когда система пыталась считать зараженный загрузочный сектор. При этом система считывала информацию не с загрузочного сектора, а с того места, где вирус сохранил копию этого сектора. Стелс-вирусами также являются вирусы Number, Beast .Как правило, стелс-вирусы либо обладают невидимым размером, либо они невиди-мы для чтения. Такие вирусы помешают свое тело внутрь файла, вызывая тем самым увеличение его размера. Однако вирус изменяет информацию о раз-
мере файла так, чтобы пользователь не мог обнаружить его присутствия. Стелс-вирусы достаточно легко обнаружить. Большинство стандартных антивирусных программ «вылавливают» стелс-вирусы. Для этого достаточно запустить антивирусную программу до того, как вирус будет размещен в памяти машины. Надо запустить компьютер с чистой загрузочной дискеты, а затем выполнить антивирусную программу. Как уже говорилось, стелс-вирусы могут замаскироваться

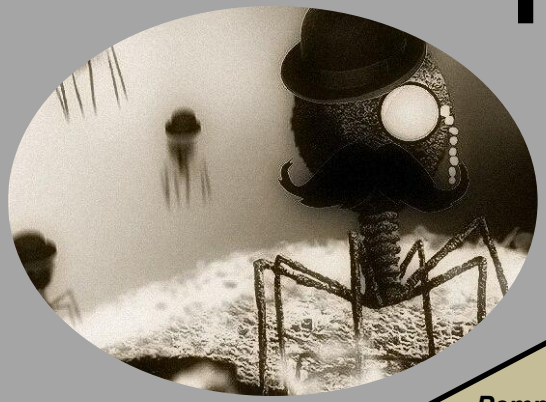
МЕДЛЕННЫЕ ВИРУСЫ

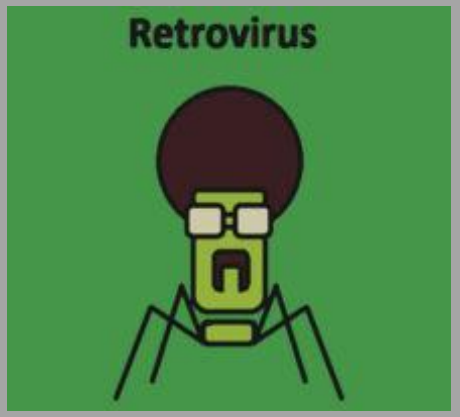
Медленные вирусы очень трудно обнаружить, так как они заражают только те файлы, которые изменяются или копируются операционной системой. Например, медленный вирус может производить заражение загрузочной записи дискеты при выполнении команд системы, изменяющих эту запись (например, FORMAT или SYS). Медленный вирус может заразить копию файла, не заразив при этом файл-источник. Одним из наиболее известных медленных вирусов является Darth_Vader, который заражает только COM-файлы и только во время их записи.

Обнаружение медленных вирусов — это достаточно сложный процесс. Хранитель целостности должен обнаружить новый файл и сообщить пользователю о том, что у этого файла нет значения контрольной суммы. Хранитель целостности — это антивирусная программа, наблюдающая за содержанием жестких дисков, а также за размером и контрольной суммой каждого из расположенных на них файлов. Если хранитель обнаружит изменения в содержании или размере, то он немедленно сообщит об этом пользователю. Однако сообщение будет выдано и в том случае, если пользователь сам создаст новый файл. Поэтому пользователь, скорее, укажет хранителю целостности вычислить новую контрольную сумму для нового (инфицированного) файла.

Наиболее удачным средством против медленных вирусов являются оболочки целостности. Оболочки целостности — это резидентные хранители целостности. Они постоянно находятся в памяти компьютера и наблюдают за созданием каждого нового файла, и у вируса не остается практически никаких шансов. Еще одним способом проверки целостности является создание ловушек. Здесь специальная антивирусная программа создает несколько COM- и EXE-файлов определенного содержания. Затем программа проверяет содержимое этих файлов. Если медленный вирус заразит их, то пользователь сразу же узнает об этом. Например, медленный вирус может наблюдать за программой копирования фай... Если DOS выполняет запрос на . копирование, то вирус п... копию файла.

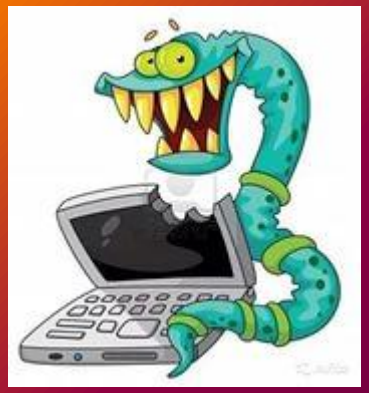
РЕТРО-ВИРУСЫ





Ретро-вирус — это вирус, который пытается обойти или помешать действиям антивирусных программ. Создание ретро-вируса является относительно несложной задачей. В конце концов, создатели вирусов обладают доступом ко всем антивирусным программам. Приобретая такую программу, они изучают ее работу, находят бреши в обороне и после этого создают вирус на основе обнаруженных просчетов. Большинство ретро-вирусов занимается поисками и удалением файлов с данными о сигнатурах вирусов. Таким образом, антивирусная программа, использовавшая этот файл, не может больше нормально функционировать. Более сложные ретровирусы занимаются поиском и удалением баз данных, содержащих информацию о целостности файлов. Удаление подобной базы производит на хранителя целостности такой же эффект, как уничтожение файлов с сигнатурами вирусов на антивирусную программу. Многие ретро-вирусы обнаруживают активизацию антивирусных программ, а затем прячутся от программы либо останавливают ее выполнение. Кроме того, они могут запустить процедуру разрушения до того, как антивирусная программа обнаружит их присутствие. Некоторые ретро-вирусы изменяют оболочку вычислений антивируса и таким образом влияют на выполнение антивирусных программ. Кроме того, существуют ретро-вирусы, использующие недостатки антивирусного программного обеспечения, чтобы замедлить его работу или свести на нет эффективность программы.

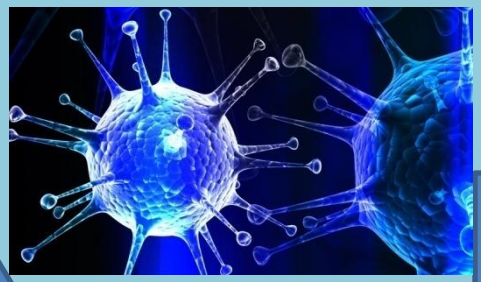
Вирус Черв



Червь Internet (известный также как червь Морриса) был самым первым вирусом, поразившим Internet. Этот вирус делал невозможной работу компьютера, создавая огромное количество своих копий в памяти компьютера. Так как червь старается остановить зараженный компьютер, создатель вируса должен наделить его способностями перемещаться с помощью сети от одной машины к другой. Удаленное воспроизведение необходимо, так как после остановки машины пользователь постарается вычистить все имеющиеся на жестком диске вирусы. Для своего распространения вирусам-червям не требуется изменять программы хоста. Для нормальной работы червям необходимы операционные системы, обеспечивающие возможность удаленного выполнения и позволяющие приходящим программам выполняться на компьютере. В 1988 году такими возможностями обладала только одна операционная система — Unix. До недавнего времени многие персональные компьютеры не могли быть заражены червем — этого не позволяют сделать ни DOS, ни Windows 95. Однако Windows NT уже обладает возможностями удаленного выполнения и поэтому может поддерживать работу вирусов-червей.Одним из самых распространенных вирусов в Internet является WINSTART. Свое название он получил от имени файла — winstart.bat, — в котором обычно и располагается тело вируса. Этот червь, как и многие остальные, копирует себя в памяти машины до тех пор, пока не будет выведена из строя операционная система. После этого компьютер автоматически зависает. Во время своего выполнения вирус параллельно занимается поиском следующей жертвы. Недостаток большинства стандартных средств аудита и хранителей целостности заключается в том, что они также могут стать жертвами вирусов.

ВООРУЖЕННЫЕ ВИРУСЫ

Вооруженные вирусы защищают себя с помощью специального кода, благодаря которому сильно усложняется отслеживание и дизассемблирование вируса. Вооруженные вирусы могут воспользоваться для защиты «пустышкой». Это — код, позволяющий увести разработчика антивирусных программ от настоящего кода вируса. Кроме того, вирус может включать в себя специальный фрагмент, указывающий на то, что вирус расположен в одном месте, хотя на самом деле его там не будет. Одним из наиболее известных вооруженных вирусов является Whale.



ВИРУСЫ-КОМПАНЬОНЫ

Свое название эти вирусы получили потому, что параллельно с заражаемым файлом они создают файл с таким же именем, но с другим расширением. Например, вирус-компаньон может сохранить свое тело в файле winword.com. Благодаря этому операционная система перед каждым запуском файла winword.exe будет запускать файл winword.com, который будет располагаться в памяти компьютера. Обычно вирусы-компаньоны генерируются вирусами-фагами.

СОСТАВНЫЕ ВИРУСЫ

Составные вирусы заражают как исполняемые файлы, так и загрузочные сектора дисков. Кроме того, они могут заражать загрузочные сектора дискет. Такое название они получили потому, что заражают компьютер различными путями. Если запустить инфицированную программу, вирус заразит загрузочную запись жесткого диска. При следующем включении машины вирус активизируется и будет заражать все запущенные программы. Одним из наиболее известных составных вирусов является One-Half, который обладает признаками стелс-вируса и полиморфного вируса.

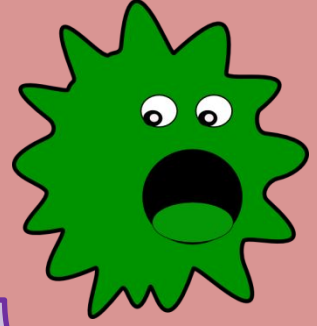
ВИРУСЫ-ФАГИ

Вирус-фаг — это программа, которая изменяет другие программы или базы данных. Компьютерные профессионалы называют эти вирусы фагами потому, что по своему действию они напоминают живые микроорганизмы. Обычно фаги замещают текст программы своим собственным кодом. Чаще всего они являются генераторами вирусов компаньонов. Фаги — это наиболее опасный вид вирусов. Дело в том, что они не только размножаются и заражают другие программы, но и стремятся уничтожить все зараженные программы.

ФАЙЛОВЫЕ ВИРУСЫ

•Файловым вирусом может быть троянский конь, вооруженный вирус, стелс-вирус и некоторые другие. Файловые вирусы опасны для данных, хранящихся на сервере, одноранговых сетей и, в какой-то степени, Internet. Далее приводятся три пути заражения сетевого сервера: Копирование (пользователем или администратором) зараженных файлов прямо на сервер. После этого вирус, расположившийся в файле, начнет заражать все остальные файлы.Выполнение файлового вируса на рабочей станции может заразить сеть. После своего запуска вирус сможет заразить любое приложение, хранимое на сервере. Если же вирус сумеет проникнуть в какой-либо файл, расположенный на сервере, то он сможет заразить и все машины в сети. Выполнение резидентного вируса на рабочей станции может вызвать заражение всей сети. После своего запуска резидентный вирус может получить информацию о передаваемых данных и скопировать себя на сервер, не обладая при этом прямым доступом к расположенной на сервере информации. Абсолютно не важно, как вирус попадет в сеть. Он может быть размещен на дискете, получен с сообщением электронной почты или загружен из Internet вместе с исполняемым файлом. Как только вирус попадает на компьютер, обладающий доступом к другим сетевым компьютерам, то он способен заразить все остальные машины. Заразив всего лишь одну машину в сети, вирус начнет свое «шествие» по всей сети и в конце концов попадет на сервер.
После заражения файлового сервера любой пользователь, запустивший зараженную программу, может заразить файлы на своем жестком диске или другие файлы, размещенные на том же сервере. Кроме того, администратор, зарегистрировавшийся в сети с правами суперпользователя, может обойти запреты на доступ к файлам и каталогам и заразить еще большее количество файлов. Серверы это очень удобное для вирусов место.

МАКРОВИРУСЫ



Как уже говорилось, макровирусы — это один из наиболее опасных типов компьютерных вирусов. В настоящее время они представляют собой наиболее быстро развивающуюся разновидность «компьютерных инфекций», способных перемещаться посредством Internet. Макровирусы представляют опасность не только для сетей, но и для автономных компьютеров, т. к. они не зависят от компьютерной платформы и от конкретной операционной системы. Более того, эти вирусы заражают не исполняемые файлы, а файлы с данными, которых гораздо больше.

Количество макровирусов растет с каждым днем. По официальным данным, в октябре 1996 года было зарегистрировано менее 100 макровирусов. В мае 1997 года их количество достигло 700. Как вы узнаете, макровирус — это небольшая программа, написанная на внутреннем языке программирования (иногда эти языки называют языками разработки сценариев или макроязыками) какого-то приложения. В качестве таких приложений обычно выступают текстовые или табличные процессоры, а также графические пакеты.

Обычно макровирусы распространяются путем создания копий в каждом новом документе. Таким образом макровирус может попадать на другие машины вместе с зараженными документами. Наиболее часто макровирусы удаляют файлы так, чтобы впоследствии их нельзя было восстановить. Макровирусы могут выполняться на любом типе компьютеров. Главное, чтобы на машине была нужная им программа обработки документов вместе со своим внутренним языком программирования.В настоящее время большинство известных макровирусов написано на Microsoft Word Basic или недавно появившемся Visual Basic for Application (VBA); WordBasic — это внутренний язык программирования текстового процессора Word for Windows (начиная с версии 6.0) и Word 6.0 for Macintosh. Так как при каждом использовании программы из пакета Microsoft Office выполняется и VBA, то написанные с его помощью макровирусы представляют для системы чрезвычайную опасность.

Другими словами, макровирус, созданный с помощью VBA, может заражать и таблицы Excel, и базы данных Access, и презентации PowerPoint.

Средства, помогающие предотвратить заражение вирусов

- резервное копирование информации (создание копий файлов и системных областей жестких дисков);
- избежание пользования случайными и неизвестными программами. Чаще всего вирусы распространяются вместе с компьютерными программами;
- перезагрузка компьютера перед началом работы, в частности, в случае, если за этим компьютером работали другие пользователи;
- ограничение доступа к информации, в частности физическая защита дискеты во время копирования файлов с нее.
- К программным средствам защиты относят разные антивирусные программы (антивирусы).
- Слайд 2

Антивирусная программа

Антивирусная программа-это программа специфического типа, созданная для обнаружения, опознания и последующего устранения вредоносных кодов, программ, зараженных файлов, спам-рассылок и прочих неприятностей. Помимо этого, антивирус способен препятствовать проникновению нежелательных кодов в операционную систему компьютера или мобильного устройства, а также лечить уже зараженные файлы, не допуская их удаления.

...ипы антивирусных программ:

- 1) **программы-детекторы**: *предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;*
- 2) **программы-лекари**: *предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;*
- 3) **программы-ревизоры**: *предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;*
- 4) **лекари-ревизоры**: *предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.*
- 5) **программы-фильтры**: *предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.*
- 6) **программы-вакцины**: *используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).*

Следует заметить, что выбор одного "наилучшего" антивируса крайне ошибочное решение. Рекомендуется использовать несколько разных антивирусных пакетов одновременно. Выбирая антивирусную программу следует обратить внимание на такой параметр, как количество распознающих сигнатур (последовательность символов, которые гарантированно распознают вирус). Второй параметр - наличие эвристического анализатора неизвестных вирусов, его присутствие очень полезно, но существенно замедляет время работы программы. На сегодняшний день существует большое количество разнообразных антивирусных программ. Рассмотрим коротко, распространенные в странах СНГ.

DRWEB

Один из лучших антивирусов с мощным алгоритмом нахождения вирусов. Полифаг, способный проверять файлы в архивах, документы Word и рабочие книги Excel, выявляет полиморфные вирусы, которые в последнее время, получают все большее распространение. Достаточно сказать, что эпидемию очень опасного вируса OneHalf остановил именно DrWeb. Эвристический анализатор DrWeb, исследуя программы на наличие фрагментов кода, характерных для вирусов, разрешает найти почти 90% неизвестных вирусов. При загрузке программы, в первую очередь DrWeb проверяет самого себя на целостность, после чего тестирует оперативную память. Программа может работать в диалоговом режи[illegible]т удобный настраиваемый интерфейс польз[illegible]я.

ADINF

Антивирус-ревизор диска ADINF (Avanced DiskINFoscope) разрешает находить и уничтожать, как существующие обычные, stealth- и полиморфные вирусы, так и совсем новые. Антивирус имеет в своем распоряжении лечащий блок ревизора ADINF - Adinf Cure Module - что может обезвредить до 97% всех вирусов. Эту цифру приводит "Диалогнаука", исходя из результатов тестирования, которое происходило на коллекциях вирусов двух признанных авторитетов в этой области - Д.Н.Лозинского и фирмы Dr.Solomon's (Великобритания).

ADINF загружается автоматически в случае включения компьютера и контролирует boot-сектор и файлы на диске (дата и время создания, длина, контрольная сумма), выводя сообщения про их изменения. Благодаря тому, что ADINF осуществляет дисковые операции в обход операционной системы, обращаясь к функциям BIOS, достигаются не только возможность выявления активных stealth-вірусів, но и высокая скорость проверки диска. Если найден boot-вирус, то ADINF просто восстановит предшествующий загрузочный сектор, который хранится в его таблице. Если вирус файловый, то здесь на помощь приходит лечащий блок Adinf Cure Module, который на основе отчета основного модуля о зараженных файлах сравнивает новые параметры файлов с предыдущими, хранящиеся в специальных таблицах. При выявлении расхождений ADINF восстанавливает предыдущее состояние файла, а не уничтожает тело вируса, как это делают полифаги.

AVP

Антивирус AVP (AntiVirus Program) относится к полифагам, в процессе работы проверяет оперативную память, файлы, в том числе архивные, на гибких, локальных, сетевых и CD-ROM дисках, а также системные структуры данных, такие как загрузочный сектор, таблицу разделов и т.д. Программа имеет эвристический анализатор, который, по утверждениям разработчиков антивируса способен находить почти 80% всех вирусов. Программа AVP является 32-разрядным приложением для работы в среде операционных систем Windows 98, NT и 2000, имеет удобный интерфейс, а также одну из самых больших в мире антивирусную базу. Базы антивирусов к AVP обновляются приблизительно один раз в неделю и их можно получить с Internet. Эта программа осуществляет поиск и изъятие разно[illegible]их в том числе:

полиморфных, или самошифрующихся вирусов;

стелс-вирусов, или вирусов-невидимок;

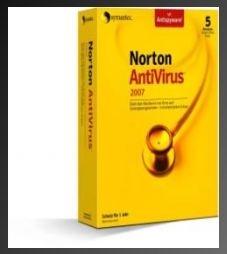
новых вирусов для Windows;

макровирусов, заражающих документы Word и таблицы Excel.

Кроме того, программа AVP осуществляет контроль файловых операций в системе в фоновом режиме, выявляет вирус до момента реального заражения системы, а также определяет неизвестные вирусы с помощью эвристического модуля.

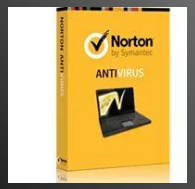
Eset NOD32

NOD32 обеспечивает надежную, современную защиту от угроз, которым подвергается ваш ПК. Вирусы, черви, трояны и другие неприятности теперь не смогут причинить никакого вреда информации, ценной для вас. Усовершенствованные методы обнаружения, которые используются этой программой, обеспечивает защиту даже против будущих, циальных угроз, которыми являются сетевые черви и вирусы.



Symantec Norton Anti-Virus

Разработанная компанией Symantec программа Norton AntiVirus является наиболее популярным антивирусным средством в мире. Эта программа автоматически удаляет вирусы, интернет-червей и троянские компоненты, не создавая помех работе пользователя. Norton AntiVirus позволяет противостоять угрозам самых современных spyware- и adware-программ и блокирует работу таких программ еще до того момента, как пользователь перенаправляется на другой сайт.



Panda Antivirus

Panda Antivirus является самым простым и интуитивно понятным в использовании решением безопасности для домашнего ПК. После установки программы пользователь может забыть о вирусах, программах-шпионах, руткитах, хакерах, онлайн-мошенниках и больше не беспокоиться о сохранности конфиденциальной информации.

Panda Antivirus имеет простые настройки, легкий и понятный интерфейс, автоматическое обновление (после установки сразу будет искать обновления), осуществляет контроль на уровне TCP/IP. Panda Antivirus является достаточно надежным антивирусом подойдет в первую очередь для домашнего пользования

Конец