

Персональный компьютер. Шаг за шагом

ПЯТЫЙ ТОМ

© А.В. ФРОЛОВ, Г.В. ФРОЛОВ, 1996

Осторожно: компьютерные вирусы

Все, что вы должны знать о компьютерных вирусах

АННОТАЦИЯ

В этой книге вы найдете практически всю информацию, необходимую для квалифицированной борьбы с компьютерными вирусами в среде операционных систем MS-DOS, Microsoft Windows, IBM OS/2, Novell NetWare. Мы постарались обобщить громадный опыт, накопленный сотрудниками АО “ДиалогНаука” в этой области, делая упор на практические рекомендации.

Книга предназначена как для начинающих пользователей персональных компьютеров, так и для тех, кто уже обладает достаточным опытом работы. В ней вы найдете методики борьбы с вирусами, описание приемов проведения антивирусной профилактики с помощью специально предназначенных для этого средств, описание наиболее распространенных вирусов и многое другое.

ВВЕДЕНИЕ

Персональные компьютеры получают все большее и большее распространение, внедряясь во все новые сферы человеческой деятельности. Этому способствует постоянное и устойчивое снижение стоимости компьютеров, появление удобных в работе программ с дружественным интерфейсом, всемерное развитие глобальных компьютерных сетей, которые предоставляют доступ к неограниченным запасам информации.

Надежность аппаратного обеспечения компьютерных систем стала достаточно высока, поэтому теперь человек передоверяет компьютерам решение многих жизненно важных задач. Пользователям современных компьютеров незнакомы проблемы, связанные со сбоями дисковых систем, занимающих целые комнаты в вычислительных центрах или другого столь же “компактного” оборудования ЭВМ серии ЕС.

Однако существует и другая опасность, подстерегающая даже высоконадежные резервированные компьютерные системы. Это так называемые компьютерные вирусы, которые есть ни что иное, как программы, специально предназначенные для того, чтобы нарушать нормальную работу компьютерных систем.

Коварность вирусов не знает границ, а вред, который они могут принести в крупной компьютерной системе, поражает воображение. Не зря во многих странах создание и распространение вирусов преследуется по закону как уголовное преступление. Представьте себе, какие могут быть последствия потери информации в крупном банке, медицинском учреждении или нарушения работы военной компьютерной системы. А между тем подобные случаи уже возникали в ряде стран.

Важное свойство компьютерных вирусов - способность “размножаться”, бесконтрольно распространяясь в компьютерной среде. Переносчики компьютерных вирусов - это дискеты, локальные и глобальные сети, а в последнее время и компакт-диски, особенно с нелегальным программным обеспечением. Вирусная эпидемия может в считанные дни или часы охватить крупный вычислительный центр (а то и

несколько центров), полностью парализовав его работу. При этом издержки могут исчисляться миллионами и десятками миллионов долларов.

Что же можно противопоставить этой более чем реальной угрозе?

Как и в борьбе с обычными вирусами, в борьбе с компьютерными вирусами применяется профилактика, диагностика и лечение.

Каждый из нас с детства знает, что перед едой нужно мыть руки. Эта нехитрая профилактическая мера может спасти вас от такого, например, заболевания, как холера. Когда вы работаете с персональным компьютером, также необходимо принимать ряд несложных профилактических мер, направленных на предупреждение вирусного вторжения. Тщательно соблюдая элементарные меры безопасности, можно сберечь немало времени и денег.

К сожалению, беспечность пользователей и системных администраторов часто приводит к плачевному исходу, когда для восстановления информации на диске компьютера приходится прибегать к услугам высококвалифицированных (и, соответственно, высокооплачиваемых) специалистов. Но и они не всемогущи - если вирус расписал весь диск нулевыми байтами, то что тут можно сделать?

Для диагностики (обнаружения вирусов) обычно используют специальные программы, которые пользователи часто называют антивирусами (хотя есть более тонкая классификация).

Регулярная диагностика имеет большое значение, так как чем раньше обнаружен вирус, тем больше вероятность успеха лечения (все, как и с обычными вирусами). Дело в том, что компьютерные вирусы делают свое черное дело не сразу, а с некоторой задержкой, необходимой на распространение. Чем раньше будет обнаружен вирус, тем легче его обезвредить.

Что касается лечения компьютера, зараженного вирусами, то оно не всегда возможно. Лечение также выполняется при помощи специальных антивирусных программ, однако успех этой операции зависит от многих факторов. В частности, он зависит от того, насколько далеко зашли вредоносные действия вирусов.

Применение антивирусных программ не всегда эффективно. Вы должны уметь ими пользоваться, как и обычными лекарствами. Переписав у знакомого или из электронной доски объявлений пару антивирусных программ, многие ограничиваются их ежедневным запуском. Успокаивая себя отсутствием предупреждающих сообщений о появлении вирусов, такие пользователи бывают неприятно поражены, когда взявшийся “из неоткуда” вирус уничтожает на диске что-нибудь очень нужное.

Причина этого заключается в том, что в мире ежедневно создаются новые вирусы. Некоторые из этих вирусов используют изощренные приемы маскировки, затрудняющие их обнаружение. Поэтому старые версии антивирусных программ оказываются бессильными.

Одна из основных причин распространения вирусов - программы, полученные случайным образом или загруженные из электронных досок объявлений. Риск получения

вируса вместе с лицензионным дистрибутивом программного обеспечения намного меньше, хотя он все-таки есть. Поэтому новое программное обеспечение имеет смысл проверять самыми последними версиями антивирусных средств.

Нам хотелось бы также избавить вас от излишней “вирусофобии”. Иногда вирусам приписывают фантастические возможности. Услышав о гипнотизирующих и зомбирующих вирусах, бедный пользователь в страхе шарахается от компьютера или надевает резиновые перчатки, вставляя дискету. Не надо этого делать! Во-первых, перчатки все равно не помогут, а во-вторых... впрочем, может быть завтра такой вирус появится и на самом деле.

В этой книге мы рассмотрим различные аспекты, связанные с компьютерными вирусами. Мы уделим большое внимание механизму распространения вирусов различных типов, так как знание этого механизма - половина успеха в борьбе с вирусами.

Вы узнаете о том, как правильно выполнять антивирусную профилактику отдельных компьютеров и локальных сетей компьютеров, научитесь пользоваться самыми современными антивирусными средствами, причем не только программными, но и аппаратными.

Так как раннее обнаружение вирусов увеличивает шансы на успех, мы приведем соответствующие методики и рекомендации, в частности, мы расскажем о том, как обнаружить вирусы-невидимки, маскирующие свое присутствие в системе.

Для тех, кто пользуется антивирусными средствами АО “ДиалогНаука”, есть возможность получения самых последних версий антивирусных программ через модем. Поэтому мы расскажем о том, как пользоваться электронной доской BBS, которая создана специально для подписчиков антивирусного комплекта “ДиалогНаука”.

Отдельная глава книги посвящена борьбе с вирусами в локальных сетях персональных компьютеров, получивших повсеместное распространение. Плохо защищенная локальная сеть представляет собой как раз ту “питательную среду”, в которой компьютерные вирусы размножаются особенно быстро и где они могут нанести наибольший вред. Мы приведем конкретные рекомендации для различных сетевых операционных систем, которые предназначены для пользователей сети и системных администраторов.

Для тех из вас, кто интересуется проблемой вирусов глубже, мы расскажем о наиболее слабых местах операционных систем, которые служат объектом нападения вирусов. Мы также расскажем о некоторых приемах восстановления информации после вирусных атак, которые могут быть рекомендованы только для квалифицированных пользователей или системных программистов.

БЛАГОДАРНОСТИ

Мы приносим свою искреннюю благодарность всем, кто помогал нам писать эту книгу и надеемся, что она станет серьезной поддержкой пользователям компьютеров в борьбе с вирусами.

В первую очередь мы признательны сотрудникам АО “ДиалогНаука”, в тесном контакте с которыми создавалась книга:

- *генеральному директору АО “Диалог Наука” Антимонову Сергею Григорьевичу - за идею создания книги о том, как бороться с вирусами;*
- *руководителю антивирусного отдела АО “ДиалогНаука” Лященко Юрию Павловичу - за редактирование книги и многочисленные советы по ее содержанию;*
- *Лозинскому Дмитрию Николаевичу - за популярное изложение жизненного цикла вируса и за предоставленные описания вирусов;*
- *Данилову Игорю Анатольевичу - за многочисленные консультации по вопросам функционирования современных вирусов, а так же за предоставленные описания вирусов;*
- *Ладыгину Виталию Сергеевичу - за подробное описание вируса Win.CyberTech и рассказ о вирусах, маскирующихся на уровне контроллера жесткого диска;*
- *Фомину Юрию Николаевичу - за рассказ о принципах аппаратной защиты от вирусов;*
- *Мостовому Дмитрию Юрьевичу и Зуеву Денису Григорьевичу - за консультации по использованию программы ADInf и лечащего модуля*

Кроме того, мы благодарим Абрамкина Алексея Михайловича за прекрасные рисунки, которые он сделал для нашей книги, Фролову Ольгу Викторовну, ставшую одной из первых читателей, корректора Кустова В. С. и сотрудников издательского отдела АО “Диалог-МИФИ” Голубева О. А., Дмитриеву Н. В., Виноградову Е. К. и Кузьминову О. А.

КАК СВЯЗАТЬСЯ С АВТОРАМИ

Вы можете передать нам свои замечания и предложения по содержанию этой и других наших книг через электронную почту:

Сеть	Наш адрес	Сеть	Наш адрес
Relcom	frolov@glas.apc.org	CompuServe	>internet: frolov@glas.apc.org
GlasNet	frolov@glas.apc.org	UUCP	cdp!glas!frolov

Internet frolov@glas.apc.org

Если электронная почта вам недоступна, присылайте ваши отзывы в АО “Диалог-МИФИ” по адресу:

✉ Адрес: инд. 115409, Москва, ул. Москворечье, 31, корп. 2,

☎ Тел. (095) 324-43-77

По вопросам антивирусной защиты обращайтесь непосредственно в АО “ДиалогНаука” по адресу:

✉ Адрес: инд. 117967, Москва ГСП-1, ул. Вавилова 40, ВЦ РАН, офис 103а.

☎ Тел. (095) 135-6253, 137-0150, 938-2970

FidoNet: 2:5020/69

E-mail:

antivir@dials.msk.su - поставки и обслуживание

bob@dials.msk.su - по вопросам связи со станцией BBS

loz@dials.msk.su - передача новых вирусов

id@dials.msk.su - передача новых вирусов

Сервер WWW: <http://www.dials.ccas.ru>

Сервер FTP: <ftp:dials.ccas.ru>

Приносим свои извинения за то, что не можем ответить на каждое письмо. Мы также не занимаемся рассылкой дискет и исходных текстов к нашим книгам. По этому вопросу обращайтесь непосредственно в издательство “Диалог-МИФИ”.

1 ЧТО ТАКОЕ КОМПЬЮТЕРНЫЕ ВИРУСЫ И КАК ОНИ РАБОТАЮТ

Что же такое компьютерный вирус? Представьте себе работу мелкого клерка и его рабочее место. На столе стоит телефон, копировальный аппарат и другие канцелярские принадлежности. Рядом стоит шкаф с папками и документами.

В папках содержатся инструкции, которые клерк должен выполнять. Каждый день он берет очередную папку и начинает с ней работать. Инструкции в папках могут содержать алгоритмы расчета зарплаты, указания по обработке поступающей документации и т. д.

Клерк монотонно выполняет свою работу день за днем и вдруг недоброжелатель вкладывает ему в папку еще один лист с дополнительными инструкциями. В них клерку

предлагается скопировать этот лист на копировальной машине и вложить его в следующую папку. Со временем такой лист распространится по папкам и в конце концов, его копия будет находиться в каждой папке.

Кроме инструкций, отвечающих за распространение, дополнительный лист может содержать другие инструкции. Например, в них может указываться, что клерк должен уничтожить папку, взятую наугад из шкафа с документами или перевести некоторую сумму на определенный счет в банке.

Теперь представьте, что работу клерка выполняет центральный процессор. Шкаф с папками документов - это жесткий диск компьютера. Сами папки - это файлы программ, записанные на диске. В этом случае дополнительный лист, подброшенный кем-то в одну из папок, достаточно точно соответствует компьютерному вирусу.

Наиболее общее определение компьютерного вируса можно дать как самораспространяющийся в информационной среде компьютеров программный код. Он может внедряться в выполнимые файлы программ, распространяться через загрузочные секторы дискет и жестких дисков.

Существуют достаточно оригинальные вирусы, распространяющиеся через файлы документов, подготовленных в текстовом процессоре Microsoft Word for Windows и электронной таблице Microsoft Excel for Windows. Кроме перечисленных вирусов существуют и другие, например, вирусы, заражающие командные файлы - файлы с расширением BAT. Прогресс в мире вирусов не стоит на месте, десятки, если не сотни скучающих программистов делают свое черное дело и на свет появляются все более страшные монстры.

К сожалению, действие большинства вирусов не ограничивается размножением и распространением. Они могут выполнять относительно безопасные или напротив, разрушительные действия.

Внешне действия вирусов могут выражаться в том, что периодически, например, по достижении определенного времени, вирус активизируется и выполняет какие-либо операции. Вирусы могут выводить на экран посторонние надписи, "осыпать" символы, уже отображенные на экране, перезагружать компьютер, замедлять работу компьютера, исполнять на встроенном динамике компьютера всевозможные мелодии, удалять файлы и каталоги, стирать выбранные случайным образом секторы жестких и гибких дисков.

Существуют вирусы, делающие "полезную" работу. Например, один из вирусов, поражающих файлы программ, одновременно сжимает их, уменьшая размер. Благодаря этому на диске компьютера становится больше свободного места. Такой вирус выполняет функции широко распространенной программы DIET, но делает это автоматически, не спрашивая на то разрешения у пользователя.

Можно придумать много другой полезной работы, которая под силу вирусам. Однако мы не станем отнимать хлеб у писателей вирусов, скажем только, что даже "полезные" вирусы могут быть очень опасны.

Некоторые эффекты, вызываемые вирусами, например, внезапная перезагрузка компьютера или зависание, часто воспринимаются как аппаратная неисправность компьютера. На это и рассчитывают писатели вирусов. Действительно, причиной этому может послужить аппаратная неисправность компьютера.

Однако не торопитесь вызывать технических специалистов или самостоятельно открывать компьютер. Сначала выполните полную диагностику компьютера, воспользовавшись всеми антивирусными средствами, которыми вы располагаете.

В настоящее время насчитываются тысячи различных вирусов и их модификаций. Мы будем классифицировать их по способу распространения. Подавляющее большинство вирусов можно разделить на две большие группы:

- *вирусы, внедряющиеся в файлы,*
- *вирусы, заражающие загрузочные секторы жестких и гибких дисков.*

Существует много вирусов, которые одновременно можно включить в обе эти группы. Такие вирусы являются комбинированными. Они могут распространяться, заражая файлы и загрузочные секторы дисков.

Резидентные и нерезидентные вирусы

Операционная система MS-DOS является однозадачной. В любой момент времени может работать только одна программа. Когда пользователь закончит с ней работать, программа выгружается из оперативной памяти и пользователь может запустить новую программу. Естественно, это не всегда удобно. Например, если вы пишете в текстовом редакторе финансовый отчет, вам может потребоваться калькулятор. Очень неудобно для запуска калькулятора каждый раз завершать текстовый редактор, а потом запускать его снова.

Чтобы как-то смягчить неудобства, вызванные однозадачностью MS-DOS, был создан механизм резидентных программ. При запуске резидентной программы она сразу возвращает управление операционной системе, но оставляет в оперативной памяти резидентный модуль.

Даже если потом запускаются другие программы этот модуль остается в памяти. Затем, когда пользователь нажимает определенную комбинацию клавиш или при другом условии резидентная программа может активизироваться и выполнить некоторую работу.

В качестве примера можно привести программы резидентных калькуляторов. Они могут быть загружены из командной строки операционной системы или из файла AUTOEXEC.BAT и остаются резидентными в памяти. Если пользователь нажимает определенную комбинацию клавиш, на экране появляется панель калькулятора. Пользователь может выполнить любые вычисления и вернуться в свою программу. Резидентные программы могут выполнять и другие действия. Например, они могут выполнять функции будильника.

Механизм резидентных программ, предусмотренный для сугубо мирных целей, был использован авторами вирусов. Обычные, нерезидентные вирусы получают управление и становятся активными только во время запуска зараженной программы. После запуска вирусом настоящей программы, он окончательно теряет управление, до тех пор, пока зараженная программа опять не будет запущена. За это небольшое время вирус должен заразить другие программы и выполнить заложенные в него автором дополнительные функции.

Резидентный вирус, получив управление, оставляет в оперативной памяти компьютера небольшой модуль, который остается активным вплоть до перезагрузки компьютера. Резидентный модуль вируса может использоваться для решения самых различных задач.

Обычно он применяется для заражения новых программ. Резидентный модуль отслеживает запуск или открытие файлов программ, проверяет, не были ли они уже заражены, и если нет, то заражает их.

Интересно, что если на компьютере, зараженном резидентным вирусом, поражающим выполнимые файлы при их открытии, запустить антивирусную программу, которая не может определить этот вирус, то по окончании проверки окажутся зараженными все проверяемые выполнимые файлы.

Некоторые разновидности вирусов, называемые стелс-вирусами, используют резидентный модуль, чтобы замаскировать свое присутствие. Они могут перехватывать обращения к файловой системе и скрывать изменение длины зараженных файлов. Более подробно о стелс-вирусах вы можете прочитать в разделе “Маскировка вирусов”.

И, конечно, резидентный модуль используется для создания всевозможных спецэффектов. Здесь все зависит от фантазии и знаний, которыми обладает автор вируса. Те, кто попроще, могут испортить данные, записываемые на диск, замедлить работу компьютера. Более изысканные в программировании и менее злобные авторы создают всевозможные видеоэффекты и звуковые композиции.

Любая резидентная программа, и в том числе резидентные модули вирусов, уменьшают объем доступной оперативной памяти. Это изменение можно заметить с помощью команды MEM, входящей в состав операционной системы MS-DOS.

Команда MEM отображает информацию об использовании оперативной памяти компьютера. С помощью нее можно узнать, сколько оперативной памяти установлено на компьютере, сколько памяти занято и сколько свободно для использования:

Memory Type	Total	Used	Free
Conventional	640K	204K	436K
Upper	0K	0K	0K
Reserved	384K	384K	0K
Extended (XMS)	15 360K	14 336K	1 024K
Total memory	16 384K	14 924K	1 460K

Total under 1 MB 640K 204K 436K

Total Expanded (EMS) 1 024K (1 048 576 bytes)
Free Expanded (EMS) 1 024K (1 048 576 bytes)

Largest executable program size 436K (446 256 bytes)
Largest free upper memory block 0K (0 bytes)
MS-DOS is resident in the high memory area.

Команда MEM позволяет подробно исследовать резидентные модули, загруженные в память. Для этого при вызове команды ей надо указать дополнительные параметры. Подробное описание команды MEM изложено в десятом томе “Библиотеки системного программиста” - “Компьютер IBM PC/AT, MS-DOS и Windows. Вопросы и ответы”.
‡Здесь мы приведем только основные сведения.

MEM [/CLASSIFY | /DEBUG] [/PAGE]

Если указать дополнительный параметр /CLASSIFY (или /C), то будет представлена информация по каждому резидентному модулю, размещенному в оперативной памяти.

Вместо параметра /CLASSIFY можно указать параметр /DEBUG (или /D). В этом случае будет собрана дополнительная информация о загруженных драйверах.

Команда MEM выводит на экран очень много информации. Так как экран компьютера может одновременно отображать ограниченное количество строк, то выполняется свертка изображения. Дополнительный параметр /PAGE (или /P) позволяет после заполнения очередного экрана выдерживать паузу.

Вирусы могут оставлять в оперативной памяти резидентные модули. Фактически все загрузочные вирусы и большинство файловых вирусов являются резидентными.

Резидентные модули вируса могут затруднить его обнаружение и удаление. Чтобы не дать вирусу шанс получить управление и оставить резидентный модуль в памяти, рекомендуется для проверки компьютера выполнять загрузку с чистой системной дискеты.

Вирусы в загрузочных секторах дисков

Сразу после включения питания компьютера начинает работать процедура проверки POST (Power On Self Test). В ходе проверки определяется конфигурация компьютера, проверяется работоспособность основных его подсистем. Процедура POST записана в микросхеме постоянного запоминающего устройства, расположенного на системной плате компьютера.

Если компьютер имеет энергонезависимую память (CMOS-память), из нее считываются значения текущих даты и времени, конфигурация дисковой подсистемы. Заметим, что CMOS-память установлена практически на всех компьютерах. Она отсутствовала только на первых моделях компьютеров IBM PC и IBM PC/XT.

Затем процедура POST проверяет, вставлена ли дискета в дисковод A:. Если дискета вставлена, тогда дальнейшая загрузка операционной системы происходит с дискеты. Если дискета не вставлена, загрузка выполняется с жесткого диска.

Практически все современные системные платы и версии программы Setup позволяют изменить порядок загрузки компьютера. Например, вы можете указать, что компьютер сразу должен загружаться с жесткого диска и только в случае отсутствия жесткого диска загрузка будет выполняться с дискеты.

Последовательность загрузки операционной системы MS-DOS с дискеты и с жесткого диска немного различаются. Мы опишем оба случая, так как это важно для понимания механизма распространения загрузочных вирусов.

Загрузка компьютера с системной дискеты

Если загрузка компьютера происходит с дискеты, то процедура POST считывает с нее загрузочную запись (Boot Record) в оперативную память. Эта запись всегда расположена в самом первом секторе дискеты и представляет собой маленькую программу. Кроме программы загрузочную запись содержит структуру данных, определяющую формат дискеты и т. д. Затем процедура POST передает управление загрузочной записи.

Получив управление, загрузочная запись приступает непосредственно к загрузке операционной системы. Она считывает с дискеты и загружает в оперативную память файлы IO.SYS и MSDOS.SYS. Для операционных систем, совместимых с MS-DOS эти имена могут отличаться. Например в операционной системе IBM PC-DOS загружаются файлы IBMIOS.COM IBMSYS.COM.

Затем, если на дискете записан файл конфигурации CONFIG.SYS, анализируется его содержимое и загружаются указанные в нем драйверы.

После этого с дискеты считывается командный процессор COMMAND.COM и управление передается ему. Командный процессор завершает загрузку операционной системы и выполняет команды, записанные в файле AUTOEXEC.BAT.

После выполнения команд, записанных в файле AUTOEXEC.BAT, командный процессор отображает на экране системное приглашение и ожидает ввода команд:

A: \>

Файлы CONFIG.SYS и AUTOEXEC.BAT могут отсутствовать. Если отсутствует файл AUTOEXEC.BAT, тогда после окончания загрузки операционной системы командный процессор предлагает ввести текущую дату и время:

Current date is Fri 15-04-1996

Enter new date (mm-dd-yy):

Current time is 2:28:33.47p

Enter new time:

Если вы не желаете изменять дату и время, нажмите два раза клавишу <Enter>. В этом случае дата и время останутся без изменения, и на экране появится системное приглашение MS-DOS. Вы можете создать на системной дискете пустой файл AUTOEXEC.BAT, тогда дата и время запрашиваться не будут и после загрузки операционной системы на экране сразу появится системное приглашение.

Загрузка компьютера с несистемной дискеты

Мы рассмотрели вариант загрузки компьютера с системной дискеты. Возможен вариант, при котором пользователь случайно или по ошибке попытается загрузить компьютер с несистемной дискеты. На такой дискете отсутствуют файлы операционной системы IO.SYS, MSDOS.SYS и COMMAND.COM. Тем не менее, загрузочная запись присутствует даже на несистемной дискете.

Когда процедура POST считывает и передает управление загрузочной записи, она определяет, что дискета несистемная (так как на ней отсутствуют файлы операционной системы) и отображает на экране соответствующее сообщение:

Non-System disk or disk error

Replace and press any key when ready

В некоторых случаях сообщение может иметь другой внешний вид:

This disk is not bootable

If you wish to make it bootable,
run the DOS program SYS after the
system has been loaded

Please insert a DOS diskette into
the drive and strike any key...

Эти сообщения означают, что дискета не содержит необходимых файлов и загрузить операционную систему с нее невозможно. Вам предлагается вставить в компьютер системную дискету и перезагрузить компьютер.

В разделе “Создание системной дискеты” мы расскажем, как из несистемной дискеты сделать системную.

|| Загрузочный вирус может распространяться как через системные, так и через несистемные дискеты

Загрузка компьютера с жесткого диска

Загрузка компьютера с жесткого диска происходит несколько сложнее. Процедура POST считывает с жесткого диска главную загрузочную запись (MBR - Master Boot Record) и записывает ее в оперативную память компьютера. Главная загрузочная запись содержит программу первоначальной загрузки и таблицу разделов, в которой описаны все разделы жесткого диска.

Формирование главной загрузочной записи и таблицы разделов происходит во время первоначальной установки компьютера и разделения его жестких дисков на разделы и логические диски. Обычно эту операцию делают один раз, используя для этого команду FDISK операционной системы MS-DOS.

Главная загрузочная запись хранится в самом первом секторе жесткого диска. Поэтому процедура POST всегда знает, где она расположена.

Затем управление передается только что прочитанной с диска программе первоначальной загрузки. Она анализирует содержимое таблицы разделов, выбирает активный раздел и считывает загрузочную запись активного раздела (Boot Record). Загрузочная запись активного раздела аналогична загрузочной записи системной дискеты и выполняет те же самые функции. Она считывает в оперативную память файлы IO.SYS и MSDOS.SYS, анализирует файл конфигурации CONFIG.SYS, записанный на диске активного раздела, и загружает указанные в нем драйверы. После этого управление передается командному процессору COMMAND.COM. Командный процессор завершает загрузку операционной системы, а затем выполняет команды, записанные в файле AUTOEXEC.BAT.

Как работает загрузочный вирус

При заражении дискеты или жесткого диска компьютера загрузочным вирусом, последний заменяет загрузочную запись или главную загрузочную запись. Настоящая загрузочная запись или главная загрузочная запись обычно не пропадает (некоторые вирусы не сохраняют исходной загрузочной записи). Вирус копирует их в один из свободных секторов (рис. 1.1).

Таким образом, вирус получает управление сразу после завершения процедуры POST. Затем он, как правило, действует по стандартному алгоритму. Вирус копирует себя в конец оперативной памяти, уменьшая при этом объем свободной оперативной памяти. После этого он перехватывает несколько функций BIOS, так что обращение к ним передает управление вирусу. В конце вирус загружает в оперативную память компьютера настоящий загрузочный сектор и передает ему управление. Далее компьютер загружается как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов.

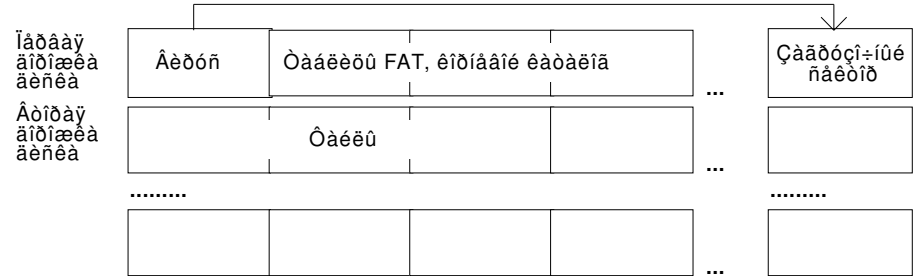


Рис. 1.1. Загрузочный вирус

Обычно загрузочный вирус заражает компьютер, когда пользователь загружает компьютер с дискеты, на которой уже есть вирус (вне зависимости от того системная эта дискета или нет). Чаще всего это происходит случайно. Вы работаете с дискетой и оставляете ее в дисковом A: компьютера. Если теперь вы перезагрузите компьютер или произойдет сбой работы компьютера из-за скачка питания, то загрузка компьютера начинается с зараженной дискеты и управление получает вирус. Он сразу заражает жесткий диск компьютера, устанавливает себя резидентным в памяти. Затем вирус загружает компьютер обычным образом. Если дискета загрузочная, то произойдет загрузка операционной системы, в противном случае на экране появляется предложение вставить в дисковод A: системную дискету и перезагрузить компьютер.

Теперь даже после перезагрузки компьютера с жесткого диска путем выключения питания удалить вирус нельзя, так как он уже записан на жестком диске. Сразу после включения питания компьютера вирус опять получит управление и разместит себя резидентно в памяти.

Дальнейшее распространение зависит от особенностей вируса. Обычно применяется простая схема. Если вы вставите в дисковод дискету, не зараженную вирусом, и обратитесь к ней, например, чтобы считать названия записанных на ней файлов, вирус получает сигнал, что дискета вставлена в дисковод. Вирус считывает загрузочную запись с дискеты и записывает ее в какой-либо другой сектор дискеты. Вместо оригинальной загрузочной записи записывается код вируса.

Некоторые вирусы, например Joshi, формируют на дискете дополнительную дорожку. Информация с этой дорожки не может быть считана и записана обычными средствами операционной системы. Вирус может использовать эту дорожку для хранения настоящего загрузочного сектора и некоторых своих модулей. Надо заметить, что использование дополнительных дорожек не является изобретением писателей вирусов. Эта методика применяется многими системами защиты от копирования.

Интересный эффект получается, если дискета или диск последовательно заражены несколькими загрузочными вирусами. В зависимости от того, какие секторы эти вирусы используют для хранения настоящего загрузочного сектора, возможны два случая.

В первом случае, когда вирусы используют различные секторы, они будут работать вместе. Сначала получает управление вирус, заразивший дискету последним. Он выполняет свою работу и загружает второй вирус, который заразил дискету раньше. В принципе такая цепочка вирусов может быть достаточно длинной. Последний вирус, который получит таким образом управление, в конце концов загрузит настоящий загрузочный сектор.

Обычно перед заражением диска (или дискеты), загрузочные вирусы проверяют, был ли он заражен ранее. Поэтому повторное заражение одним вирусом не происходит. Если же после заражения диска одним вирусом, его заразит другой загрузочный вирус, то первый вирус посчитает, что он не заражал диск раньше и заразит его еще раз. В результате может потеряться исходная загрузочная запись и компьютер зависнет во время загрузки.

Во втором случае вирусы, заразившие дискету, хранят настоящий загрузочный сектор в одном и том же месте. Когда второй вирус заражает дискету, он записывает код первого вируса в сектор, где первый вирус хранит настоящую загрузочную запись. В результате исходная загрузочная запись оказывается безвозвратно утерянной, а компьютер зависает: второй вирус будет снова и снова считывать и запускать свой вирусный код.

Вирус Ball

Первый раз мы столкнулись с вирусами много лет назад, еще будучи студентами московского инженерно физического института. В то время персональные компьютеры еще только начали появляться и были большой редкостью. Наша кафедра снимала несколько часов машинного времени в неделю в одном научном институте.

И вот в один прекрасный день на экране компьютера появился небольшой шарик. Он перемещался по экрану, отражаясь от его границ и некоторых символов. Первое время мы были в ужасной панике, думая что испортили дорогостоящий компьютер IBM PC/XT и все его программное обеспечение.

После перезагрузки шарик исчезал и мы надеялись, что дефект пропадет сам собой. Только через несколько дней мы решили сказать об этом местным инженерам. Они прореагировали очень спокойно, сообщив нам, что это компьютерный вирус Ping Pong, живущий на их компьютерах очень давно.

Для борьбы с вирусом использовали специальную антивирусную программу SCAN фирмы McAfee. Она легко находила вирус на дискетах и жестких дисках компьютеров, а затем удаляла его. После такой процедуры вирус долгое время не появлялся и некоторое время мы жили спокойно.

Однако кроме нас машинное время снимали много других организаций и каждый приходил работать со своими дискетами, поэтому вирус кочевал с дискеты на дискету. Вылечить его было практически невозможно, так как очень сложно было заставить всех пользователей проверить все свои дискеты.

Впоследствии выяснилось, что вирус Ping Pong, он же вирус Ball, распространялся через загрузочные секторы дискет и дисков. Оригинальный загрузочный сектор записывается на свободное место. Соответствующий сектор помечается как испорченный (Bad cluster). Испорченный кластер несколько уменьшал доступный размер дисков и дискет, но мы списывали это на их низкое качество.

Вирус Stoned

Второй вирус, с которым мы столкнулись, также оказался загрузочным. Антивирусные программы распознавали его как вирус Stoned. Он получил это название из-за того, что во время загрузки операционной системы на экране иногда появляется надпись "Your PC is now Stoned!". Мы немного остановимся на этом вирусе, так как он имеет очень много модификаций. Насчитывается большое количество вирусов, для которых он послужил прототипом.

Вирус достаточно легко опознается визуально. На дискетах он записывает себя на место загрузочной записи, а на жестких дисках - на место главной загрузочной записи. Если вы просмотрите соответствующие секторы в любом редакторе, например Norton Disk Editor, вы увидите надписи "Your PC is now Stoned!" и "LEGALISE MARIJUANA!". Как пользоваться программой Norton Disk Editor, вы узнаете из шестой главы нашей книги.

Когда вирус Stoned появился в первый раз, мы изучали язык ассемблера и особенности архитектуры персональных компьютеров, совместимых с IBM PC. Поэтому мы полностью дизассемблировали код вируса и подробно его изучили.

На дискетах исходная загрузочная запись копируется в третий сектор на первой стороне нулевой дорожки. Для дискет с объемом 360 Кбайт этот сектор приходится на последний сектор корневого каталога.

При заражении жесткого диска исходная главная загрузочная запись копируется в другое место. Она размещается в седьмом секторе на нулевой стороне нулевой дорожки. Этот сектор обычно не используется и остается свободным.

Некоторые загрузочные вирусы, не использующие методы маскировки (которые будут описаны ниже) могут быть легко обнаружены просмотром загрузочного сектора. Как выглядит загрузочная запись дискеты, созданной средствами операционной системы MS-DOS версии 5.0, в редакторе Disk Editor из пакета Norton Utilities вы можете посмотреть на рисунке 1.2.

[illegible]

Рис. 1.2. Загрузочная запись

Загрузочная запись на ваших дискахетах и жестких дисках может отличаться от приведенной нами. Это зависит как от версии операционной системы, используемой при форматировании диска, так и от некоторых других параметров.

Если вирус заразит загрузочную запись, он, естественно, изменит ее. Во многих случаях такое изменение заметно невооруженным взглядом. На рисунке 1.3 мы привели внешний вид загрузочного сектора дискеты, зараженной вирусом Form.

[]		Disk Editor																							
Object	Edit	Link	View	Info	Tools	Help																			
Sector 0																									
00000000:	EB	57	90	49	42	4D	20	20	-	33	2E	32	00	02	02	01	00	wPIBM 3.2.	0000						
00000010:	02	70	00	A0	05	F9	03	00	-	09	00	02	00	00	00	00	00	Op.a	0000						
00000020:	00	00	00	00	00	00	00	00	-	00	00	00	00	00	00	00	0F		0000						
00000030:	00	00	00	00	01	00	FA	33	-	C0	8E	D0	BC	00	7C	16	01		0000						
00000040:	FE	00	7C	00	00	C9	00	1A	-	00	87	E9	00	F0	08	47	00		0000						
00000050:	00	07	47	00	00	01	00	80	-	01	FA	33	C0	8E	D0	BC	FE		0000						
00000060:	7B	FB	1E	56	50	07	B8	C0	-	07	8E	D8	3C	F6	26	83	2E		0000						
00000070:	13	04	02	26	A1	13	04	B1	-	06	D3	E0	8E	C0	33	FF	B9		0000						
00000080:	FF	00	FC	F3	A5	C7	06	41	-	00	A5	00	8C	06	43	00	BB		0000						
00000090:	FE	01	B8	01	02	8B	0E	51	-	00	8B	16	53	00	CD	13	72		0000						
000000A0:	FE	FF	2E	41	00	0E	1F	E8	-	2B	00	E8	45	00	BD	4C	00		0000						
000000B0:	BE	45	00	BF	46	03	E8	B8	-	00	B4	04	CD	1A	80	FA	18		0000						
00000180:	44	02	FA	26	89	3F	26	8C	-	4F	02	FB	C3	BE	F9	03	BF		0000						
00000190:	03	00	C3	F7	B9	3C	00	FC	-	F3	A4	1E	F6	BF	F9	03	B9		0000						
000001A0:	FF	00	F3	A5	C7	05	55	AA	-	C3	8B	13	11	00	B1	04	D3		0000						
000001B0:	E3	A1	16	00	F6	26	10	00	-	02	C7	FE	C0	A3	03	00	8B		0000						
000001C0:	1E	13	00	2B	D8	8A	0E	0D	-	00	FE	C9	D3	BE	89	1E	05		0000						
000001D0:	00	C3	B9	02	00	BF	08	00	-	BE	0F	00	BB	F9	03	32	F6		0000						
000001E0:	B8	02	02	9C	FF	1E	45	00	-	72	73	F7	00	FF	75	06	06		0000						
000001F0:	81	08	F7	0F	EB	2B	46	47	-	3B	3E	05	00	73	5F	55	AA		0000						
Boot Record																		Sector 0							
Drive B:																		Offset 211, hex D3							

Рис. 1.3. Вирус Form в загрузочной записи

К сожалению, не все загрузочные вирусы можно так легко распознать. Активные загрузочные вирусы, использующие различные механизмы маскировки, могут обманывать Disk Editor. Например, такие вирусы могут перехватывать обращение Disk Editor к первому сектору жестких дисков и дискет, подменяя этот сектор копией оригинального первого сектора (копия первого сектора создается вирусом в момент заражения диска). В этом случае изменение загрузочного сектора не будет заметно.

Перед тем как использовать Disk Editor, загрузите MS-DOS с чистой системной дискеты. Программа Disk Editor также должна быть записана на дискете. В этом случае вирус не сможет задействовать свои механизмы маскировки.

Вирусы, внедряющиеся в файлы

Самую большую группу составляют вирусы, внедряющиеся в файлы. Они могут заражать практически любые файлы, содержащие выполнимый код. В первую очередь это файлы программ, имеющие расширения COM и EXE. Но не только они подвергаются нападению вирусов. Файлы оверлеев (расширения имен файлов OVL, OVI, OVR и др.), драйверов (SYS) также могут быть инфицированы.

Существует три большие группы файлов, которые непосредственно может запускать пользователь, вводя их имя в системном приглашении операционной системы MS-DOS. К ним относятся выполнимые файлы в формате COM и EXE, а также командные файлы, имеющие расширение BAT.

Выполнимые файлы в формате COM и EXE в корне отличаются от командных файлов с расширением BAT. В отличие от последних, они состоят из команд центрального процессора, то есть содержат машинные инструкции. Вместе с командами

процессора в выполнимых файлах могут размещаться данные: тексты сообщений, числовые константы и т. д. Чтобы создать выполнимый файл, используют специальные программы-трансляторы и редакторы связей.

Файлы в форматах COM и EXE отличаются в основном только своим форматом. Выполнимый файл COM состоит из одних инструкций процессора и данных. Размер COM файла обычно не превышает 65536 байт. Естественно это накладывает большие ограничения на программы в этом формате.

Когда вы запускаете программу в формате COM, операционная система считывает файл программы с жесткого диска или дискеты и размещает его в оперативной памяти, выбирая для этого свободный участок. Затем операционная система передает управление на самую первую команду загруженной программы. После окончания работы программы она возвращает управление операционной системе.

Файлы в формате EXE имеют значительно более сложную структуру, чем файлы COM. За счет этого они могут иметь больший размер, превышающий 65536 байт.

Кроме процессорных команд и данных, файлы в формате EXE содержат специальный заголовок, расположенный в самом начале файла. Заголовок EXE-файлов имеет сложный формат. На наш взгляд, его точный формат представляет интерес в основном для авторов вирусов. Поэтому мы приведем здесь только самые общие сведения.

Первое поле заголовка содержит сигнатуру EXE-файла - два символа MZ. Вы можете просмотреть любой EXE-файл в текстовом редакторе. Два первых символа всегда будут MZ. Некоторые выполнимые файлы могут иметь другую сигнатуру - ZM. Они также распознаются операционной системой как файлы в формате EXE.

Затем в заголовке файла следует таблица настройки. Когда пользователь запускает EXE-файл, операционная система загружает его в оперативную память, а затем настраивает его в соответствии с таблицей настройки. Только после этого управление передается на первую команду программы, адрес которой также записан в заголовке файла. Подробно формат заголовка EXE-файла описан в 18 томе из серии книг “Библиотека системного программиста”.

Командные BAT-файлы - это обычные текстовые файлы, состоящие из команд операционной системы. Для создания такого файла достаточно иметь любой текстовый редактор, который может сохранять файлы в обычном текстовом формате. В качестве примера можно привести текстовый редактор Notepad, входящий в состав операционной системы Windows.

Кроме команд операционной системы и вызовов других программ, командный файл может содержать строки комментариев. Такие строки обозначаются командой REM и полностью игнорируются. Вы можете воспользоваться строками комментариев, чтобы добавить текстовое описание к командному файлу или чтобы временно запретить выполнение отдельных команд такого файла:

REM Подключаем драйверы локальной сети

```
lsl.com
ne2000.com
ipxodi.com
netx /c=c:\net\net.cfg
REM login - команда временно отключена -
```

Когда вы запускаете командный файл, операционная система считывает его строка за строкой и выполняет прочитанные команды (рис. 1.4).

Оі÷èà âõîäà (îäðåäü êîìàíäîâ òäîäàèì)

Ëñîîâîóé òàéé îäîäàèì

Рис. 1.4. Програм ма до зараж ения

Заражая файл, вирусы тем или иным способом записывают свой код внутрь выполняемого файла и изменяют его таким образом, чтобы после запуска файла управление получил код вируса (рис. 1.5). Вирус может записать свой код в конец, начало или середину файла. Вирус также может разделить свой код на несколько блоков и разместить их в разных местах зараженной программы.

Далее вирус отрабатывает свои задачи: заражает другие файлы, устанавливает в памяти собственные резидентные модули и выполняет другие функции. Затем вирус, как правило, передает управление зараженной программе и далее она исполняется как обычно.

[illegible]

Обычно изменения в зараженных файлах видны невооруженным глазом в любом редакторе, в который можно загрузить выполнимый файл для просмотра. Кроме того заметно увеличение длины зараженного файла. Некоторые вирусы, находясь в резидентной памяти, могут маскироваться. В этом случае изменения в зараженном файле будут незаметны.

Text	View:	D:\...!\collaps\mouse.com	Col	0		22,431 Bytes	0%										
00000	E9	30	3C	00	00	00	EB	39	EB	43	00	00	00	FF	6C	0= <...596C...	
00010	00	00	00	00	00	00	00	00	00	49	4E	4E	7F	6C	047 24 FF 6C	PING\$ \$!	
00020	88	0B	A0	00	CE	0B	EE	00	0E	0C	A0	00	BE	0C	CE	0C	00<>+&@%#?~&
00030	DE	0C	AE	09	4E	47	00	00	00	00	00	00	00	00	00	00	I&PING.....
0575F	00	0A	24	20	4D	6F	75	73	65	20	64	72	69	76	65	72	J\$ Mouse driver
0576F	20	63	61	6E	20	6E	6F	74	20	62	65	20	72	65	6D	6F	\$ can not be remo
0577F	76	65	64	20	77	68	69	6C	65	20	57	69	6E	64	6F	77	ved while Window
0578F	73	20	69	73	20	72	75	6E	6E	69	6E	67	21	00	0A	24	s is running!J\$

Вы также можете увидеть изменения в самом выполняемом файле. Заметно, что изменены несколько первых байт файла (в них записана команда перехода на код вируса). В конце зараженного файла появились новые данные - это код самого вируса.

[illegible]

Рис. 1.7. Дамп файла MOUSE.COM, зараженного вирусом OneHalf

Вирусы-спутники

Как известно, в операционной системе MS-DOS существуют три типа файлов, которые пользователь может запустить на выполнение. Это командные или пакетные файлы. Командные файлы состоят из команд операционной системы и имеют расширение имени файла BAT.

В одном каталоге могут одновременно находиться несколько выполнимых файлов, имеющих одинаковое имя, но разное расширение имени. Например, в каталоге DOS записаны файлы MSD.COM и MSD.EXE. Вы можете создать в этом же каталоге командный файл MSD.BAT.

Когда вы желаете выполнить программу и вводите ее имя в системном приглашении MS-DOS, вы обычно не указываете расширение файла. Какой же файл в этом случае будет выполнен?

Оказывается, в этом случае операционная система MS-DOS будет выполнять файл, имеющий расширение COM. Если в текущем каталоге или в каталогах, указанных в переменной среды PATH, существуют только файлы с расширением EXE и BAT, то выполняться будет файл с расширением EXE.

Когда вирус-спутник заражает файл, имеющий расширение EXE или BAT, он создает в этом же каталоге еще один файл, имеющий такое же имя и расширение COM. Вирус записывает себя в этот COM-файл.

В качестве иллюстрации сказанного мы приводим содержимое каталога C:\PROGRAM. Первоначально в нем был записан один файл программы расчета CALC.EXE. После заражения этого файла вирусом-спутником в каталоге C:\PROGRAM появился файл CALC.COM:

C:\PROGRAM>DIR

Volume in drive C is LIBRARY

Volume Serial Number is 1F64-394F

Directory of C:\PROGRAM

```
.      <DIR>    26.11.95 18:55
..     <DIR>    26.11.95 18:55
CALC   COM     1 754 30.09.93 6:20
CALC   EXE     29 390 30.09.93 6:20
      2 file(s)    31 144 bytes
      2 dir(s)    26 599 424 bytes free
```

Если, запуская зараженную программу CALC.EXE, вы наберете в системном приглашении ее имя без расширения, то будет запущен вирус-спутник, файл которого имеет расширение COM:

C:\PROGRAM>CALC

Получив управление, вирус может выполнять различные действия: заражать другие файлы, устанавливать резидентный модуль, и т. д. Затем вирус может запустить саму зараженную программу, имеющую расширение EXE.

В отличие от других файловых вирусов, вирусы-спутники обычно никак не изменяют зараженные программы. Поэтому для лечения зараженных файлов достаточно просто удалить файлы вируса, имеющие расширение COM.

Для маскировки вирусы-спутники обычно устанавливают для файла вируса атрибут “Скрытый”. В этом случае команда DIR не отобразит имя файла вируса.

C:\PROGRAM>DIR

Volume in drive C is LIBRARY

Volume Serial Number is 1F64-394F

Directory of C:\PROGRAM

```
.      <DIR>    26.11.95 18:55
..     <DIR>    26.11.95 18:55
CALC   EXE     29 390 30.09.93 6:20
      1 file(s)    29 390 bytes
      2 dir(s)    26 599 424 bytes free
```

Однако такая маскировка очень слаба. Достаточно указать команде DIR параметр /A и она покажет список всех файлов в текущем каталоге, включая скрытые и системные файлы.

Вирус CloneWar

Под таинственным названием CloneWar скрывается целая группа вирусов-спутников. Во избежании путаницы их различают по длине файла вируса-спутника. На время написания книги были известны 5 вариантов вируса CloneWar длиной 228, 246, 261, 546 и 923 байт. Механизм их распространения полностью соответствует описанной нами технологии. Вирус выполняет поиск в текущем каталоге выполнимых файлов с расширением EXE. Затем он создает файл с таким же именем, но с расширением COM и записывает себя в него.

Когда пользователь вводит после системного приглашения имя зараженной программы без расширения, то запускается файл с расширением COM, который содержит вирус. Он заражает другие EXE файлы, а затем запускает зараженную программу.

Самая короткая из известных версий вируса CloneWar имеет длину 228 байт. Версия 246 вируса CloneWar содержит внутри себя небольшой стих:

Beyond
The rim of the star-light
My love
Is wand'ring in star-flight
I know
He'll find in star-clustered reaches
Love
Strange love a star woman teaches.
I know
His journey ends never
His star trek
Will go on forever.
But tell him
While he wanders his starry sea
Remember, remember me.

Самая большая версия вируса, имеющая длину 923 байта, проверяет значение системного таймера и в некоторых случаях исполняет через динамик компьютера небольшую мелодию. Затем код вируса закидывается, вызывая зависание компьютера.

Со временем идея вируса-спутника получила дальнейшее развитие. Кто-то из писателей вирусов резонно заметил, что любой выполнимый файл можно переименовать, а затем создать файл с таким же именем, но содержащий код вируса. Когда пользователь запускает свою программу, на самом деле запускается программа-вирус. Она заражает другие программы, а затем загружает в оперативную память и исполняет настоящую программу пользователя.

Простейшие вирусы-спутники используют всего несколько функций операционной системы - поиск файла с заданным именем в текущем каталоге, переименование файла и создание нового файла. Подобные средства работы с файлами существуют фактически во всех системах программирования. Поэтому написать подобный вирус может практически любой начинающий программист, в распоряжении которого есть система разработки программ, которая может создавать выполнимые файлы.

Вирус Carbuncle

Вирус Carbuncle также представляет собой вирус-спутник, но работает не так, как вирус CloneWar.

При запуске вируса Carbuncle создает в текущем каталоге файл CARBUNCL.COM. Для маскировки этому файлу присваивается атрибут скрытый. Затем вирус ищет в текущем каталоге выполнимые файлы. Если вирус найдет в каталоге файл с расширением

EXE, то он изменяет его расширение на CRP и создает пакетный файл с таким же именем. Этот файл получает расширение BAT. В него вирус записывает несколько команд MS-DOS, позволяющих запустить файл вируса CARBUNCL.COM и саму зараженную программу. Ниже мы привели пример такого файла для зараженной программы PROGRAM.EXE.

```
@ECHO OFF
CARBUNCL
RENAME PROGRAM.CRP PROGRAM.EXE
PROGRAM.EXE
RENAME PROGRAM.EXE PROGRAM.CRP
CARBUNCL
```

Если пользователь решит запустить зараженную программу и введет в системном приглашении имя программы без указания расширения, то операционная система просмотрит весь каталог в поисках файла с таким именем. Так как файл с расширением EXE она не обнаружит, то будет выполнен файл с расширением BAT.

Чтобы замаскировать исполнение нескольких команд пакетного файла, команда @ECHO OFF отключает вывод на экран исполняемых команд пакетного файла.

Следующая строка пакетного файла, созданного вирусом, запускает сам вирус CARBUNCL.COM. Затем зараженному файлу возвращается его настоящее расширение EXE и выполняется его запуск. После того как программа отработает, ее расширение опять заменяется на CRP. В конце снова запускается файл вируса CARBUNCL.COM.

Так как после заражения программы файл с расширением EXE уже не существует, то если при запуске программы указать ее полное имя с расширением, операционная система не сможет найти этот файл и на экране появится предупреждающее сообщение:

Bad command or file name

Вирус CloneWag ведет себя в этой ситуации значительно лучше. В этом случае сразу будет запущена настоящая программа. Вирус просто не получит управления.

Вирус Carbuncle занимается не только распространением своих копий. В некоторых случаях он может уничтожить зараженный файл. При запуске файл вируса проверяет значение системного таймера и если оно меньше или равно 16, то вирус записывает свой код в файл первого зараженного файла в текущем каталоге.

Внутри файла вируса содержатся следующие текстовые строки:

```
@ECHO OFF
CARBUNCL
RENAME
PC CARBUNCLE: Crypt Newsletter 14
```

Вирусы в COM и EXE файлах

Формат выполнимых COM-файлов достаточно прост, чтобы любой программист средней квалификации, знакомый с языком ассемблера, смог написать вирус.

Основная идея таких вирусов заключается в том, что вирус записывает свой код внутрь заражаемого файла. В самом простом случае вирус дописывает свой код в конец файла. Затем вирус считывает и сохраняет несколько первых байт заражаемого файла. На их место записывается команда передачи управления коду вируса.

После запуска зараженной программы управление передается первой команде, замененной вирусом на команду перехода. Поэтому управление сразу передается вирусу.

Получив управление, вирус выполняет действия, определенные его автором. Обычно в этот момент вирус заражает другие выполнимые файлы, устанавливает собственные резидентные модули, совершает другие противоправные действия.

Окончив эту работу, вирус восстанавливает первые команды зараженного файла и передает на них управление. Теперь начинает работать настоящая программа в ее неизменном виде.

Вирусы, заражающие выполнимые файлы, могут записывать свой код не только в конец файла. В качестве примера можно привести вирус Anarchy.2048 и Megadeth. Когда Megadeth заражает выполнимый COM-файл программы, он считывает и сохраняет в конце файла первые байты кода программы. Затем вирус записывает свой код в начало файла, поверх только что сохраненного кода программы.

Во время запуска программы код вируса сразу получает управление. Выполнив все свои действия, он восстанавливает начало зараженного файла, уничтожая свой код и передает ему управление.

Мы уже говорили, что размер выполнимых файлов в формате COM обычно не превышает 65536 байт. В принципе, можно создать COM файлы большего размера, но для этого они должны самостоятельно загружать себя. Большинство вирусов, заражающих COM-файлы, следят, чтобы суммарный размер файла и вируса не превышал данного значения. Если это условие не выполняется, заражение не происходит.

Среди вирусов, заражающих только COM-файлы, существуют и своего рода шедевры. Например, вирус Micro-92 имеет длину всего 92 байта. Вирус резидентный. Существует только в качестве академического. Автор вируса, Соловьев Михаил Анатольевич, прислал его непосредственно Лозинскому, гарантируя, что он не получит дальнейшего распространения.

Однако рекорд продержался недолго. Игорь Данилов создал вирус Micro-66 длиной 66 байт. Он существует только в качестве коллекционного экземпляра, никогда не распространялся и распространяться не будет. На момент написания книги самый короткий из известных нам вирусов имел длину 58 байт.

Процедура заражения вирусами EXE-файлов немного отличается от только что рассмотренной нами. Такие вирусы должны учитывать, что EXE-файлы имеют заголовок. При заражении вирус записывает себя в файл программы и может изменить заголовок EXE-файла.

Вирусы в драйверах

В операционной системе MS-DOS существует специальный вид программ, называемых драйверами. Драйверы запускаются только на этапе загрузки операционной системы, во время ее инициализации и интерпретации файла конфигурации CONFIG.SYS. Файлы драйверов обычно имеют расширение SYS.

Ряд вирусов разработан специально для заражения драйверов. Такие вирусы дописывают свой код к файлу драйвера и модифицируют его таким образом, чтобы вирус остался в оперативной памяти компьютера после загрузки драйвера.

Основные файлы операционной системы IO.SYS и MSDOS.SYS также могут быть заражены. Интересно, что в Microsoft Windows 95 файл MSDOS.SYS не содержит исполняемого кода, а предназначен для хранения параметров конфигурации системы:

```
[Paths]
WinDir=C:\WIN
WinBootDir=C:\WIN
HostWinBootDrv=C

[Options]
BootMulti=1
BootGUI=1
Network=0
;
;The following lines are required for compatibility with other programs.
;Do not remove them (MSDOS.SYS needs to be >1024 bytes).
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
...
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Естественно, в случае заражения этого файла Windows 95 перестанет правильно работать.

Вирусы в BAT-файлах

Среди огромного количества файловых вирусов, заражающих выполнимые файлы в формате COM и EXE, существует несколько вирусов, способных заражать пакетные файлы. Для этого используется весьма изощренный способ. Мы рассмотрим его на примере вируса BAT.Batman. При заражении пакетного файла в его начало вставляется текст следующего вида:

```
@ECHO OFF
REM [...]
copy %0 b.com>nul
b.com
del b.com
rem [...]
```

В квадратных скобках [...] схематично показано расположение байт, которые являются ассемблерными инструкциями или данными вируса. Команда @ECHO OFF

отключает вывод на экран названий выполняемых команд. Строка, начинающаяся с команды REM, является комментарием и никак не интерпретируется.

Команда copy %0 b.com>nul копирует зараженный командный файл в файл B.COM. Затем этот файл запускается и удаляется с диска командой del b.com.

Самое интересное, что выполнимый файл B.COM, созданный вирусом, до единого байта совпадает с зараженным командным файлом. Но командный файл состоит из команд операционной системы, а выполнимый COM-файл - из команд центрального процессора. Как же работает такая программа? Если переименовать любой текстовый файл в выполнимый, просто заменив его расширение на COM, он, конечно же, не будет работать. В лучшем случае компьютер просто зависнет.

Оказывается, что если интерпретировать первые две строки зараженного BAT-файла как программу, она будет состоять из команд центрального процессора, которые фактически ничего не делают.

Текст файла	BAT-файла		Команды ассемблера	Описание команд
@ECHO OFF	@	40h	INC AX	Увеличить на единицу значение регистра AX
	E	45h	INC BP	Увеличить на единицу значение регистра BP
	C	43h	INC BX	Увеличить на единицу значение регистра BX
	H	48h	DEC AX	Уменьшить на единицу значение регистра AX
	O	4Fh	DEC DI	Уменьшить на единицу значение регистра DI
		20h	AND [BX+46],CL	Сравнить значение регистра CL со значением ячейки памяти
	O F	4Fh 46h		
	F	46h	INC SI	Увеличить на единицу значение регистра SI
		0Dh	OR AX,520A	Записать в регистр AX результат логической операции ИЛИ между текущим значением AX и 520Ah
REM	R	0Ah 52h		
	E	45h	INC BP	Увеличить на единицу значение регистра BP

	M	4Dh	DEC BP	Уменьшить на единицу значение регистра BP
		20h	AND [SI],DH	Записать в регистр AX результат логической операции И между значением регистра DH и значением ячейки памяти
		34h		

Центральный процессор выполняет эти команды, а затем начинает выполнять настоящий код вируса, записанный после признака комментария REM. Получив управление, вирус перехватывает прерывания операционной системы и оставляет себя резидентным в оперативной памяти компьютера.

Резидентная часть вируса следит за записью данных в файлы. Если первая строка, записываемая в файл, содержит команду @echo, вирус считает, что записывается командный файл и заражает его.

Вirus BAT.Winstart

Вirus BAT.Winstart использует такую же технологию, что и вирус BAT.Batman. При запуске зараженного BAT-файла вирус копирует его в файл Q.COM, который создается в корневом каталоге диска C:. Затем файл Q.COM запускается уже как обычный выполнимый файл. В этот раз он устанавливает свой резидентный модуль в оперативной памяти и переименовывает файл C:\Q.COM в C:\WINSTART.BAT. Резидентный модуль вируса отслеживает момент запуска пользователем других программ и создает файл WINSTART.BAT в текущем каталоге.

@ECHO OFF

:s%r#

COPY %0.BAT C:\Q.COM>NUL

C:\Q

[...]

Когда командный файл WINSTART.BAT интерпретируется, как выполнимый файл в формате COM, то первая строка @ECHO OFF будет состоять из команд центрального процессора, которые фактически ничего не делают (см. вирус BAT.Batman). Вторая строка :s%r# будет воспринята как команда перехода на код вируса, схематично показанный квадратными скобками. Получив управление, основной коод вируса перехватывает прерывания операционной системы и оставляет себя резидентным в оперативной памяти компьютера.

Почему командный файл вируса называется WINSTART.BAT?

Файл WINSTART.BAT содержит команды, выполняемые при запуске операционной системой Windows в расширенном режиме. В этот файл обычно вносят вызовы резидентных программ, которые должны быть доступны только приложениям Windows. Программы MS-DOS, выполняемые в Windows, не имеют доступа к этим резидентным программам. За счет этого для программ MS-DOS остается больше свободной памяти.

Файл WINSTART.BAT не создается автоматически при установке Windows. Он должен быть создан самим пользователем и записан в каталог Windows, корневой каталог диска C: или любой другой каталог, определенный переменной среды PATH.

Вероятно, автор вируса рассчитывал на то, что вирус BAT.Winstart будет получать управление всякий раз, когда на компьютере запускается операционная система Windows.

Заражение файлов AUTOEXEC.BAT и CONFIG.SYS

Файлы конфигурации AUTOEXEC.BAT и CONFIG.SYS, содержат команды, выполняемые во время загрузки операционной системы. В том числе в этих файлах перечислены драйвера и программы, которые надо загрузить.

Обычно файлы AUTOEXEC.BAT и CONFIG.SYS создаются во время установки операционной системы и модифицируются во время установки различного программного обеспечения. Начинающие пользователи сами не изменяют эти файлы и не знают, что в них находится.

Целый ряд вирусов, например Em, Nocom, Some, DrWatson, вносят изменения в файлы AUTOEXEC.BAT и CONFIG.SYS. Эти вирусы создают на диске выполнимый файл, содержащий код вируса, а затем наглым образом вставляют команду запуска этого файла в AUTOEXEC.BAT или CONFIG.SYS.

Вirus BAT.282

Неопасный нерезидентный вирус. Создает в корневых каталогах дисков B: и C: файл VIRUS.BAT, содержащий вирусный код. Вставляет в файл AUTOEXEC.BAT вызов файла VIRUS.BAT

Обращайте внимание на все изменения в файлах AUTOEXEC.BAT и CONFIG.SYS. Изменение этих файлов, не связанное с установкой нового программного обеспечения, может быть результатом работы вируса.

Комбинированные вирусы

Большая часть вирусов не ограничивается заражением выполнимых файлов одного типа, например, только EXE- или только COM-файлов. Такие вирусы могут заражать и EXE- и COM-файлы. Некоторые вирусы также заражают еще и файлы оверлеев и драйверов.

Существуют файлово-загрузочные вирусы. Они распространяются как через выполнимые файлы, так и через загрузочные секторы жестких дисков и дискет. Если вы получите такой вирус, записав на свой компьютер зараженный выполнимый файл, то

получив управление, вирус запишет свою копию в главную загрузочную запись или загрузочный сектор жесткого диска. Дальнейшее распространение вируса происходит уже двумя путями - при копировании с компьютера зараженных программ и через загрузочные секторы дискет, используемых на компьютере.

За счет того, что один и тот же вирус может заражать различные объекты - выполнимые файлы, драйверы, загрузочные секторы, он получает больше возможностей для распространения.

Повторное заражение файлов и загрузочных секторов

Большинство вирусов заражают один и тот же файл или загрузочную запись только один раз. Такие вирусы перед заражением нового файла проверяют, не был ли он заражен раньше. В качестве признака, по которому определяется заражение, могут использоваться нестандартное время создания файла (операционная система MS-DOS позволяет устанавливать время создания файла 62 секунды), заведомо неправильная дата создания файла (например 2001 год). Более сложные вирусы определяют факт заражения поиском своей сигнатуры и т. д.

Самые примитивные вирусы могут заражать один файл по нескольку раз. Размер такого файла будет постоянно увеличиваться, значительно сокращая объем доступной дисковой памяти.

Несколько разных вирусов могут заразить один и тот же файл или загрузочную запись. Когда такой файл запускается, то сначала управление получает один вирус, затем другой и наконец выполняется сама зараженная программа.

Вирус Yankee Doodle

Целый ряд вирусов, заражающих выполнимые файлы. Некоторые версии вируса в определенное время исполняют на встроеном динамике компьютера мелодию Yankee Doodle. Интересно, что этот вирус борется с загрузочным вирусом Ball. Он изменяет его код таким образом, что вирус Ball через некоторое время самостоятельно удаляет себя с жесткого диска компьютера.

Вирус DIR

Летом 1991 года разразилась эпидемия нового вируса. Его проявления были весьма интересны. Во время копирования зараженных файлов в любом случае копировались только 1024 байта, несмотря на то, что фактические длины файлов были совершенно другие. Проверка целостности структуры файловой системы с помощью программы CHKDSK или Norton Disk Doctor выявляла наличие большого количества потерянных кластеров и пересечений файлов. Если, обнаружив нарушение в структуре файловой системы, пользователь пытался ее исправить, то все зараженные файлы оказывались испорченными.

Однако, несмотря на то что внешне зараженные программы кажутся совершенно неработоспособными, они работали как обычно. Так появился новый тип вируса, впоследствии названный DIR.

Способ размножения вируса DIR значительно отличается от используемых обычными файловыми вирусами и вирусами-спутниками. Тем не менее, мы отнесли его к группе файловых вирусов, так как объектом нападения становятся именно исполнимые файлы программ.

Чтобы лучше понять механизм распространения вируса DIR, мы проведем небольшой экскурс в структуру файловой системы MS-DOS. Более подробную информацию вы найдете в шестой главе этой книги.

При описании загрузочных вирусов мы уже рассказывали, что данные хранятся на жестких дисках и дискетах в отдельных секторах. Несколько секторов, расположенных рядом, называют кластером. Когда на диске создается новый файл, операционная система отводит для него несколько свободных кластеров. Кластеры файла не обязательно должны следовать друг за другом. Поэтому операционная система хранит список номеров всех кластеров, распределенных файлу, в специальной таблице. Эта таблица называется таблицей распределения файлов (FAT - File Allocation Table).

В таблице распределения файлов для каждого кластера есть один элемент. Его значение характеризует состояние кластера. Например, свободный кластер отмечается нулевым значением, а кластер, непригодный для использования, отмечается числом FF7h (FFF7h). Если кластер распределен файлу, то соответствующий элемент FAT содержит номер следующего кластера файла. Последний кластер файла отмечается числом в диапазоне от FF8h до FFfh (от FFF8h до FFFfh).

Сама таблица FAT находится практически сразу после загрузочной записи логического диска. Точное ее расположение описано в специальной структуре данных, записанной в загрузочном секторе. Однако таблица FAT не содержит ни названий файлов, ни других их атрибутов. Для этого операционная система поддерживает другую служебную структуру, которая называется корневым каталогом. Каждый логический диск имеет собственный корневой каталог.

В корневом каталоге описаны файлы и другие каталоги, которые в нем содержатся. Описание каждого файла и каталога включает его имя с расширением, дату и время создания, длину (для каталога она равна нулю), атрибуты и зарезервированное поле, которое не используется. Еще в описании файла хранится номер первого кластера, отведенного файлу или каталогу. Получив этот номер, операционная система может узнать все остальные номера кластеров файла через таблицу FAT (рис. 1.8).

Другие каталоги имеют точно такую же структуру, что и корневой каталог. В них также находятся описания файлов и других подкаталогов.

Когда пользователь запускает файл на выполнение, операционная система просматривает описания файлов в текущем каталоге текущего логического диска. Если файл с нужным именем найден, операционная система узнает из описания файла номер

первого кластера файла, а затем по таблице FAT определяет остальные номера кластеров. После этого данные из кластеров файла считываются в оперативную память. Здесь они объединяются в один непрерывный участок, даже если кластеры файла были разбросаны по всему логическому диску.

Затем операционная система выполняет подготовительную работу, зависящую от типа файла (COM- или EXE-файл) и передает ему управление. На этом загрузка программы завершается и программа начинает работать.

Заражение вирусом DIR происходит следующим образом. Вирус DIR копирует свой код в один из кластеров заражаемой дискеты или логического диска. Этот кластер помечается в таблице FAT как конец файла. Затем вирус меняет описания файлов COM и EXE в структурах каталогов. Вирус записывает вместо номера первого кластера файла номер кластера, содержащего его код (рис. 1.9). Настоящий номер первого кластера зараженного файла шифруется и записывается в неиспользуемую область описания файла.

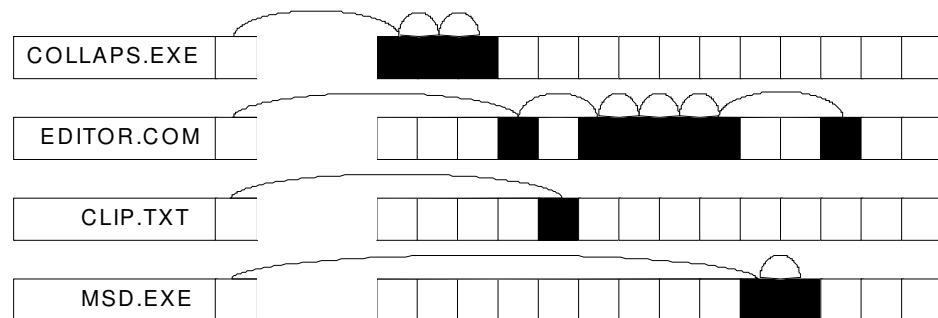


Рис. 1.8. Структура каталогов

Когда пользователь запускает один из зараженных файлов, с диска считывается только один кластер, содержащий код вируса. Таким образом, вирус сразу получает управление. Он устанавливает себя резидентным в оперативной памяти и перехватывает все обращения к диску. Затем вирус определяет настоящее расположение файла программы и загружает ее.

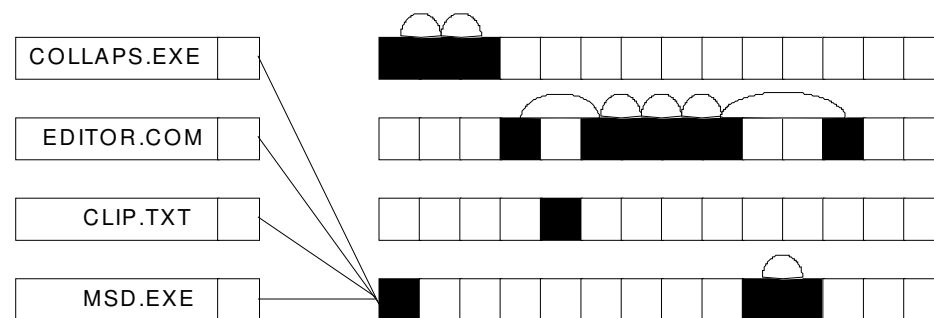


Рис. 1.9. Структура каталогов после заражения вирусом DIR

Если теперь операционная система будет обращаться к каталогу, вирус передаст ей правильные значения для номеров первых кластеров зараженных файлов.

Впоследствии появилось несколько разновидностей вируса DIR, отличающихся друг от друга в основном только скрытыми функциями, выполняемыми вирусами. Для лечения вируса DIR и его разновидностей вы можете использовать антивирусную программу Aidstest, однако можно обойтись и без антивируса, достаточно скопировать выполнимые файлы, заменив их расширение, например, на CO_ и EX_ соответственно.

Маскировка вирусов

Обычные вирусы, заражающие файлы, обнаружить достаточно легко. Для этого можно, например, записать длины всех выполнимых файлов и периодически проверять их. Идентифицировать такие вирусы также очень просто. Так как вирусы всегда дописывают к файлу одну и ту же последовательность кода, антивирусные программы могут просматривать выполнимые файлы и загрузочные секторы в поисках таких последовательностей. В большинстве случаев антивирусная программа может не хранить в себе шаблоны всех известных вирусов. Достаточно определенных характерных для данного вируса последовательностей, которые называются сигнатурами.

Например, для вируса BAT.Batman характерной может служить следующая последовательность (подробное описание вируса BAT.Batman смотри выше):

```
copy %0 b.com>nul
b.com
del b.com
```

Для вируса WinWord.Concept такой характерной последовательностью может служить одна из следующих строк:

```
see if we're already installed
iWW6Instance
WW6Infector
```

Многие загрузочные вирусы также легко могут быть обнаружены простым просмотром загрузочных секторов жестких дисков компьютера и дискет. Например, вирус Stoned, содержит строки "Your PC is now Stoned!" и "LEGALISE MARIJUANA!".

Однако далеко не все вирусы ведут себя так грубо. Многие из них маскируют свое присутствие, используя для этого различные приемы. Вследствии естественного отбора антивирусными программами шанс выжить есть только у вирусов, применяющих разнообразные методы маскировки.

Шифрующиеся и полиморфные вирусы

Чтобы затруднить обнаружение, некоторые вирусы шифруют свой код. Каждый раз, когда вирус заражает новую программу, он зашифровывает собственный код, используя новый ключ. В результате два экземпляра такого вируса могут значительно отличаться друг от друга, даже иметь разную длину.

Естественно, вирус может работать только в том случае, если исполняемый код расшифрован. Когда запускается зараженная программа (или начинается загрузка с зараженной загрузочной записи) и вирус получает управление, он должен расшифровать свой код.

Процедура расшифровки не может сама быть зашифрована, в противном случае она не сможет работать. Этим пользуются антивирусные программы, использующие в качестве сигнатуры код процедуры расшифровки.

Тем не менее, авторы вирусов нашли выход из этой ситуации. Для шифрования вирусов они стали использовать не только разные ключи, но и разные процедуры шифрования. Два экземпляра таких вирусов не имеют ни одной совпадающей последовательности кода. Такие вирусы, которые могут полностью изменять свой код, получили название полиморфных. Наиболее известные из них - это Phantom-1, Natas, OneHalf, SatanBug.

Первым полиморфным вирусом считают V2Px.1260. Он был создан Марком Вашбурном (Mark Washburn) в качестве экспериментального вируса. На настоящий момент существует огромное количество полиморфных вирусов. Вот только несколько их названий: Basilisk.1639, CeCe.1994, CeCe.1998, CommanderBomber, Dir-II.TheHndV, Flip.2153, Flip.2343, Flip.2365, Fly.1769, Holms.6161, Invisible.2926, Invisible.3223, RDA.Fighter.5871, RDA.Fighter.5969, RDA.Fighter.7408, RDA.Fighter.7802.

К сожалению, сегодня создавать полиморфные вирусы могут не только программисты, обладающие высокой квалификацией. Существует несколько готовых средств разработки таких вирусов. Они позволяют разрабатывать полиморфные вирусы без понимания того, как последние устроены.

Первым таким средством создания полиморфных вирусов стал Dark Angel MuTation Engine (иногда называется MtE или DAME), созданный болгарским автором вирусов известным, как Dark Avenger.

В состав MuTation Engine входит объектный модуль, который необходимо подключить к создаваемому вирусу, подробная документация и пример его

использования. Благодаря MuTation Engine появилось много полиморфных вирусов. Среди них MtE.CoffeeShop, MtE.Darkstar, MtE.Dedicated.

Вслед за MuTation Engine появились еще несколько средств разработки полиморфных вирусов, имеющих различный уровень сложности и сервиса:

- *AWME (Anti WEB Mutation Engine)*
- *CLME (Crazy Lord Mutation Engine)*
- *DSCE (Dark Slayer Confusion Engine)*
- *GCAE (Golden Cicada Abnormal Engine)*
- *NED (NuKE Encryption Device)*
- *SMEG (Simulated Metamorphic Encryption Generator)*
- *TPE (TridenT Polymorphic Engine)*
- *VICE (Virogen's Irregular Code Engine)*

После появления очередного средства разработки полиморфных вирусов некоторые авторы вирусов создавали на их основе собственные вирусы.

Интересно, что AWME является отечественной разработкой и создан в Казани. По нашим сведениям, AWME ориентирован на противодействие антивирусной программе Doctor Web. Более подробно об этом можно прочитать в разделе “Doctor Web”. AWME распространяется в виде исходного текста на языке ассемблера.

Современные антивирусные средства, например Doctor Web, умеют не только успешно идентифицировать полиморфные вирусы, но также и удалять их из зараженной программы.

Шифрование кода вируса значительно усложняет процесс его исследования. Обычные программы не смогут дизассемблировать такой вирус. Тот, кто отважится разобраться в зашифрованном вирусе, должен будет разбираться с ним, выполняя код вируса команда за командой в пошаговом режиме отладчика.

Стелс-вирусы

Стелс-вирусы пытаются скрыть свое присутствие в компьютере. Они имеют резидентный модуль, постоянно находящийся в оперативной памяти компьютера. Этот модуль устанавливается в момент запуска зараженной программы или при загрузке с диска, зараженного загрузочным вирусом.

Резидентный модуль вируса перехватывает обращения к дисковой подсистеме компьютера. Если операционная система или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль вируса может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова.

Примером стелс-вируса может служить Magdzie.1114. Это файловый вирус, заражающий выполнимые файлы в формате EXE. При запуске зараженной программы в оперативной памяти устанавливается вирусный резидентный модуль, который перехватывает обращения к файловой системе компьютера. Если операционная система запускает или открывает для чтения файл зараженной программы, вирус временно удаляет из нее свой код. Обратное заражение происходит, когда операционная система закрывает файл.

Вирус Magdzie проявляется, удаляя все файлы, название которых начинается с CHKLIST. 27 мая вирус выводит на экран небольшой текст и движущийся графический узор.

Загрузочные вирусы действуют по такой же схеме. Когда какая-либо программа считывает данные из загрузочного сектора, они заменяются настоящим содержимым загрузочного сектора.

В качестве загрузочного вируса, использующего для маскировки стелс-технологию, можно привести вирус July29. Вирус распространяется, замещая главную загрузочную запись на жестких дисках и загрузочную запись на дискетах. Настоящие загрузочные секторы сохраняются. Когда программа пытается прочитать или записать данные в главную загрузочную запись жесткого диска или загрузочную запись дискеты, резидентный модуль вируса подставляет неинфицированный сектор.

Маскировка стелс-вирусов срабатывает только в том случае, если в оперативной памяти компьютера находится резидентный модуль вируса. Когда вы загружаете компьютер с системной дискеты, у вируса нет шансов получить управление и поэтому стелс-механизм не работает.

Большинство антивирусных программ требует, чтобы для проверки и лечения компьютера он был загружен с системной дискеты, на которой нет вирусов. Такая дискета должна быть подготовлена заранее. Более подробно об этой процедуре вы можете прочитать в разделе “Создание системной дискеты”.

Комбинированный метод маскировки

Чтобы достичь еще большей неуязвимости вирусы могут комбинировать различные методы маскировки. Так, многие вирусы комбинируют в себе свойства полиморфных и стелс-вирусов.

К таким вирусам относятся вирусы серии OneHalf. Эти вирусы не только скрывают свое присутствие, используя стелс-технологию, они также маскируются, полностью изменяя свой код при заражении очередного файла или загрузочного сектора.

Внешние проявления болезни

Большинство вирусов не только размножаются, заражая новые и новые компьютеры, они еще выполняют дополнительные действия или, другими словами, спецэффекты, предусмотренные их автором.

У разных вирусов эти дополнительные действия могут быть опасными или неопасными, бросающимися в глаза или скрытыми, трудно обнаружимыми. Рассказать обо всех проявлениях вирусов невозможно, для этого надо описать каждый вирус. Мы расскажем только о наиболее типичных и наиболее интересных случаях.

Даже те вирусы, которые не совершают явных разрушительных действий, могут представлять опасность из-за ошибок, допущенных авторами вирусов

Опасные вирусы

Большую и самую опасную группу составляют вирусы, выполняющие разрушение программного обеспечения компьютера и файлов данных, записанных на его дисках.

Вирусы могут стирать файлы с жесткого диска, записывать мусор в отдельные секторы диска. Действие таких вирусов часто проявляется в разрушении файловой системы компьютера. Отдельные вирусы способны полностью уничтожить всю информацию на жестких дисках компьютера и дискетах, выполнив операцию форматирования.

Действие других вирусов менее бросается в глаза, и от этого они становятся еще опасней. Эти вирусы могут незаметно изменять данные в случайным образом выбранных файлах. Вы можете долгое время не замечать эти изменения, пока они не приведут к серьезным последствиям.

Интересный и опасный случай представляют вирусы, которые изменяют программную среду компьютера таким образом, что становятся ее неотъемлемой частью. Подобные вирусы очень сложно удалить. Если файлы, зараженные этими вирусами, просто удалить или восстановить с резервных копий, то система вообще может перестать работать.

В качестве примера можно привести файлово-загрузочный резидентный вирус OneHalf. Проникая в компьютер, вирус заражает главную загрузочную запись. Во время загрузки компьютера вирус постепенно шифрует секторы жесткого диска, начиная с самых последних. Когда резидентный модуль вируса находится в памяти, он контролирует все обращения к зашифрованным секторам и расшифровывает их, так что все программное обеспечение компьютера работает нормально. Если OneHalf просто удалить из оперативной памяти и загрузочного сектора, то станет невозможно правильно прочитать информацию, записанную в зашифрованных секторах диска.

Когда вирус зашифрует половину жесткого диска, он отображает на экране надпись:

Dis is one half.

Press any key to continue ...

После этого вирус ожидает, когда пользователь нажмет на какую-либо клавишу и продолжает свою работу. Для некоторых версий вируса отображаемая им надпись может несколько отличаться от приведенной нами.

Вирус OneHalf использует различные механизмы для своей маскировки. Он является стелс-вирусом и использует при распространении полиморфные алгоритмы. Обнаружение и удаление вируса OneHalf - достаточно сложная задача. Далеко не все антивирусные программы, которые определяют этот вирус могут его удалить. Например, антивирусная программа Norton Antivirus for Windows 95 версии 4.0 только обнаруживает OneHalf. Чтобы его удалить, пользователь должен вызвать специальную службу.

По итогам работы антивирусной скорой помощи АО “ДиалогНаука” вирус OneHalf занимает одно из первых мест по распространенности. Это связано с тем, что многие популярные антивирусные программы, например AIDSTEST, не обнаруживают этот вирус. Тем не менее, вы можете удалить OneHalf при помощи антивирусной программы Doctor Web. Эта программа позволяет обнаружить и полностью освободить компьютер от многочисленных вариантов вируса OneHalf. Doctor Web аккуратно расшифровывает все участки жесткого диска, зашифрованные вирусом. Операция расшифровки может занять значительное время, в зависимости от того, насколько много секторов диска вирус успел зашифровать.

Разрушение аппаратуры компьютера

Могут ли вирусы вызывать аппаратные повреждения компьютера? На момент написания книги точной информации о таких вирусах не было. Сведения о вирусах, которые могут перепрограммировать видеоадаптер таким образом, чтобы он выжег люминофор на экране монитора, и вирусах, которые вводят в резонанс головки жесткого диска, достоверно не подтверждены.

Тем не менее, существуют вирусы, которые могут основательно вывести компьютер из строя. Многие компьютерные вирусы стирают или портят содержимое энергонезависимой CMOS-памяти компьютера. В результате чего компьютер перестает загружаться.

Отдельные вирусы используют еще более изощренный метод - они устанавливают в CMOS-памяти пароль для загрузки системы. При этом блокируется как загрузка компьютера, так и доступ к программе Setup. Убрать такой пароль можно, на время отключив питание энергонезависимой памяти. Для этого необходимо открыть корпус компьютера и переставить перемычки на системной плате.

Существуют системные платы (например Enterprise-II), на которых CMOS-память и питающий их аккумулятор расположены внутри одной микросхемы. Сбросить такую CMOS-память, отключив питание, невозможно. После того как вирус установит свой

пароль, вам остается только угадать его или отправить системную плату на завод-изготовитель (либо просто купить новую системную плату).

Вирус и человек

В 1994 году в печати появилось сообщение о новом компьютерном вирусе, который может убить пользователя компьютера. Вирус якобы использует прием, давно известный в рекламной сфере: если человек смотрит кино и каждый двадцать пятый кадр заменяется другим изображением, то он подсознательно воспринимает изображение, не осознавая этого. Действуя на подсознание таким образом, можно склонить человека к определенным действиям.

Вирус заменяет некоторые кадры изображения на экране компьютера. Изображение, которое вирус передает подсознанию пользователя, вызывает у последнего повышение давления и, возможно, смерть.

Мы не станем останавливаться на медицинских и психологических аспектах этого вопроса - этим должны заниматься медики и психологи. От себя заметим, что до настоящего момента достоверной информации о вирусе-убийце нет. В принципе, уровень современной компьютерной техники позволяет менять изображение на мониторе с достаточной частотой - до сорока кадров в секунду. И, возможно, скоро ваше здоровье действительно будет напрямую связано со “здоровьем” компьютера.

Вирусы и логические бомбы

Многие вирусы содержат в себе логические бомбы. До определенного момента такой вирус никак себя не проявляет. Когда наступит время, логическая бомба срабатывает и вирус выполняет скрытую в нем функцию.

Самые известные вирусы, срабатывающие по достижении определенного времени - Michelangelo и Jerusalem. Вирус Michelangelo уничтожает информацию с диска, используемого для загрузки 6 марта, в день рождения Микеланджело. Вирус Jerusalem или Черная пятница удаляет файлы всех программ, запускаемых в пятницу тринадцатого числа.

Вирс Armagedon.1079

Неопасный резидентный вирус. С пяти до шести часов утра вирус пытается соединиться через модем с удаленным абонентом. Содержит строк у "Armagedon the GREEK"

Безопасные вирусы

Много вирусов не выполняют деструктивных действий, а содержат своего рода шутки - забавные видео- или аудио-эффекты. Такие вирусы могут отображать на экране

монитора разнообразные надписи, проигрывать на встроенном динамике компьютера простенькие мелодии и т. д. Тем не менее, большинство вирусов не содержат в себе абсолютно ничего интересного, кроме факта, что кому-то не лень было тратить свое время на такую ерунду.

Абсолютно безопасных вирусов не бывает. Даже если они не выполняют явных разрушительных действий, в них могут содержаться ошибки, вызывающие неправильную работу операционной системы и пользовательских программ. Кроме того, внедряясь в программы, вирусы нарушают авторские права программистов.

В любом случае, если компьютер стал вести себя странно, следует сразу прекратить работу и проверить его на заражение вирусами. Возможно, быстрое обнаружение вируса не позволит ему нанести значительный ущерб.

Вирусы в файлах документов

Долгое время мало кто подозревал, что компьютерные вирусы могут распространяться, заражая текстовые файлы документов. Пользователи свободно обменивались документами, подготовленными в различных текстовых редакторах, не опасаясь, что вместе с ними на компьютер проникнет вирус.

Однако летом 1995 г. появился первый такой вирус. Этот вирус, получивший название WinWord.Concept, распространяется, заражая файлы документов в формате текстового процессора Microsoft Word for Windows версии 6.0 и 7.0.

С первого взгляда такое сообщение кажется фантастическим, так как вирус должен содержать выполняемые команды, а в документе обычно хранится только текст и его шрифтовое оформление. Не все пользователи, даже проработав в среде Microsoft Word for Windows несколько лет, знают, что вместе с документом могут храниться макрокоманды, созданные с использованием специального языка программирования WordBasic. Эти макрокоманды фактически являются самыми настоящими программами.

Первая ласточка - вирус WinWord.Concept

Вирус WinWord.Concept никак не маскирует свое присутствие. Наоборот, он создан таким образом, чтобы облегчить свое обнаружение и анализ. Макрокоманды вируса WinWord.Concept не закрыты от чтения и их очень легко проанализировать. Мы получили этот вирус в АО “ДиалогНаука” и самостоятельно провели такой анализ. Вирус состоит из пяти макрокоманд, общий объем которых составляет примерно 110 строк на языке WordBasic. В добавок к этому автор вируса снабдил его комментариями.

Когда пользователь открывает зараженный файл документа, Microsoft Word for Windows автоматически выполняет содержащуюся в нем макрокоманду AutoOpen. Эта макрокоманда принадлежит вирусу. Она просматривает названия всех макрокоманд, определенных в файле стилей NORMAL.DOT. Если среди них обнаружена макрокоманда PayLoad, считается, что файл стилей уже заражен. Если присутствует макрокоманда FileSaveAs, вирус также не будет устанавливаться. Видимо автор посчитал, что в этом случае нужно слишком много возиться.

Если просмотрен весь список макрокоманд и среди них не обнаружены ни макрокоманды PayLoad, ни FileSaveAs, вирус копирует в файл стилей NORMAL.DOT макрокоманды PayLoad, FileSaveAs, AAAZFS и AAAZAO.

После копирования макрокоманд вирус добавляет в файл конфигурации WINWORD6.INI текстового процессора параметр WW6I=

WW6I=1

В конце выполнения вирусной макрокоманды AutoOpen вирус отображает на экране временную диалоговую панель. На этом установка вируса считается оконченной и вы увидите в окне редактирования текстового процессора открытый документ.

Заражение документов происходит, когда пользователь сохраняет их при помощи команды "Save As". В этом случае выполняется макрокоманда вируса FileSaveAs. Она отображает на экране обычную диалоговую панель "Save As".

Пользователь вводит в этой диалоговой панели имя файла документа, под которым он будет сохранен. Заметим, что обычно документ сохраняется в формате “Word Document” (формат указывается в поле “Save File as Type”). В принципе, документ можно сохранить и в других форматах, например, в обычном текстовом формате или в формате RIF (Rich-Text Format).

Если пользователь сохраняет документ в формате документов текстового процессора Microsoft Word for Windows (формат “Word Document”), тогда вирус изменяет формат сохраняемого документа. Вместо того чтобы сохранить документ в формате документов текстового процессора Microsoft Word for Windows, он сохраняет его в формате файла стилей, предварительно записав в него макрокоманды AutoOpen, AAAZAO, AAAZFS и PayLoad.

Таким образом, WinWord.Concept незаметно изменяет формат документа, сохраняя его на диске как файл стилей. Внешне такой файл практически не отличается от обыкновенного файла документа. Он также имеет расширение DOC, а при загрузке в текстовый процессор вы увидите набранный вами текст.

Никаких дополнительных действий вирус WinWord.Concept не выполняет. В макрокоманду PayLoad, которая могла быть использована для этого, автор включил только один комментарий:

Sub MAIN

REM That's enough to prove my point

End Sub

Но за счет того, что зараженный документ сохраняется в формате файла стилей, текстовый процессор не позволит вам сохранить его в другом формате. Когда вы выберете из меню File строку Save As, на экране появится диалоговая панель Save As, но поле выбора типа документа - “Save File as Type” будет показано серым цветом и недоступно для изменения.

Как обнаружить WinWord.Concept?

Вы легко можете проверить, заражен ли текстовый процессор Microsoft Word for Windows вирусом WinWord.Concept даже без специальных программ. Самый простой способ основан на том, что активный вирус записывает в файл конфигурации WINWORD6.INI параметр WW6I.

Файл WINWORD6.INI располагается в каталоге Windows и вы можете просмотреть его в любом текстовом редакторе, например в редакторе Notepad, входящем в состав Windows.

Запустите приложение Notepad. Если файл WINWORD6.INI имеет большой размер и вам трудно его просматривать, выберите из меню Search строку Find. На экране откроется диалоговая панель Find. Введите в поле Find What текст WW6I, который надо найти и нажмите кнопку Find Next. Если в файле обнаружится параметр WW6I, скорее всего, ваш компьютер заражен вирусом WinWord.Concept.

Другой способ обнаружения вируса предполагает, что вы запустили текстовый процессор Microsoft Word for Windows. Выберите из меню Tools строку Macro. На экране появится диалоговая панель Macro (рис. 1.10). Из списка Macros Available In выберите строку All Active Templates. Обратите внимание на список макрокоманд Macro Name. Если в нем находятся строки AAAZAO, AAAZFS, AutoOpen, FileSaveAs, PayLoad, текстовый процессор инфицирован вирусом WinWord.Concept.

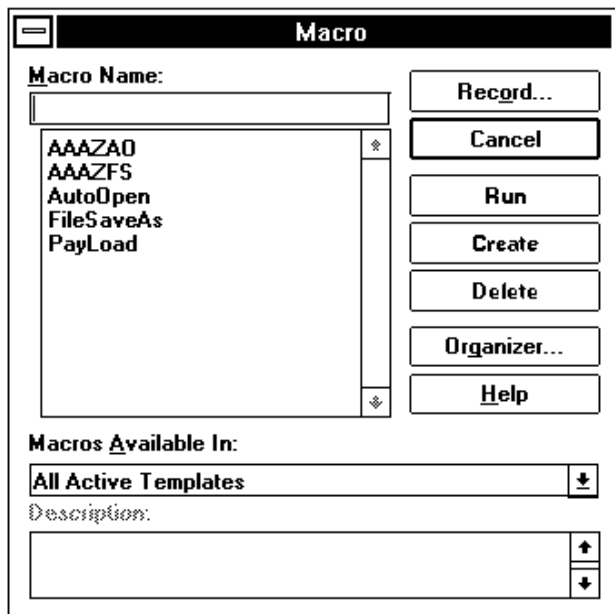


Рис. 1.10. Диалоговая панель "Macro"

И еще один способ самостоятельного обнаружения вируса основан на том, что зараженные файлы документов или стилей содержат в себе несколько незашифрованных текстовых строк:

[see if we're already installed](#)
[iWW6Instance](#)
[WW6Infector](#)
[AAAZFS](#)
[AAAZAO](#)
[That's enough to prove my point](#)

Эти строки можно обнаружить с помощью любой программы просмотра файлов в формате ASCII. Например, с помощью встроенной программы просмотра оболочки Norton Commander.

Просмотр вручную всех файлов на всех дисках компьютера займет много времени. Чтобы ускорить этот процесс, удобно воспользоваться специальными программами поиска. Очень удобно приложение Find File, входящее в состав Microsoft Office.

Запустите приложение Find File и откройте диалоговую панель Search. Вирус WinWord.Concept может располагаться в файлах *.DOC, *.DOT, *.BAK. Поэтому укажите эти имена в поле File Name. Затем нажмите кнопку Advanced Search. На экране появится диалоговая панель Advanced Search. Нажмите на закладку Location и пользуйтесь органами управления этой панели, сформируйте список каталогов, в которых будет проводиться поиск. Мы рекомендуем внести в этот список корневые каталоги всех логических дисков компьютера.

Затем нажмите на закладку Summary и введите в поле Containing Text текст для поиска. В качестве текста можно воспользоваться предложением "That's enough to prove my point", текст которого взят из вируса. Убедитесь, что поиск будет выполняться по всем файлам. Для этого поля Title, Autor, Keywords и Subject должны остаться незаполненными. Убедитесь также, что в процессе поиска будут просмотрены все файлы вне зависимости от времени их создания. Для этого нажмите закладку Timestamp.

Нажмите кнопку OK. Вы вернетесь в диалоговую панель Search. Чтобы начать поиск, нажмите кнопку OK. Приложение Find File просмотрит все файлы документов и стилей. После окончания поиска оно составит список имен файлов, в которых было обнаружено искомое предложение и которые, вероятно, инфицированы вирусом WinWord.Concept.

Вирус WinWord.Nuclear

Практически сразу после появления вируса WinWord.Concept был обнаружен еще один вирус подобного вида WinWord.Nuclear. Этот вирус использует точно такую же технологию распространения, что и вирус WinWord.Concept.

Вирус WinWord.Nuclear уже далеко не такой безобидный, как WinWord.Concept. Когда пользователь направляет свой документ на печать, то вирус с вероятностью 1/12 добавляет в конце файла собственную фразу:

And finally I would like to say:

STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!

В переводе на русский язык она звучит следующим образом:

И в конце я хотел бы сказать:

ОСТАНОВИТЕ ВСЕ ФРАНЦУЗСКИЕ ИСПЫТАНИЯ ЯДЕРНОГО ОРУЖИЯ В ТИХОМ ОКЕАНЕ!

Если фраза добавится в конце черновой распечатки, это только полбеда, но в случае, когда распечатанный документ отправляется адресату непросмотренным, можно представить себе удивление последнего. Такая ситуация может возникнуть, если к компьютеру подключен факс-модем и вместо печати документа на принтере он отправляется удаленному абоненту в качестве факсимильного сообщения.

Достаточно странно, что вирус, написанный пацифистом, пятого апреля пытается удалить основные файлы операционной системы - IO.SYS, MSDOS.SYS и COMMAND.COM. Но из-за ошибок автора вируса и особенностей текстового процессора эта попытка не удастся.

Вирус WinWord.Nuclear заражает не только файлы документов и стилей. Что удивительно, WinWord.Nuclear может заразить обыкновенные выполнимые файлы в формате COM и EXE. Он также может заразить EXE-файлы, предназначенные для операционной системы Windows.

Для заражения выполнимых файлов используется оригинальный способ. Вирус запускает программу DEBUG, передавая ей в качестве параметра ранее сформированный им файл PH33R.SCR.

Программа DEBUG - это простой отладчик, который входит в состав дистрибутива MS-DOS и копируется на жесткий диск компьютера во время установки операционной системы, поэтому он присутствует практически на всех компьютерах. В числе прочего DEBUG позволяет просмотреть и изменить содержимое оперативной памяти, запустить программу и т. д.

Вирусы в макрокомандах

Мы уже рассказали вам о вирусах в макрокомандах текстового процессора Microsoft Word for Windows. Вирусы, использующие подобные пути распространения, существуют не только в Microsoft Word for Windows.

|| *Когда мы уже заканчивали писать эту книгу, получили сообщения о появлении еще трех вирусов, предназначенных для текстового процессора Microsoft Word for Windows - WinWord.Colours, WinWord.DMV и WinWord.Hot*

В качестве примера можно привести вирус WinMacro.Weider, распространяющийся в среде редактора электронных таблиц Excel. Этот пакет имеет встроенные средства создания макрокоманд, сходные с языком WordBasic текстового процессора Microsoft Word for Windows.

Появление подобных вирусов возможно и в других приложениях Windows. На наш взгляд, единственной возможностью обезопасить себя от таких новинок является постоянное обновление ваших антивирусных программ и внимательное изучение публикаций по антивирусной тематике.

Вирус WinWord.Concept, а также другие аналогичные вирусы можно назвать кросс-платформными. Компьютер с любой архитектурой, а не только совместимый с IBM PC, на котором установлен текстовый процессор Microsoft Word for Windows, может быть заражен таким вирусом.

Как противостоять вирусам в файлах документов

Текстовый процессор Microsoft Word for Windows позволяет запретить автоматическое выполнение макрокоманд. Для этого можно воспользоваться одним из перечисленных ниже способов:

- При запуске Microsoft Word for Windows из приложения Program Manager *держите нажатой клавишу <Shift>*
- Укажите Microsoft Word for Windows *дополнительный параметр /m (WINWORD.EXE /m).*
- Когда вы открываете документ для редактирования, *держите нажатой клавишу <Shift>.*

Естественно, использование этих средств вызывает некоторые неудобства, а в некоторых случаях может привести к нежелательным последствиям (будет запрещено автоматическое выполнение всех макрокоманд, даже тех которые нужны). Кроме того, есть сведения, что эти приемы срабатывают не во всех случаях.

Вместо этого вы можете сами полностью блокировать автоматическое выполнение макрокоманд. Для этого следует определить макрокоманду с именем AutoExec. Эта макрокоманда будет автоматически вызываться при каждом запуске текстового процессора.

Выберите из меню Tools строку Macro. На экране появится диалоговая панель Macro. Наберите в поле Macro Name строку AutoExec и нажмите кнопку Create. Появится окно текстового редактора, содержащее заготовку макрокоманды AutoExec:

Sub MAIN

End Sub

Вставьте между этими двумя строками команду DisableAutoMacros:

Sub MAIN

DisableAutoMacros

End Sub

Завершите работу текстового процессора, отвечая утвердительно на предложение записать новую макрокоманду в файл NORMAL.DOT и предложение сохранить сам файл NORMAL.DOT. Если вы работаете в русской версии текстового процессора Microsoft Word for Windows, этот метод также можно использовать с учетом русских названий меню и диалоговых панелей.

К сожалению, запрещение автоматического выполнения макрокоманд не позволяет обнаружить и обезвредить уже существующие вирусы, но дальнейшая их деятельность в среде Microsoft Word for Windows будет остановлена.

Вирусы и Windows

Несмотря на то, что выполнимые файлы Windows, которые вы можете запускать, также имеют расширение EXE, формат этих файлов значительно отличается от выполнимых файлов операционной системы MS-DOS. Новый формат выполнимых файлов получил название Microsoft New Executable (NewEXE) или Windows Executable. Мы будем называть эти файлы выполнимыми файлами в формате Windows. Обычные вирусы не в состоянии правильно внедриться в такие файлы и зараженная программа становится неработоспособной.

Однако, несмотря на то что Windows установлена на большинстве персональных компьютеров, старые вирусы не вымерли. В первую очередь это произошло из-за того, что работа в среде Windows совсем не означает отказа от программного обеспечения MS-DOS. Существует достаточно много нужных программ, предназначенных для работы в MS-DOS. В первую очередь это небольшие утилиты - программы-архиваторы, программы для копирования дискет - и, конечно же, огромное количество всевозможных игр. Естественно, все это программное обеспечение используется и будет использоваться еще очень долго.

Но даже полный отказ от программ MS-DOS не снимет угрозу распространения вирусов. Во-первых, остается возможность заражения загрузочных секторов жестких дисков и дискет. Во-вторых, внимание писателей вирусов рано или поздно переключится на Windows и появятся новые типы вирусов, способных функционировать и распространяться в новой среде. Подтверждением этому стали вирусы, заражающие выполнимые файлы Windows, и вирусы, заражающие документы, подготовленные в текстовом процессоре Microsoft Word for Windows. В начале 1996 года, практически сразу после появления Microsoft Windows 95, появилось сообщение о первом вирусе, разработанном специально для этой операционной системы. Этот вирус получил название BOZA.

Вирусы MS-DOS для Windows

Обычный выполнимый файл Windows может служить отличной средой для распространения вирусов. Если вы запускаете выполнимый файл операционной системы

Microsoft Windows из командной строки MS-DOS, он сообщает, что его необходимо запускать из Windows:

[This program requires Microsoft Windows.](#)

или

[This program cannot be run in DOS mode.](#)

Иногда вместо этого сообщения может отображаться какая-нибудь другая информация или выполняться иные действия. Например, некоторые приложения Windows, запущенные из среды MS-DOS, пытаются загрузить Windows.

Авторы вирусов не упустили возможность внедрить вирус в этот участок кода. Вирус Grog.Bog.233 выполняет поиск выполнимых файлов Windows и заражает их, добавляя команды вируса в код, выполняемый при запуске файла в среде MS-DOS. Если запустить такой файл в MS-DOS, то он сначала выводит на экран предупреждающее сообщение, а затем управление передается вирусу.

Bupyc SMEG.Trivia.2437

Неопасный нерезидентный полиморфный вирус. В пятницу у 13 числа выводит сообщение "This program requires Microsoft Windows.", после чего заканчивает выполнение инфицированной программы. Данный вирус был создан Black Baron для демонстрации использования его полиморфного генератора SMEG версии 0.3

Конечно, вирус Grog.Bog.233 трудно назвать настоящим вирусом, созданным для работы в операционной системе Windows. В конечном итоге он работает только при запуске зараженного файла в MS-DOS. Более того, в операционной системе Windows 95 этот вирус будет работать, только если вы завершите графическую оболочку Windows, оставив компьютер работать в режиме командной строки.

Вирусы, заражающие выполнимые файлы Windows

Данный класс вирусов на сегодня, пожалуй, один из самых немногочисленных. Возможно, это связано с тем, что люди, способные написать такие вирусы, имеют слишком высокую квалификацию, чтобы бесцельно тратить свое время.

В качестве примера вирусов для Windows мы рассмотрим вирусы Win.Vir14 (другие названия - WinVir или WVir), Win.Twitch (Twitch), Win.CyberTech, Win.Vik и Win.Lamer.

Вирус Win.Vir14 заражает выполнимые EXE-файлы в формате операционной системы Windows. Выполнимые файлы MS-DOS не заражаются. Когда пользователь запускает зараженное приложение, управление сразу получает вирус. Он просматривает файлы текущего каталога и заражает выполнимые файлы Windows. Вирус дописывает свой код к заражаемым файлам и увеличивает их размер.

Затем вирус восстанавливает запущенный файл, удаляя из него код вируса. После этого приложение завершается и управление сразу возвращается операционной системе. Сама зараженная программа не выполняется. Если пользователь попытается запустить это приложение еще раз, оно будет работать как обычно.

Внутри кода вируса содержатся две текстовые строки:

Virus_for_Windows v1.4

МК92

Вирус Win.Twitch значительно более сложный, чем WinVir. Когда пользователь запускает зараженный файл Windows, вирус оставляет в оперативной памяти компьютера работающий модуль, а затем выполняет настоящее приложение. Модуль, оставленный в памяти, вызывает периодическое подергивание изображения на экране монитора.

Из всех известных на сегодня вирусов Windows, наиболее опасен вирус Win.CyberTech. После запуска на компьютере программы, зараженной вирусом Win.CyberTech, он изменяет ядро операционной системы - модуль KERNEL. В зависимости от версии Windows и режима, в котором она работает, заражаются файлы KRNL386.EXE или KRNL286.EXE. Вирус перехватывает функцию WinExес, которая используется для запуска приложений Windows и заражает все запускаемые приложения.

После заражения очередного приложения, вирус определяет текущую дату и проверяет несколько условий:

Сегодня число между 29-м апреля и 1-м мая

Сегодня пятница и число от 1-го до 13-го

Сегодня число между 26-м и 31-м декабря

Сегодня 6-е марта и год после 1994

Если хотя бы одно из этих условий выполняется, вирус отображает на экране небольшую диалоговую панель с единственной кнопкой ОК. Когда пользователь нажмет кнопку, вирус начинает разрушать данные, записанные на жестком диске компьютера.

Вирус Win.Lamer - первый из известных нам вирусов Windows, который применяет для маскировки полиморфный механизм. Заражая очередное приложение, Win.Lamer изменяет свой код, чтобы затруднить антивирусным программам свое обнаружение.

Операционная система OS/2 и вирусы/2

В последнее время все большую популярность получает операционная система OS/2, разработанная известной фирмой IBM. С выходом в свет новой, полностью 32-разрядной мультизадачной версии этой операционной системы IBM OS/2 Warp, многие пользователи стали устанавливать ее на своих компьютерах.

На момент написания книги было известно всего несколько вирусов, предназначенных специально для операционной системы OS/2 - OS2Vir1, OS2.First, OS2.Jiskefet, OS2.Rexx.

Описание вируса OS2Vir1, которое мы обнаружили в справочной системе IBM AntiVirus, с трудом позволяет назвать его настоящим вирусом. Способность OS2Vir1 к

распространению ограничивается заражением EXE файлов, расположенных в текущем каталоге. Заражая выполнимый файл, OS2Vir1 записывает свой код в начало файла-жертвы, не сохраняя оригинальный код программы. Поэтому зараженная программа оказывается неработоспособной. Трудно предположить, что вирус, использующий такую технологию заражения, получит сколько-нибудь широкое распространение.

Вирусы OS2.First, OS2.Jiskefet, OS2.Rexx несколько сложнее. Они могут распространяться, сохраняя у заражаемых программ способность нормально работать. Все три известных нам вируса - OS2.First, OS2.Jiskefet и OS2.Rexx используют вызовы операционной системы DOS. Поэтому их нельзя назвать вирусами, полностью разработанными для операционной системы OS/2.

Автоматизированные средства разработки вирусов

Нет, мы не ошиблись, и это не типографская опечатка. В этом разделе речь действительно пойдет об автоматизированных средствах разработки вирусов. На сегодня в мире насчитывается больше десятка таких средств. С их помощью создание нового вируса становится не сложнее, чем создание нового документа в текстовом редакторе. Используя автоматизированные средства разработки вирусов, любой пользователь может создать собственный вирус буквально за пару минут.

Самые простые средства разработки работают в пакетном режиме - все настройки выполняются через обыкновенный текстовый файл. Результатом их работы является файл с исходным текстом вируса, написанного на языке ассемблера. Из этого “полуфабриката” легко получить готовый вирус, воспользовавшись транслятором с языка ассемблера.

Надо отметить, что исходный текст вируса может служить хорошим пособием для будущих писателей вирусов. Тем более, что обычно вместе со средствами разработки вирусов поставляется полная документация.

Более сложные автоматизированные средства разработки вирусов имеют продуманную диалоговую оболочку со множеством вложенных меню.

Вот только несколько названий автоматизированных средств разработки вирусов:

- *The Virus Construction Set (VCS)*
- *The Virus Creation Laboratory (VCL)*
- *The Phalcon/Skism Mass Produced Code generator (PS-MPC)*
- *The Instant Virus Production kit (IVP)*
- *The Second Generation in Virus Creation (G²)*

Лаборатория компьютерного оружия

Автоматизированные средства разработки дают хорошее представление о возможностях вирусов. Поэтому мы рассмотрим их более подробно на примере The Virus

Creation Laboratory (VCL). VCL представляет собой достаточно старую разработку. Она датирована 1992 годом:

Copyright (c) 1992 Nowhere Man and [NuKE] WaReZ
Version 1.00

Создание вируса при помощи VCL становится просто детской забавой. Программа имеет развитую диалоговую оболочку, содержащую многочисленные меню, окна и диалоговые панели.



Уровень сервиса, предоставляемый пользователю VCL, практически не поддается описанию. Например, для большего удобства в состав дистрибутива VCL входят PIF-файл для запуска из среды Windows и пиктограмма.

Любому, кто создает вирус при помощи VCL, достаточно задать в меню и диалоговых панелях его свойства. На рисунке 1.11 показано, как можно задать основные свойства будущего вируса. Обычные переключатели меню Options позволяют указать, какие типы файлов вирус должен поражать, будет ли он реализовывать алгоритмы самошифровки и защиты от отладки. Вы можете указать способ поиска новых жертв, насколько быстро вирус должен заражать файлы компьютера и т. д.

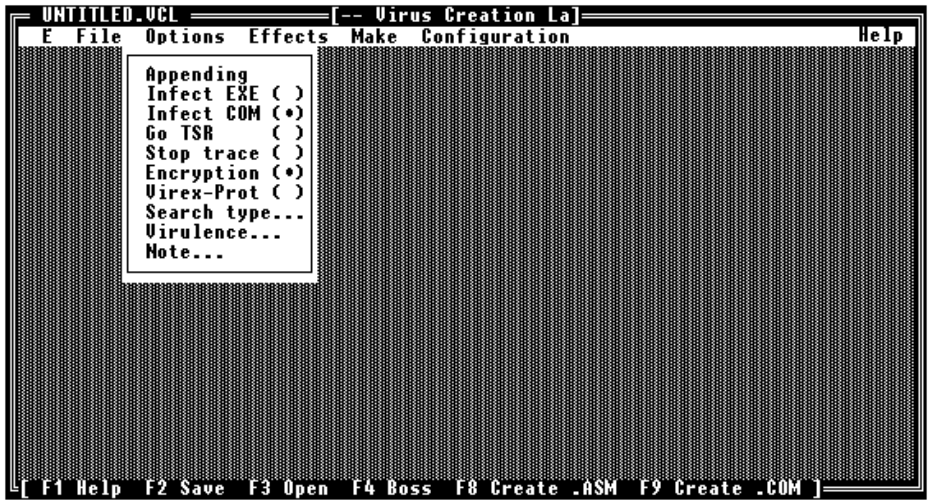


Рис. 1.11. Автоматизированные средства разработки вирусов

Большинство вирусов не только создают свои копии, заражая новые файлы и загрузочные секторы дисков, они также могут выполнять всевозможные действия. VCL легко позволяет подключить к вирусу вредоносные функции. Для этого предназначено меню Effects. Список действий, которые VCL позволяет встроить в вирус, представлен в таблице приведенной ниже. Прочитайте эту таблицу внимательно - ведь это список

признаков появления вируса на вашем компьютере! Конечно, список неполный, вирусы могут выполнять гораздо более сложные действия.

Эффект	Описание
Beep the PC speaker	Подать звуковой сигнал через встроенный динамик компьютера
Change low RAM	Изменить объем стандартной оперативной памяти
Clear the screen	Очистить экран монитора компьютера
Cold reboot	Выполнить холодную перезагрузку компьютера
Corrupt file(s)	Разрушить файлы с заданными именами
Disable LPT port	Отключить параллельный порт компьютера
Disable Print Screen	Отключить функцию печати содержимого экрана
Disable COM port	Отключить последовательный порт компьютера
Display a string	Вывести на экран заданную строку
Drop a program	Выполнить программу
Erase file(s)	Удалить файлы
Lock up the computer	Зациклить компьютер
Machine gun sound	Подать звук стреляющего пистолета
Out value to port	Вывести определенное значение в заданный порт компьютера
Out random to ports	Вывести случайное значение в заданный порт компьютера
Play a tune	Проиграть мелодию
Print a string	Напечатать на принтере текстовую строку
Drop to ROM BASIC	Запустить интерпретатор языка BASIC, записанный в ПЗУ компьютера
Send string to COM	Вывести строку в последовательный порт. Эту возможность можно использовать для программирования модемов
Swap two LPT ports	Поменять имена двух параллельных портов компьютера
Swap two COM ports	Поменять имена двух последовательных портов компьютера
Trash a disk	Испортить информацию в нескольких секторах на заданном диске
Trash some disks	Испортить информацию в нескольких секторах на каком-нибудь диске
Display an ANSI	Вывести на экран строку команд ANSI. Она может содержать такие команды как установка курсора в заданную позицию экрана, выбор цвета текста и цвета фона, отображение символов и т. д.

Warm reboot	Выполнить “теплую” перезагрузку компьютера
-------------	--

Создаваемый вирус может создавать несколько эффектов из приведенного списка. Те, кому этого недостаточно, могут подключить к вирусу собственные модули, определенные в ассемблерном файле.

Set Conditions

Boolean

ALL

Before/After

AFTER

Trigger Routine

Op

Value

CPU type

<=

386

Trigger Routine

Op

Value

DOS version

<

6

Trigger Routine

Op

Value

Number of floppies

>

1

Trigger Routine

Op

Value

Year

==

1997

Trigger Routine

Op

Value

Month

==

1

Рис. 1.12. Выбор условия для срабатывания вируса

Для каждого выбранного эффекта VCL позволяет выбрать условие его выполнения (рис. 1.12). Условия могут основываться на некоторых характеристиках компьютера и его программной среды. Следующая таблица содержит список параметров, которые могут проверять вирусы, созданные VCL.

Параметр	Описание
Country code	Код страны
CPU type	Тип центрального процессора компьютера
Day	Текущий день месяца
DOS version	Версия операционной системы
EMS memory	Объем расширенной памяти
Number of game ports	Количество игровых портов, установленных в компьютере
Hour	Текущий час
Number of floppies	Количество дисководов, подключенных к компьютеру
Minute	Текущая минута
Month	Текущий месяц
Number of LPT ports	Количество параллельных портов компьютера

RAM memory	Объем оперативной памяти
Random number	Случайное число
Clock rollover	Переполнение таймера
Second	Текущая секунда
Number of COM ports	Количество последовательных портов компьютера
Weekday	Текущий день недели
Year	Текущий год
All files infected	Инфицирование всех файлов
Under 4DOS	Работа в среде 4DOS

Когда все свойства заданы, для создания вируса достаточно нажать всего одну клавишу. По выбору вы можете получить исходный текст вируса на языке ассемблера или готовый к исполнению файл.

Исходный текст вируса на языке ассемблера, который создает VCL, имеет исчерпывающие комментарии, позволяющие в нем легко разобраться:

```
search_files  proc near
               mov  dx,offset com_mask ; DX points to "*.COM"
               call find_files          ; Try to infect a file
done_searching: ret                               ; Return to caller
com_mask      db  "*.COM",0                   ; Mask for all .COM files
search_files  endp
find_files     proc near
               push bp                         ; Save BP
               mov  ah,02Fh                    ; DOS get DTA function
               int  021h
```

К счастью, антивирусные программы могут достаточно хорошо обнаруживать вирусы, созданные при помощи автоматизированных средств разработки. Поэтому такие разработки скорее всего не смогут значительно распространиться и нанести большой вред.

Плохие програ ммы

К сожалению, не только вирусы мешают нормальной работе компьютера и его программному обеспечению. Принято выделять еще, по крайней мере, три вида вредоносных программ. К ним относятся программы-черви, троянские программы и логические бомбы. Четкого разделения на эти виды не существует, троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т. д.

Троянские программы

Все знакомы с греческим мифом о том, как была завоевана неприступная Троя. Греки оставили ночью у ворот Трои деревянного коня, внутри которого притаились солдаты.

Когда горожане, движимые любопытством, втащили коня за стены города, солдаты вырвались наружу и завоевали город.

Троянские программы действуют подобным образом. Их основное назначение совершенно безобидное или даже полезное. Но когда пользователь запишет программу в свой компьютер и запустит ее, она может незаметно выполнять другие, недокументированные функции.

Часто троянские программы используются для первоначального распространения вирусов. Такая программа записывается автором на станцию BBS, и оттуда загружается ничего не подозревающими пользователями на свои компьютеры. Когда пользователь запустит ее, она, помимо выполнения маскирующей функции, заражает компьютер вирусом.

После того как троянская программа выполнит свою скрытую функцию, она может самоуничтожиться, чтобы затруднить обнаружение причины нарушений в работе системы.

Логические бомбы

Логической бомбой называется программа или ее отдельные модули, которые при выполнении определенного условия выполняют несанкционированные действия. Логическая бомба может сработать по достижении определенной даты, когда в базе данных появится или исчезнет запись и т. д. Условие, при котором бомба срабатывает, определяется ее создателем. Логическая бомба может быть встроена в вирусы, троянские программы или в обыкновенное программное обеспечение.

Широко известен случай, когда программист, разрабатывающий бухгалтерскую систему, заложил в нее логическую бомбу. Она периодически проверяла ведомости на получение зарплаты и когда из нее исчезла фамилия создателя программы, бомба уничтожила всю систему.

Логические бомбы используются шантажистами. Через определенное время, после того как программист,строивший логическую бомбу, покидает компанию, она может полностью разрушить систему. Шантажист сообщает руководству компании, что в систему заложена логическая бомба и он может ее удалить (за определенную плату).

Программы-черви

Программы-черви нацелены их авторами на выполнение определенной функции. Они могут быть ориентированы на проникновение в систему и модификацию некоторых данных.

Можно создать программу-червь, подсматривающую пароль для доступа к банковской системе и изменяющую базу данных таким образом, чтобы на счет программиста была переведена большая сумма денег.

Самая известная программа-червь написана студентом Корнельского (Cornell) университета Робертом Моррисом (Robert Morris). Червь был запущен второго ноября

1988 года в сеть Internet. За пять часов червь Морриса смог проникнуть на более чем 6000 компьютеров, подключенных к сети.

Очень сложно узнать, является ли программа троянской и заложена ли в нее логическая бомба. Программист имеет полную власть над своим детищем. Изучение сомнительной программы или системы может занять очень много времени и потребовать значительных финансовых затрат.

Мы не рекомендуем копировать к себе программы с BBS, обмениваться программным обеспечением со своими знакомыми и приобретать незаконные копии фирменного программного обеспечения. В любую из этих программ могут быть встроены дополнительные вредоносные функции и их использование приведет к нарушению работы вашей компьютерной системы.

Как происходит заражение

Как вирусы попадают в компьютер? Вы обязательно должны уяснить себе этот вопрос, чтобы по возможности перекрыть все возможные каналы поступления новых вирусов.

К счастью, вирус не может просто так появиться на компьютере (если, конечно, вы сами не разрабатываете его). Когда незараженный компьютер полностью изолирован от внешнего мира - от него отключены дисководы, он не подключен к локальной сети и в нем не установлен модем, вирус не может попасть в такой компьютер.

Компьютерный вирус не появится от того, что вы оставили на ночь открытой форточку и устроили сквозняк. Дождь и снег за окном также не могут служить источником возникновения компьютерного вируса.

Чтобы вирус проник на компьютер, необходимо, чтобы последний выполнил зараженную программу или загрузился с зараженной дискеты. Наиболее часто вирусы попадают в компьютер вместе с пиратским программным обеспечением, программами Freeware и Shareware.

Вот основные пути, по которым вирусы проникают в компьютер:

- *получение программ с электронной доски объявлений и через глобальные сети;*
- *обмен дискетами и программами ;*
- *проникновение вируса из локальной сети*

Мы не можем сейчас предусмотреть все возможные пути проникновения вирусов в компьютер. Так, например, совсем недавно появился новый вид вирусов, распространяющихся через файлы документов текстового процессора Microsoft Word for Windows. После этого даже казавшееся ранее абсолютно безопасным копирование документов несет в себе опасность заражения.

Использование пиратского программного обеспечения

Незаконное использование программного обеспечения, при котором оно многократно копируется многими людьми, легко позволяет вирусам распространяться от компьютера к компьютеру. В нашей стране, да и во всем мире, пиратское копирование программ широко распространено.

Быстрее всего вирусы распространяются, заражая выполнимые файлы компьютерных игр. Немногие могут удержаться, чтобы не скопировать у хорошего знакомого новую версию популярной игры, просто переписав на свои дискеты все ее файлы. Затем кто-нибудь перепишет игру у вас и так далее и так далее... Если на одном из компьютеров этой цепочки находится вирус, и он заразит выполнимые файлы игры, то все остальные любители развлечений также получат вирус.

Только в случае законного использования программ вы можете быть спокойны за то, что не получите вирус или троянскую программу. В крайнем случае, у вас будет кому выдвинуть претензии.

Тем не менее, известны случаи, когда даже фирменное программное обеспечение содержало в себе вирус, поэтому вы всегда должны внимательно относиться к проблеме антивирусной защиты компьютера.

Широкое использование программ Freeware и Shareware

Помимо фирменного программного обеспечения существуют так называемые бесплатные (Freeware) и условно бесплатные (Shareware) программы. Вы можете свободно копировать и использовать такое программное обеспечение. Программы Shareware отличаются от Freeware тем, что если вы используете их дольше определенного срока и они вам понравились, вы должны отправить их создателю небольшое количество денег, обычно от пяти до двадцати американских долларов.

В качестве Shareware распространяются программы архиваторы, например архиватор ARJ, различные графические пакеты и другие мелкие полезные программы.

Для того чтобы файловый вирус проник в компьютер, достаточно запустить зараженную программу с дискеты или с сетевого диска

Несмотря на свою привлекательность, программное обеспечение Freeware и Shareware может послужить для проникновения вирусов. Это происходит вследствие того, что программы Freeware и Shareware поступают конечному пользователю через длинную цепочку копирований. Существует вероятность, что во время такого копирования программа может быть заражена вирусом.

Поэтому следует по возможности избегать бесплатных и условно бесплатных программ. Особенно это касается тех случаев, когда компьютер используется для выполнения ответственных задач.

Электронная доска объявлений и глобальные сети

За последние несколько лет широкое распространение получили так называемые электронные доски объявлений (Bulletin Board System - BBS). BBS - это компьютер, снабженный одним или несколькими модемами, на котором выполняется специальная почтовая программа. Эта программа позволяет пользователям удаленных компьютеров связываться с BBS по телефонным линиям и выполнять обмен сообщениями и файлами.

Каждый обладатель модема может позвонить на BBS со своего компьютера, записать на нее или считать себе любые файлы. Таким образом, на BBS может попасть программа, зараженная вирусом, троянская программа или программа-червь.

Правила пользования различными BBS могут значительно отличаться друг от друга. Для некоторых BBS запрещена запись новых файлов. Пользователь может только загрузить файлы с BBS и обмениваться текстовыми сообщениями. На других BBS, наоборот, поощряется запись пользователями новых файлов. От объема записанных пользователем файлов зависит, какой объем файлов пользователь может получить для себя.

Несмотря на то, что все вновь загруженные файлы должны, по идее, проверяться системным оператором BBS на вирусы, иногда они этого могут не делать. Даже если проверка осуществляется, новые вирусы, не известные антивирусным программам, используемым системным оператором BBS, могут остаться незамеченными. В случае, когда на BBS загружена троянская программа, проверка антивирусными программами скорее всего ничего не даст.

Многие авторы вирусов специально записывают на BBS зараженные программы, чтобы инициировать таким образом распространение своего детища. Однако совсем не обязательно, что зараженная программа записана на BBS специально. Возможно тот, кто ее записал, сам не знал о наличии вируса.

Другие пользователи, которые переписут с BBS на диски своего компьютера зараженную программу, получают вместе с ней вирус.

Следует помнить, что не только выполнимые файлы могут быть заражены вирусами. Даже текстовый файл в формате Microsoft Word for Windows может содержать в себе вирус.

Любой файл, содержащий в себе выполнимые инструкции, будь то команды центрального процессора или программы, написанные на языке макрокоманд, могут содержать вирус

Если вам все же приходится использовать в своей работе программы, полученные с BBS, необходимо в обязательном порядке проверять их на наличие вирусов.

Обмен дискетами

Ваш компьютер подвергается опасности заражения вирусами не только когда вы записываете себе выполнимые файлы и файлы документов, содержащие макрокоманды.

Загрузочные вирусы могут проникнуть в компьютер, когда он загружается с зараженной дискеты. Подчеркнем, что зараженная дискета не обязательно должна быть системной, то есть содержать файлы операционной системы. Загрузочный вирус может быть на любой дискете.

Обычно это происходит, когда вы случайно оставляете дискету в дисковом, а затем перезагружаете компьютер. Во время первоначальной загрузки компьютер считывает загрузочную запись с дискеты и передает ей управление. Если дискета заражена, вирус сразу получает управление и заражает жесткий диск компьютера. Теперь даже после выключения питания компьютера и загрузки его с жесткого диска вирус будет активизирован.

Файловые вирусы получают управление при запуске зараженного файла. Возможно, что работая на компьютере, вы не запустите ни одного зараженного файла и вирус так и не получит управления. Загрузочный вирус выполняется каждый раз, когда вы загружаете компьютер.

Сама по себе зараженная загрузочным вирусом дискета не представляет непосредственной опасности. Вы можете вставить ее в компьютер, скопировать с нее любые файлы или записать новые файлы с жесткого диска компьютера. Вирус при этом не сможет заразить компьютер. Только загрузка с дискеты позволяет вирусу активизироваться.

Базовая система ввода/вывода (Basic Input Output System - BIOS) большинства современных компьютеров позволяет установить порядок загрузки операционной системы. Если вы укажете, что операционная система должна загружаться сначала (или только) с жесткого диска, загрузочный вирус не проникнет к вам с зараженной дискеты, даже если вы случайно оставите ее в дисковом. Чтобы установить порядок загрузки операционной системы, надо запустить программу BIOS Setup, а затем руководствоваться описанием системной платы компьютера.

Однако мы не советуем вам специально экспериментировать с зараженными дискетами и копировать с них выполнимые файлы. Многие файлово-загрузочные вирусы могут также распространяться, заражая обычные выполнимые файлы. Такой вирус может заразить загрузочные секторы жесткого диска при запуске обычной программы.

Известны случаи, когда загрузочный вирус был обнаружен на отформатированных дискетах, только что купленных в магазине. Вирус попал на них еще на заводе, во время форматирования новых дискет.

Вирусы на компакт-дисках

В настоящее время все большее распространение получают устройства чтения компакт-дисков. Эти устройства позволяют читать специальные диски, объем которых составляет больше 600 Мбайт. Постоянное снижение цены на устройства чтения компакт-дисков и их совершенствование позволяют предположить, что в скором времени все компьютеры будут оснащены таким устройством.

К сожалению, записать информацию на компакт-диск значительно сложнее, чем прочитать. Существует две технологии их изготовления. Принципиальное различие между ними состоит в количестве дисков, которые можно изготовить за определенное время. Ни одна из этих технологий не позволяет стирать уже записанные данные и записывать на их место другие.

Первая технология предполагает наличие сложного технологического оборудования. Заготовки для таких дисков изготавливаются на основе алюминия и имеют крайне низкую стоимость, но запись на них информации окупается только при больших тиражах. Поэтому на алюминиевых дисках обычно выпускают дистрибутивы современного программного обеспечения, сложные игры, энциклопедии, то есть все, что находит широкий спрос.

Вторая технология позволяет изготавливать единичные экземпляры компакт-дисков, но устройства для их записи значительно дешевле и подключаются к компьютеру как дисковод. Сами же заготовки дисков выполняются с напылением золота и стоят дороже алюминиевых.

Файлы, записанные на компакт-дисках, могут быть заражены вирусами. Но в отличие от жестких дисков и дискет, это может случиться только если файл был заражен и записан на компакт-диск уже зараженным. Последующее использование компакт-диска не вызовет его заражения ни в каком случае, даже если компьютер, на котором вы работаете, забит вирусами до отказа. Секрет прост - обычные устройства чтения компакт-дисков физически не могут записывать данные на диск, и предназначены только для чтения.

Тем не менее вирус может находиться на компакт-диске. Это происходит в том случае, когда фирма, подготовившая компакт-диск к выпуску, не позаботилась о антивирусной безопасности и вирус заразил файл перед записью его на диск.

Особенно внимательно следует обращаться с пиратскими (не лицензионными) компакт-дисками, выпущенными подпольно. Никто не даст вам гарантию, что на них нет вирусов.

Большинство антивирусных программ позволяют проверить компакт-диск на вирусы. Следует только иметь в виду, что если вирус обнаружен, вылечить такой файл непосредственно на компакт-диске невозможно. В качестве одного из вариантов вы можете скопировать зараженный файл к себе на жесткий диск и сразу вылечить его с помощью антивирусной программы. Пользоваться можно только этим вылеченным файлом.

Проникновение вируса из локальной сети

Широкие возможности обмена данными, которые предоставляют локальные сети, позволяют вирусам распространяться с огромной скоростью. Мы посвятили локальным сетям отдельную главу. А сейчас отметим только, что вирус может проникнуть на

компьютер, подключенный к локальной сети, когда пользователь копирует себе файлы из сети или просто запускает программы из сетевых каталогов.

2 КАК С НИМИ БОРОТЬСЯ

Не надо ждать, пока вирусы зарадят ваш компьютер и успеют испортить хранимые в нем данные. Чем раньше начнется подготовка к нападению вирусов - тем лучше. Правильно организованная защита позволит сразу обнаружить появившийся вирус и он не сможет нанести программному обеспечению и вашим данным большого урона.

Основным средством борьбы с вирусами остаются антивирусные программы. В этой главе мы приведем основные сведения об антивирусных программах, приведем несколько примеров их использования.

Однако даже без применения антивирусных программ можно постараться предотвратить проникновение вирусов в компьютер и постараться уменьшить вред, который они нанесут в случае заражения.

Для тех, кто не смог уберечь свой компьютер от вирусов, мы дадим советы, как предотвратить дальнейшее распространение вируса и удалить его, максимально сохранив свои данные.

Методы обнаружения вирусов

Вы можете пользоваться антивирусным программным обеспечением, не имея представления о том, как оно устроено. Однако, в настоящее время существует очень много антивирусных программ, так что вам так или иначе придется на чем-то остановить свой выбор. Чтобы этот выбор был по возможности обоснован и установленные программы обеспечивали максимальную степень защиты от вирусов, необходимо изучить методики, применяемые этими программами.

Существует несколько основополагающих методик обнаружения и защиты от вирусов. Антивирусные программы могут реализовывать только некоторые методики или их комбинации.

- *Сканирование*
- *Обнаружение изменений*
- *Эвристический анализ*
- *Резидентный мониторинг*
- *Вакцинирование программ*
- *Аппаратная защита от вирусов*

Кроме того, большинство антивирусных программ обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов.

Объекты заражения

В первой главе мы уже рассказали о различных типах вирусов и о способах их распространения. Перед тем как приступить к рассмотрению антивирусных средств, перечислим области файловой системы компьютера, которые подвергаются заражению вирусами и которые необходимо проверять:

- *Выполнимые файлы программ, драйверов*
- *Главная загрузочная запись и загрузочные секторы*
- *Файлы конфигурации AUTOEXEC.BAT и CONFIG.SYS*
- *Документы в формате текстового процессора Microsoft Word for Windows*

Когда резидентный вирус становится активным, он помещает свой постоянно работающий модуль в оперативной памяти компьютера. Поэтому антивирусные программы должны выполнять проверку оперативной памяти. Так как вирусы могут использовать не только стандартную память, то желательно выполнять проверку верхней памяти. Например, антивирус Doctor Web проверяет первые 1088 Кбайт оперативной памяти.

Сканирование

Самая простая методика поиска вирусов, заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Определение сигнатуры вируса довольно сложная задача. Сигнатура не должна содержаться в нормальных программах, не зараженных данным вирусом. В противном случае возможны ложные срабатывания, когда вирус обнаруживается в совершенно нормальной, не зараженной программе.

Конечно, программам-сканерам не обязательно хранить в себе сигнатуры всех известных вирусов. Они могут, например, хранить только контрольные суммы сигнатур.

Антивирусные программы-сканеры, которые могут удалить обнаруженные вирусы, обычно называются полифагами. Самой известной программой-сканером является Aidtest Дмитрия Лозинского. Aidtest выполняет поиск вирусов по их сигнатурам. Поэтому он обнаруживает только простейшие полиморфные вирусы.

В первой главе мы рассказывали о так называемых шифрующихся и полиморфных вирусах. Полиморфные вирусы полностью изменяют свой код при заражении новой программы или загрузочного сектора. Если вы выделите два экземпляра одного и того же полиморфного вируса, то они могут не совпадать ни в одном байте. Как следствие, для таких вирусов невозможно определить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

Антивирусные программы-сканеры могут обнаружить только уже известные вирусы, которые были предварительно изучены и для которых была определена сигнатура. Таким образом, использование программ-сканеров не защищает ваш компьютер от проникновения новых вирусов.

Для эффективного использования антивирусных программ, реализующих метод сканирования, необходимо постоянно обновлять их, получая самые последние версии.

Эвристический анализ

Эвристический анализ является относительно новым методом в обнаружении вирусов. Он позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе, как этого требует метод обнаружения изменений.

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаются обнаружить в них код, характерный для вирусов. Так например, эвристический анализатор может обнаружить, что в проверяемой программе присутствует код, устанавливающий резидентный модуль в памяти.

Антивирусная программа Doctor Web, входящая в состав комплекта АО “ДиалогНаука”, имеет мощный эвристический анализатор, позволяющий обнаружить большое количество новых вирусов.

Если эвристический анализатор сообщает, что файл или загрузочный сектор возможно заражен вирусом, вы должны отнестись к этому с большим вниманием. Желательно исследовать такие файлы с помощью самых последних версий антивирусных программ или направить их для детального изучения в АО “ДиалогНаука”.

В комплект IBM AntiVirus входит специальный модуль, ориентированный на обнаружение вирусов в загрузочных секторах. Этот модуль использует запатентованную технологию (patent-pending neural network technology from IBM) эвристического анализа и позволяет определить, заражен ли загрузочный сектор вирусом.

Обнаружение изменений

Когда вирус заражает компьютер, он обязательно делает изменения на жестком диске, например, дописывает свой код в выполнимый файл, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник.

Антивирусные программы могут предварительно запомнить характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверять их (отсюда происходит их название программы-ревизоры). Если будет обнаружено изменение, тогда возможно что на компьютер напал вирус.

Обычно программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов, а также информацию о структуре каталогов и номера плохих

кластеров диска. Могут проверяться и другие характеристики компьютера - объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Программы-ревизоры могут обнаружить большинство вирусов, даже тех, которые ранее не были известны. Вирусы, заражающие файлы программ только при их копировании, ревизоры как правило обнаружить не могут, так как они не знают параметров файла, которые были до копирования.

Однако следует учитывать, что не все изменения вызваны вторжением вирусов. Так, загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают внутри своего исполнимого файла данные. Командные файлы изменяются еще чаще, например, файл AUTOEXEC.BAT обычно изменяется во время установки нового программного обеспечения.

Программы-ревизоры не помогут и в том случае, когда вы записали в компьютер новый файл, зараженный вирусом. Правда, если вирус заразит другие программы, уже учтенные ревизором, он будет обнаружен.

Простейшая программа-ревизор Microsoft Anti-Virus (MSAV) входит в состав операционной системы MS-DOS. Основным, и возможно единственным ее достоинством является то, что на нее не нужно дополнительно тратить деньги.

Значительно более развитые средства контроля предоставляет программа-ревизор Advanced Diskinfoscope (ADInf), входящая в состав антивирусного комплекта АО “ДиалогНаука”. Более подробно мы рассмотрим эти средства в следующем разделе, а сейчас только заметим, что вместе с ADInf вы можете использовать лечащий модуль ADInf Cure Module (ADInfExt). ADInf Cure Module использует собранную ранее информацию о файлах для восстановления их после поражения неизвестными вирусами.

Конечно, не все вирусы могут быть удалены ADInf Cure Module и другими программными средствами, основанными на контроле и периодической проверке компьютера. Например, если новый вирус шифрует диск, как это делает вирус OneHalf, тогда его удаление без расшифровки диска скорее всего приведет к потере информации. Вирусы такого типа могут быть удалены только после внимательного изучения специалистами и включения модулей для борьбы с ними в обычные полифаги - Aidstest или Doctor Web.

Известные нам на момент написания книги антивирусные программы-ревизоры непригодны для обнаружения вирусов в файлах документов, так как они по своей сути постоянно изменяются. Ряд программ после внедрения в них кода вакцины перестают работать. Поэтому для контроля за ними следует использовать программы-сканеры или эвристический анализ.

Резидентные мониторы

Существует еще целый класс антивирусных программ, которые постоянно находятся в оперативной памяти компьютера, и отслеживают все подозрительные действия,

выполняемые другими программами. Такие программы носят название резидентных мониторов или сторожей.

Резидентный монитор сообщит пользователю, если какая-либо программа попытается изменить загрузочный сектор жесткого диска или дискеты, выполнимый файл. Резидентный монитор сообщит вам, что программа пытается оставить в оперативной памяти резидентный модуль и т. д.

Большинство резидентных мониторов позволяют автоматически проверять все запускаемые программы на заражение известными вирусами, то есть выполняют функции сканера. Такая проверка будет занимать некоторое время и процесс загрузки программы замедлится, но зато вы будете уверены, что известные вирусы не смогут активизироваться на вашем компьютере.

К сожалению, резидентные мониторы имеют очень много недостатков, которые делают этот класс программ малопривлекательными для использования.

Многие программы, даже не содержащие вирусов, могут выполнять действия, на которые реагируют резидентные мониторы. Например, обычная команда LABEL изменяет данные в загрузочном секторе и вызывает срабатывание монитора.

Поэтому работа пользователя будет постоянно прерываться раздражающими сообщениями антивируса. Кроме того, пользователь должен будет каждый раз решать, вызвано ли это срабатывание вирусом или нет. Как показывает практика, рано или поздно пользователь отключает резидентный монитор.

И наконец, самый маленький недостаток резидентных мониторов заключается в том, что они должны быть постоянно загружены в оперативную память и, следовательно, уменьшают объем памяти, доступной другим программам.

В составе операционной системы MS-DOS уже есть резидентный антивирусный монитор VSafe.

Вакцинирование программ

Для того, чтобы человек смог избежать некоторых заболеваний, ему делают прививку. Существует способ защиты программ от вирусов, при котором к защищаемой программе присоединяется специальный модуль контроля, следящий за ее целостностью. При этом может проверяться контрольная сумма программы или какие-либо другие характеристики. Когда вирус заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

Увы, в отличие от прививок человеку, вакцинирование программ во многих случаях не спасает их от заражения. Стелс-вирусы легко обманывают вакцину. Зараженные файлы работают также как обычно, вакцина не обнаруживает заражения. Поэтому мы не станем останавливаться на вакцинах и продолжим рассмотрение других средств защиты.

Аппаратная защита от вирусов

На сегодняшний день одним из самых надежных способов защиты компьютеров от нападений вирусов являются аппаратно-программные средства. Обычно они

представляют собой специальный контроллер, вставляемый в один из разъемов расширения компьютера и программное обеспечение, управляющее работой этого контроллера.

Благодаря тому, что контроллер аппаратной защиты подключен к системной шине компьютера, он получает полный контроль над всеми обращениями к дисковой подсистеме компьютера. Программное обеспечение аппаратной защиты позволяет указать области файловой системы, которые нельзя изменять. Вы можете защитить главную загрузочную запись, загрузочные сектора, выполнимые файлы, файлы конфигурации и т. д.

Если аппаратно-программный комплекс обнаружит, что какая-либо программа пытается нарушить установленную защиту, он может сообщить об этом пользователю и заблокировать дальнейшую работу компьютера.

Аппаратный уровень контроля за дисковой подсистемой компьютера не позволяет вирусам замаскировать себя. Как только вирус проявит себя, он сразу будет обнаружен. При этом совершенно безразлично, как работает вирус и какие средства он использует для доступа к дискам и дискетам.

Аппаратно-программные средства защиты позволяют не только защитить компьютер от вирусов, но также вовремя пресечь работу троянских программ, нацеленных на разрушение файловой системы компьютера. Кроме того аппаратно-программные средства позволяют защитить компьютер от некавалифицированного пользователя и злоумышленника, они не дадут ему удалить важную информацию, отформатировать диск, изменить файлы конфигурации.

В настоящее время в России серийно производится только аппаратно-программный комплекс Sheriff. Он надежно предотвратит заражение компьютера, позволит пользователю тратить значительно меньше времени на антивирусный контроль компьютера обычными программными средствами.

За рубежом производится намного больше средств аппаратно-программной защиты, но их цена значительно выше, чем у Sheriff и составляет несколько сотен американских долларов. Вот несколько названий таких комплексов:

Наименование комплекса	Изготовитель
Virustrap	JAS Technologies of the Americas
C:Cure	Leprechaun Software International
V-Card	Digital Enterprises
Thunderbyte	Glynn International
Immune	Swabian Electronics Reutlingen
VIRUS BUSTER	Telstar Electronics
ExVira	Bugovics & Partner

Помимо выполнения своей основной функции, аппаратно-программные средства защиты компьютера могут обеспечивать различный дополнительный сервис. Они могут управлять разграничением прав доступа различных пользователей к ресурсам компьютера - жестким дискам, дисководам и т. д.

Защита, встроенная в BIOS компьютера

Многие фирмы, выпускающие системные платы компьютеров, стали встраивать в них простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. В случае, если любая программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение. При этом он может разрешить это изменение или запретить его.

Однако, такой контроль нельзя назвать настоящим контролем на аппаратном уровне. Программный модуль, отвечающий за контроль доступа к загрузочным секторам, находится в ПЗУ BIOS и может быть обойден вирусами, если они заменяют загрузочные секторы, обращаясь непосредственно к портам ввода/вывода контроллера жестких и гибких дисков.

Существуют вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

Вирусы Tchechen.1912 и 1914

Очень опасные резидентные шифрованные вирусы. Пытаются найти в ПЗУ BIOS те строки Megatrends и AWARD. Если поиск закончился успешно, они считают, что в компьютере установлен BIOS фирм AWARD или AMI, отключают контроль за загрузочными секторами и заражают главную загрузочную запись жесткого диска. Примерно через месяц после заражения вирус удаляет информацию со всего первого жесткого диска

Самое простое средство аппаратной защиты - отключить от компьютера все каналы, через которые в него может проникнуть вирус. Если компьютер не подключен к локальной сети и в нем не установлен модем, то достаточно отключить накопители на гибких дисках и основной канал поступления вирусов в компьютер будет перекрыт.

Однако такое отключение далеко не всегда возможно. В большинстве случаев пользователю для нормальной работы необходим доступ к дисководам или модемам. Кроме того, зараженные программы могут проникнуть в компьютер через локальную сеть или компакт-диск, а их отключение значительно сузит область применения компьютера.

Методы удаления вирусов

Обнаружить вирус на компьютере – это только половина дела. Теперь его необходимо удалить. В большинстве случаев антивирусные программы, которые обнаруживают вирус, могут его удалить. Существуют две основные методики, используемые антивирусными программами для удаления вирусов.

Если вы обнаружили вирус, проверяя выполнимые файлы, с расширениями имени COM и EXE, следует проверить все другие типы файлов, в которых содержится исполнимый код. В первую очередь это файлы с расширением SYS, OVL, OVI, OVR, BIN, BAT, BIN, LIB, DRV, BAK, ZIP, ARJ, PAK, LZH, PIF, PGM, DLL, DOC

Вы даже можете проверить вообще все файлы на жестких дисках компьютера. Возможно кто-нибудь переименовал зараженный исполнимый файл, изменив его расширение. Например, файл EDITOR.EXE переименовали в EDITOR.EX_. Такой файл проверен не будет. Если впоследствии его переименуют обратно, вирус снова сможет активизироваться и распространиться в компьютере

Первая, наиболее распространенная методика предусматривает, что антивирусная программа удаляет уже известный вирус. Чтобы вирус мог быть правильно удален, необходимо чтобы он был изучен, разработан алгоритм его лечения и этот алгоритм был реализован в новой версии антивируса.

Вторая методика позволяет восстанавливать файлы и загрузочные секторы, зараженные ранее неизвестными вирусами. Для этого антивирусная программа заранее, до появления вирусов, должна проанализировать все выполняемые файлы и сохранить о них много разнообразной информации.

При последующих запусках антивирусной программы она повторно собирает данные о выполняемых файлах и сверяет ее с данными, полученными ранее. Если обнаруживаются несоответствия, то возможно файл заражен вирусом.

В этом случае антивирус пытается восстановить зараженный файл, используя для этого сведения о принципах внедрения вирусов в файлы и информацию о данном файле, полученную до его заражения.

Некоторые вирусы заражают файлы и загрузочные секторы, замещая своим кодом часть заражаемого объекта, то есть безвозвратно уничтожая заражаемый объект. Файлы и загрузочные секторы, зараженные такими вирусами, не могут быть вылечены по первой методике, но как правило могут быть восстановлены по второй методике. Если восстановить зараженные выполнимые файлы с помощью антивирусных программ не получается, вы должны будете восстановить их с дистрибутива или резервной копии или просто удалить (если они не нужны).

С главной загрузочной записью и загрузочными секторами дело обстоит несколько сложнее. Если антивирусная программа не в состоянии восстановить их в автоматическом режиме, вы должны будете сделать это вручную, воспользовавшись командами FDISK, SYS, FORMAT. Ручное восстановление загрузочных секторов будет описано несколько позже, в шестой главе.

Существует целая группа вирусов, которые, заражая компьютер, становятся частью его операционной системы. Если вы просто удалите такой вирус, например восстановив зараженный файл с дискеты, то система может стать частично или полностью неработоспособной. Такие вирусы надо лечить пользуясь первой методикой.

В качестве примера таких вирусов можно привести загрузочные вирусы OneHalf и группу вирусов VolGU.

Во время загрузки компьютера вирус OneHalf постепенно шифрует содержимое жесткого диска. Если вирус находится резидентным в памяти, то он перехватывает все обращения к жесткому диску. В случае, когда какая-либо программа пытается считать уже зашифрованный сектор, вирус расшифровывает его. Если вы удалите вирус OneHalf, информация на зашифрованной части жесткого диска станет недоступной.

Вирус VolGU не шифрует данные, но он не менее опасен, чем OneHalf. Каждый сектор жесткого диска хранит не только данные, записанные в нем, он также содержит дополнительную проверочную информацию. Она представляет собой контрольную сумму всех байт сектора. Эта контрольная сумма используется для проверки сохранныости информации.

Обычно, когда программа обращается к дисковой подсистеме компьютера, считываются и записываются только данные, контрольная сумма корректируется автоматически. Вирус VolGU, перехватывает обращения всех программ к жесткому диску и при записи данных на диск портит контрольные суммы секторов.

Когда вирус активен, он позволяет считывать секторы с неправильной контрольной суммой. Если просто удалить такой вирус, тогда секторы с неправильной контрольной суммой читаться не будут. Операционная система сообщит вам о ошибке чтения с жесткого диска (сектор не найден).

Подготовка к вирусной атаке

Пользователи компьютеров должны заблаговременно подготовиться к возможной атаке вирусов, а не ждать до последней минуты, когда вирус уже появится. Благодаря этому вы сможете быстрее обнаружить вирус и удалить его.

В чем же должна заключаться такая подготовка?

- ♦ *Заранее подготовьте системную дискету. Запишите на нее антивирусные программы-полифаги, например Aidstest и Doctor Web*

- ♦ *Постоянно обновляйте версии антивирусных программ, записанных на системной дискете*
- ♦ *Периодически проверяйте компьютер при помощи различных антивирусных средств. Контролируйте все изменения на диске с помощью программы-ревизора, например ADInf. Новые и изменившиеся файлы проверяйте программами-полифагами Aidstest и Doctor Web*
- ♦ *Проверяйте все дискеты перед использованием. Для проверки применяйте как можно более поздние версии антивирусных программ*
- ♦ *Проверяйте все выполнимые файлы, записываемые на компьютер*
- ♦ *Если вам нужен высокий уровень защиты от вирусов, установите в компьютер аппаратный контроллер защиты, например Sheriff. Совместно с использованием аппаратного контроллера и традиционных антивирусных средств позволяют максимально обезопасить вашу систему*

Создание системной дискеты

Обычно в компьютере установлены два накопителя на гибких магнитных дисках. Один - для дискет размером 5.25 дюйма, а второй для дискет размером 3.5 дюйма. Операционная система MS-DOS, а также операционные системы Windows, Windows 95, Windows NT и OS/2 присваивают им имена A: и B:. Какой из дисководов имеет имя A:, а какой B:, зависит от аппаратуры компьютера.

Как правило, пользователь может изменить имена дисководов. Для этого необходимо открыть корпус компьютера и переключить несколько разъемов. Если есть такая возможность, то эту работу следует доверить техническому специалисту.

Накопители на магнитных дисках размером 5.25 дюйма постепенно выходят из употребления, поэтому в новых компьютерах устанавливают только один накопитель на гибких магнитных дисках, рассчитанный на дискеты размера 3.5 дюйма. В этом случае он имеет имя A:, диск B: отсутствует.

Загрузить компьютер с помощью системной дискеты можно только с дисковода A:. Таким образом, для изготовления системной дискеты к своему компьютеру вы должны взять дискету соответствующего размера.

Существует множество программ, позволяющих подготовить системную дискету. Такие программы входят в состав всех операционных систем - MS-DOS, Windows 3.1, Windows 95 и OS/2 и др.

Самыми простыми программами для подготовки системных дискет являются команды FORMAT или SYS, входящие в состав операционных систем MS-DOS и Windows 95 и поэтому в первую очередь мы опишем именно их.

Использование команды FORMAT

Команда FORMAT выполняет форматирование дискеты и может записать на нее файлы операционной системы. При форматировании гибких дисков FORMAT выполняет разметку дорожек на дискете, и формирует системные области - загрузочный сектор, таблицу размещения файлов и корневой каталог.

Во время форматирования дискеты вся информация, записанная на ней, стирается. Так как FORMAT заново записывает на дискету загрузочный сектор, то если она ранее была заражена загрузочным вирусом, вирус удаляется. Можно сказать, что команда FORMAT выполняет основную функцию антивируса - удаляет с дискеты любые вирусы.

При вызове команды FORMAT можно задать большое количество различных параметров. Их описание вы можете найти в четвертом томе серии “Персональный компьютер - шаг за шагом”, который называется “Что вы должны знать о своем компьютере”. В этой книге мы опишем только несколько самых необходимых нам параметров:

FORMAT drive: [/S] [/U] [/Q]

В качестве параметра drive вы должны задать имя дисководов, который будет форматировать дискету. Параметр /S означает, что после форматирования дискеты на нее переносятся основные файлы операционной системы и дискета становится системной. Для подготовки системной дискеты следует обязательно указать этот параметр.

Как мы говорили, команда FORMAT удаляет с формируемой дискеты все записанные на ней файлы. Обычно FORMAT записывает на дискете скрытую информацию, позволяющую в случае необходимости восстановить удаленные с нее файлы.

|| Для восстановления файлов, удаленных во время выполнения
|| форматирования дискеты, используйте команду UNFORMAT

Если вы твердо уверены, что восстанавливать их не придется, можно ускорить форматирование дискеты, указав дополнительный параметр /U. В этом случае информация о удаляемых файлах не сохраняется и их нельзя будет восстановить.

Вы можете значительно ускорить процесс подготовки системной дискеты, если укажите команде FORMAT дополнительный параметр /Q. В этом случае выполняется быстрое форматирование дискеты:

Опишем процесс подготовки системной дискеты более подробно. Введите следующую команду:

FORMAT A: /S /U

На экране появится предложение вставить дискету в дисковод A: и нажать клавишу <Enter>:

Insert new diskette for drive A:
and press ENTER when ready...

Начнется процесс форматирования. На экране в процентах будет отображаться объем выполненной работы.

Formatting 1.2M
77 percent completed.

После окончания форматирования на дискету записываются основные файлы операционной системы. Затем вы можете ввести метку дискеты. Метка должна содержать не более одиннадцати символов. После ввода метки нажмите клавишу <Enter>. Если вы не желаете присваивать дискете метку, нажмите клавишу <Enter> сразу:

Format complete.
System transferred

Volume label (11 characters, ENTER for none)?

Затем на экране появится различная статистическая информация: общая емкость дискеты, объем пространства, занятый файлами операционной системы, объем доступного свободного пространства. Если на дискете обнаружены плохие секторы, недоступные для использования, отображается их суммарный объем в байтах. Ниже выводится размер сектора в байтах, количество свободных секторов на дискете и ее серийный номер:

1,213,952 bytes total disk space
198,656 bytes used by system
1,015,296 bytes available on disk

512 bytes in each allocation unit.
1,983 allocation units available on disk.

Volume Serial Number is 2C74-14D4

Format another (Y/N)?

На этом подготовку системной дискеты можно считать завершенной. Если вы не планируете сразу создать несколько системных дискет, нажмите клавишу <N>. Чтобы создать еще одну системную дискету, нажмите клавишу <Y> и повторите описанный нами процесс еще раз.

Использование команды SYS

Если у вас есть свободная чистая отформатированная дискета, быстрее всего можно сделать ее системной при помощи команды SYS. Для этого вставьте дискету в дисковод компьютера и введите следующую команду:

SYS [drive1:][path] drive2:

Команда SYS имеет один обязательный параметр - drive2. Этот параметр должен задавать имя дисководов, в котором подготавливается системная дискета. Вам следует указать в качестве параметра drive2 имя A: или B:.

|| Загрузка компьютера происходит с диска A:. Вы должны изготовить
|| системную дискету соответствующего размера

Необязательные параметры *drive1* и *path* определяют расположение системных файлов на диске. Если вы не укажете эти параметры, команда SYS будет брать системные файлы из корневого каталога текущего диска.

Запись антивирусных программ на системную дискету

На системной дискете располагаются основные файлы операционной системы MS-DOS: IO.SYS, MSDOS.SYS, COMMAND.COM, DBLSPACE.BIN. Если системная дискета изготовлена в операционной системе совместимой с MS-DOS, например IBM PC-DOS, то имена этих файлов могут быть другие.

Файлы IO.SYS и MSDOS.SYS представляют собой ядро операционной системы. Файл COMMAND.COM обычно называют командным процессором. Это та самая программа, которая выводит на экран компьютера системное приглашение и выполняет команды операционной системы. Последний файл на системной дискете - DBLSPACE.BIN. Он содержит расширение операционной системы, которое обеспечивает доступ к уплотненным дискам системы DoubleSpace.

Основные файлы операционной системы - IO.SYS, MSDOS.SYS имеют атрибут "скрытый файл" и не показываются командой DIR. Чтобы увидеть их, добавьте к команде DIR параметр /A.

DIR A:\A

После того как вы изготовили системную дискету, на ней осталось еще много свободного места. Суммарный объем, занимаемый основными файлами операционной системы MS-DOS - IO.SYS, MSDOS.SYS, COMMAND.COM, DBLSPACE.BIN составляет около 200 Кбайт. Таким образом, если вы использовали дискету с высокой плотностью записи, то в вашем распоряжении оказывается больше мегабайта свободного пространства.

Запишите на системную дискету программное обеспечение, необходимое для тестирования и восстановления поврежденной операционной системы. В первую очередь необходимо записать антивирусные программы, выполняющие поиск вирусов и программу для проверки целостности файловой системы. Полезно записать команды FORMAT и FDISK - они могут понадобиться для ручного восстановления системы. Для удобства можно дополнительно записать на системную дискету оболочку, например Norton Commander, и любой текстовый редактор.

В следующей таблице перечислены программы, которые окажут вам помощь при восстановлении работоспособности компьютера. Желательно все их записать на системную дискету. В случае, если они не поместятся на одну системную дискету, подготовьте еще одну дискету и запишите оставшиеся программы на нее.

Программа	Назначение
-----------	------------

Aidstest	Антивирусная программа-полифаг. Позволяет обнаружить и удалить большое количество вирусов. Полиморфные вирусы, которые Aidstest не может обнаружить, определяются программой Doctor Web
Doctor Web	Антивирусная программа-полифаг, в которой реализован эвристический алгоритм поиска вирусов. Позволяет обнаружить сложные полиморфные вирусы. Вы должны использовать ее вместе с антивирусом Aidstest
ScanDisk или Norton Disk Doctor	Во многих случаях причиной неисправности и странного поведения компьютера служат не вирусы, а испорченная файловая система. Программы ScanDisk и Norton Disk Doctor обнаруживают и автоматически исправляют ошибки в файловой системе MS-DOS
CheckIt	Программа для тестирования всех подсистем компьютера. Позволяет обнаружить неисправность аппаратуры
Norton Commander	Оболочка для операционной системы MS-DOS. Значительно облегчает работу с компьютером. Содержит встроенный текстовый редактор, программы просмотра файлов в различных форматах
FORMAT	Команда MS-DOS. Предназначена для форматирования жестких и гибких дисков компьютера
FDISK	Команда MS-DOS. Предназначена для создания и удаления логических дисков. Команды FDISK и FORMAT могут понадобиться в случае полного разрушения информации на жестком диске. Их применение описывается в главе “Восстановление файловой системы”
Disk Editor	Редактор диска. Позволяет просматривать и редактировать любую информацию, записанную на диске, включая системные области. Disk Editor позволяет отредактировать главный загрузочный сектор, загрузочные секторы, таблицы размещения FAT, структуры каталогов и файлы

В некоторых случаях для доступа к жестким дискам компьютера могут использоваться специальные драйверы или резидентные программы. Их обязательно нужно записать на подготовленную системную дискету. Чтобы они автоматически подключались при загрузке компьютера с системной дискеты, создайте на ней файлы CONFIG.SYS и AUTOEXEC.BAT, записав в них команды загрузки необходимых драйверов.

Если к компьютеру подключено устройство чтения компакт-дисков, запишите на системную дискету программное обеспечение, необходимое для его использования. Для

MS-DOS вам надо записать драйвер устройства чтения и программу MSCDEX, входящую в состав операционной системы. Доступ к устройству чтения позволит оперативно восстановить программное обеспечение, записанное на компакт-дисках.

Операционная система Windows 95 не нуждается в программе MSCDEX, однако если графическая оболочка этой системы на загружаемая, MSCDEX все же надо подключить

После того как вы полностью подготовили системную дискету и записали на нее все необходимые программы, установите на нее защиту от записи. Для этого на дискете размером 5,25" необходимо наклеить прорезь на краю дискеты, а на дискете размером 3,5" открыть окно защиты. Защита от записи даст гарантию того, что вы случайно не испортите содержимое дискеты и вирусы не смогут на нее проникнуть. Так как дискеты иногда выходят из строя, то на этот случай лучше всего иметь несколько идентичных системных дискет.

Загрузка с системной дискеты

Чтобы загрузить компьютер с системной дискеты, надо установить приоритетную загрузку операционной системы с гибких магнитных дисков. Приоритет загрузки операционной системы определяется в CMOS-памяти. Чтобы изменить его, следует запустить программу Setup. Подробнее о программе Setup вы можете узнать из четвертого тома серии "Персональный компьютер - шаг за шагом", который называется "Что вы должны знать о своем компьютере".

Существуют вирусы, изменяющие приоритет загрузки компьютера. Для этого они меняют данные, записанные в CMOS-памяти. Примером таких вирусов могут быть вирусы Mammoth.6000 и EkeBug. Эти вирусы отключают в CMOS-памяти дисководы, временно подключая их, если какая-либо программа желает прочитать или записать информацию на дискету. Когда пользователь пытается загрузить компьютер с дискеты, загрузка будет выполняться с жесткого диска, так как дисковод отключен. Вирус получит управление, а затем выполнит загрузку компьютера с дискеты.

При этом с точки зрения пользователя все выглядит как обычно. Он видит, что операционная система загружается с дискеты, но к этому времени вирус уже находится в оперативной памяти и контролирует работу компьютера.

Поэтому непосредственно перед тем как выполнять загрузку MS-DOS с системной дискеты, убедитесь, что содержимое CMOS-памяти установлено правильно. Для этого запустите программу установки параметров BIOS и проверьте указанный там тип дисководов, а также порядок загрузки компьютера.

Вставьте системную дискету в дисковод A: и перезапустите компьютер. Если вы подозреваете наличие вирусов, для перезагрузки необходимо выключить и включить питание компьютера или нажать кнопку "Reset" на корпусе компьютера. Некоторые

вирусы отслеживают перезагрузку при помощи клавиш <Ctrl+Alt+Del> и могут остаться в оперативной памяти даже после такой загрузки с системной дискеты.

После первоначального тестирования компьютера начнется загрузка операционной системы с дискеты. При этом должен гореть светодиод дисковода A:. Процесс загрузки с дискеты проходит несколько медленнее, чем с жесткого диска, поэтому вам придется немного подождать. Когда загрузка операционной системы завершится, на экране появится соответствующее сообщение.

Затем операционная система запросит у вас текущую дату и время. Дата и время запрашиваются только в том случае, если на дискете (диске) отсутствует системный конфигурационный файл AUTOEXEC.BAT.

Если вы не хотите изменять дату и время, нажмите два раза клавишу <Enter>. В этом случае дата и время останутся без изменения, и на экране появится системное приглашение MS-DOS:

A:\>

Вы можете создать на системной дискете пустой файл AUTOEXEC.BAT, тогда дата и время запрашиваться не будут и после загрузки операционной системы на экране сразу появится системное приглашение.

Можно ли предотвратить проникновение вирусов

Если периодически не проводить работу по профилактике и лечению компьютеров от вирусов, возможность потери хранимой информации и разрушения операционной среды становится более чем реальной.

Негативные последствия вашей халатности могут быть различными, в зависимости от того, какой вирус попадет в компьютер. Вы можете потерять либо часть информации из файлов, хранящихся в компьютере, либо отдельные файлы, либо даже все файлы на диске. Но хуже всего, если вирус внесет небольшие изменения в файлы данных, которые сначала могут быть не замечены, а потом приведут к ошибкам в финансовых или научных документах.

Работы по профилактике и лечению компьютеров от вирусов могут включать следующие действия:

- ♦ Устанавливать программное обеспечение следует только с дискет и бутилированно
- ♦ Установите на всех ваших дискетах защиту от записи и снимайте ее только в случае необходимости
- ♦ Ограничьте обмен программами и дискетами, проверяйте такие программы и дискеты на наличие вирусов
- ♦ Периодически проверяйте оперативную память и диски компьютера на наличие вирусов с помощью специальных антивирусных программ

- *Выполняйте резервное копирование информации пользователя*

Не знакомьтесь с незнакомыми людьми

Никакие меры защиты не помогут защитить компьютер от проникновения вирусов, если вы не будете предварительно проверять все записываемые в него выполнимые файлы. На сегодняшний день такая проверка осуществима только с помощью антивирусных программ-полифагов.

Постоянное появление все новых и новых вирусов требует использования самых последних версий антивирусных программ. Желательно, чтобы ими обеспечивался поиск не только известных вирусов, но также и эвристический анализ проверяемых программ и загрузочных секторов. Он позволит обнаружить файлы, зараженные новыми, еще неизвестными и неизученными вирусами.

К сожалению, антивирусные программы не могут дать полной гарантии отсутствия в проверяемом программном обеспечении вирусов и тем более троянских программ или логических бомб. Записывая на свой компьютер программное обеспечение неизвестного происхождения, вы всегда рискуете

В больших организациях имеет смысл выделить специальный компьютер для установки в него сомнительного программного обеспечения, например компьютерных игр. Этот компьютер должен быть изолирован от остальных компьютеров организации. В первую очередь необходимо отключить его от локальной сети и запретить пользователям не только копировать с него программы, но и записывать на него файлы со своих рабочих дисков, заранее не защищенных от записи.

На время работы с подозрительным программным обеспечением используйте программы-мониторы, например монитор VSafe, входящий в состав MS-DOS. Если программа действительно окажется заражена вирусом или она содержит логическую бомбу, монитор сообщит о любых несанкционированных действиях с ее стороны. К сожалению программы-мониторы типа VSafe легко могут быть обмануты вирусами, поэтому более надежно использовать программно-аппаратные средства защиты.

В состав антивирусного комплекта “ДиалогНаука” входит программно-аппаратный комплекс защиты Sheriff. Помимо всего прочего, он выполняет все функции программ мониторов, но делает это значительно лучше. За счет того что контроль компьютера обеспечивается специальным контроллером защиты на аппаратном уровне, вирусы не смогут обмануть Sheriff.

Как защитить дискеты от записи

Вы можете защитить свои дискеты от записи. Защита работает на уровне аппаратуры компьютера и ее нельзя отключить программными методами. Поэтому вирус не сможет

заразить загрузочный сектор и выполнимые файлы, записанные на дискете с установленной защитой от записи.

Рекомендуется хранить все дискеты с установленной защитой от записи, и снимать ее только в случае, когда надо записать на нее новую информацию.

Все дистрибутивы программного обеспечения, записанные на дискетах, следует защищать от записи. Большинство программного обеспечения можно устанавливать с дисков, на которых установлено средство защиты от записи

Если вы попытаетесь записать данные на дискету с установленной защитой от записи, операционная система выведет на экран компьютера предупреждающее сообщение. Оно может иметь различный вид, в зависимости от того, какие средства используются для записи на дискету.

Например, если вы используете команды COPY или XCOPY операционной системы MS-DOS, и пытаетесь записать файл на защищенную дискету, тогда на экране появится следующее сообщение:

Write protect error reading drive A
Abort, Retry, Fail?

Пользователь должен ответить, как операционная система должна поступить в этой ситуации. Вы можете выбрать три ответа: Abort, Retry или Fail. Для этого достаточно ввести с клавиатуры первый символ выбранного ответа: Abort - <A>, Retry - <R>, Fail - <F>. Можно использовать как заглавные так и строчные буквы.

Выбор Abort или Fail означает, что операционная система должна отказаться от попытки записать информацию на дискету (Abort просто отменяет выполнение операции, а Fail указывает на необходимость вернуть программе код ошибки). Если вам надо выполнить операцию записи, снимите с дискеты защиту от записи и выберите Retry.

Необходимо внимательно отнестись к сообщению о попытке записи на защищенную дискету. Чтение файлов с дискеты, и запуск с нее большинства программ не должны вызывать записи на нее. Если вы уверены, что запись на дискету выполняться не должна, но она происходит, велика вероятность, что компьютер заражен вирусом.

Некоторые вирусы блокируют вывод сообщения о попытке нарушения защиты от записи, когда заражают выполнимые файлы или загрузочный сектор дискеты. Это позволяет им остаться незамеченными, если на дискете установлена защита. Тем не менее, вы достигнете желаемого результата, дискета останется незараженной.

Вirus Plague.2647

Неопасный резидентный стелс-вирус. При открытии инфицированных файлов удаляет из них свой код, а затем снова заражает, когда файл закрывается. При заражении файлов на дискетах проверяется установка

ли защиты от записи. Если защита успешно введена, вирус не будет пытаться заразить файлы на нем. Содержит строку "PLAGUE"

Защиту от записи можно установить на дискету любого размера - 3,5 дюймов и 5,25 дюймов. Проще всего это делается на дискетах размера 3,5 дюймов. Вам достаточно закрыть маленькое отверстие в углу дискеты специальной пластмассовой крышечкой, как это показано на рис. 2.1. Снять защиту от записи также просто: достаточно открыть защитное отверстие.

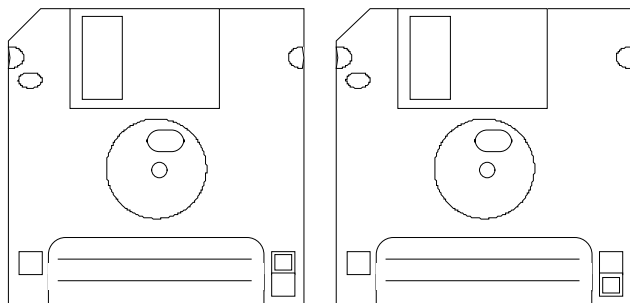


Рис. 2.1. Защита от записи на дискете размера 3,5 дюйма

Чтобы защитить от записи дискету 5,25", нужно заклеить прорезь в конверте дискеты (рис. 2.2). Для этого используется небольшой прямоугольный кусочек клейкой бумаги. Обычно такая бумага продается вместе с дискетами. В крайнем случае вы можете воспользоваться обычной изолентой. Снять защиту от записи можно, удалив приклеенный вами кусочек бумаги.

Часто снимать и устанавливать защиту на дискете 5,25" очень трудно, рано или поздно это надоест и вирус сможет проникнуть на дискету. Поэтому по возможности откажитесь от дискет размером 5,25" и замените их более удобными дискетами размера 3,5".

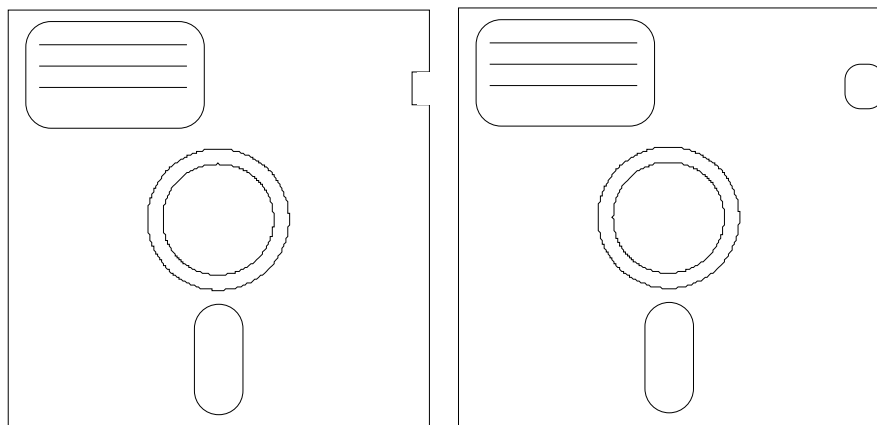


Рис. 2.2. Защита от записи на дискете размера 5,25 дюймов

Правильный выбор порядка загрузки компьютера

Операционная система может быть загружена или с жесткого диска или с дискеты. Обычно компьютер загружается с жесткого диска, однако если в момент включения питания компьютера или его перезагрузки в дисковод A: вставлена дискета (случайно или нарочно), загрузка операционной системы начнется с нее. Если дискета заражена загрузочным вирусом, он получит управление и сразу попытается заразить жесткий диск компьютера.

Большинство компьютеров позволяют указать приоритет, в котором должна выполняться загрузка операционной системы. Этот порядок устанавливается при помощи программы BIOS Setup. Более подробно о программе BIOS Setup вы прочитаете в разделе "Восстановление файловой системы".

Чтобы защитить компьютер от случайного заражения загрузочным вирусом, укажите, что операционная система должна загружаться сначала с диска C:, и только в случае его неисправности - с диска A:.

Если надо загрузить компьютер с дискеты, удостоверьтесь, что на ней нет вирусов. Для этого сначала проверьте ее несколькими антивирусными программами, например программами Doctor Web и Aidtest.

Лучше всего, если вы приготовите системную дискету заранее, а чтобы ее случайно не испортили, установите на ней защиту от записи. На системную дискету полезно записать программы для диагностики компьютера - антивирусные программы, программы проверки целостности файловой системы и исправности аппаратуры компьютера. Как создать системную дискету мы рассказали в разделе "Создание системной дискеты".

Непопулярные меры

В организациях очень эффективными могут оказаться жесткие меры защиты, связанные с отключением от компьютеров каналов возможного поступления вирусов. В первую очередь это относится к дисководам для гибких дисков. Дисководы могут быть отключены физически и сняты с компьютера или их можно отключить только в CMOS-памяти, при этом на программу BIOS Setup следует поставить пароль.

В идеальном случае от компьютера надо отключить все дисководы, устройства чтения компакт-дисков, модемы, последовательные и параллельные порты, сетевые адаптеры. Конечно это нереально, однако не следует полностью отказываться от такой идеи.

Резервное копирование

Очень важно организовать резервное копирование информации, хранимой в компьютере. В зависимости от средств, которыми вы располагаете, можно выполнять полное копирование жестких дисков компьютера или копирование только самой важной информации, которая не может быть восстановлена другим путем.

Для резервного копирования обычно используют магнитные ленты. Запись на них осуществляется специальными цифровыми магнитофонами, называемыми стримерами. Объем магнитных кассет составляет от 200 Мбайт до 4 Гбайт. В последнее время стали доступны устройства магнито-оптической дисковой памяти. По надежности и удобству использования они значительно превосходят магнитную ленту. Объем магнитооптических дисков широко варьируются и составляет от десятков мегабайт до нескольких гигабайт.

Если в вашем распоряжении нет ни стримера, ни магнитооптического диска, то во многих случаях достаточно использовать простые дискеты. Конечно запись на дискеты - это самый плохой способ резервного копирования. Во-первых, дискеты имеют очень маленький объем - немногим больше одного мегабайта. Во-вторых, дискеты очень ненадежны. Иногда с них не удается считать ранее записанную информацию.

Одной резервной копии недостаточно. Вы должны иметь несколько резервных копий. Вот небольшой пример. Вы выполняете очередное копирование и вдруг происходит сбой питания или нападение вируса. Компьютер зависает, данные записанные в компьютере и их копия оказываются испорченными

Выполняя резервное копирование, надо быть предельно осторожным. Перед копированием всегда проверяйте целостность копируемой информации. Выполняйте поиск вирусов и проверку файловой системы. Для этого используйте самые последние версии антивирусов и программы типа ScanDisk. Если не соблюдать этого правила, то все резервные копии рано или поздно окажутся испорченными.

В особо ответственных случаях выполняйте циклическое копирование данных. Например, одну копию обновляйте каждый день, вторую - каждую неделю, третью - каждый месяц.

Архивирование файлов

Если для резервного копирования используются обычные дискеты, тогда перед записью на них файлов их следует сжать какой-либо программой архивации. Программы-архиваторы позволяют уменьшить размер дисковой памяти, занимаемый файлами. Это происходит за счет устранения избыточности информации, хранимой в сжимаемых файлах.

Сжатые файлы могут занимать значительно меньше места на диске, чем их оригиналы. Так, текстовые файлы, подготовленные, например, в текстовом процессоре Microsoft Word for Windows, обычно уменьшаются вдвое. Конечно, работать с таким файлом невозможно. Перед работой его надо восстановить с помощью той же программы архивации.

В настоящее время наиболее популярны архиваторы ARJ, PKZIP, RAR. Все они выполняют примерно одинаковые функции и могут быть использованы для создания резервных копий документов.

Более подробно вопросы архивирования данных рассмотрены в десятом томе серии “Библиотека системного программиста”, который называется “Компьютер IBM PC/AT, MS-DOS и Windows. Вопросы и ответы”. Сейчас мы только приведем пример использования архиватора ARJ для подготовки резервных копий файлов. Формат вызова архиватора ARJ достаточно сложен:

```
ARJ <команда> [-<ключ> [-<ключ>...]] <имя архива>
[<имена файлов>...]
```

Первый параметр - *команда* - определяет режим работы архиватора:

Команда	Режим работы архиватора
A	Добавление новых файлов в архив
D	Удаление файлов из архива
E	Извлечение файлов из архива
L	Просмотр содержимого архива
M	Перенос файлов в архив. Файлы записываются в архив, а затем исходные файлы удаляются с диска
X	Восстановление файлов вместе со структурой каталогов и подкаталогов, в которой эти файлы были расположены при архивации
E	Восстановление файлов архива. Структура каталогов и подкаталогов не восстанавливается, все файлы из архива помещаются в один каталог
U	Обновить файлы в архиве. В архив записываются только измененные и новые файлы. Файлы, оставшиеся без изменения, заново не архивируются. За счет этого экономится много времени

После одной из приведенных команд могут следовать один или несколько необязательных дополнительных параметров *ключ*. Дополнительные параметры должны выделяться символом '-'. Приведем таблицу наиболее важных дополнительных параметров и опишем их назначение:

Дополнительный параметр	Назначение
-G	Защита создаваемого архива паролем
-R	Используется с командами "a" или "m" для указания того, что в архив должны войти файлы из текущего каталога и всех его подкаталогов

-V	<p>Создание и восстановление многотомных архивов, расположенных на нескольких дисках. Каждая дискета содержит один том архива (файл). Существует несколько модификаций параметра -v:</p> <p>VV - выдавать звуковой сигнал между обработкой отдельных томов архива;</p> <p>VA - автоматически определять объем свободного пространства на дискете (размер очередного тома архива);</p> <p>Vnnnnn - размер отдельных томов архива, например V20000 - создать архив из томов по 20 Кбайт;</p> <p>V360, V720, V1200, V1440 - создать тома, фиксированного размера по 360 Кбайт, 720 Кбайт, 1,2 Мбайт, 1,44 Мбайт</p>
-JR	Восстановить файлы из поврежденного архива. Используйте этот параметр, если восстановление файлов из архива прервалось сообщением архиваторе о нарушениях в структуре файла-архива
-X<file_name>	Не архивировать файл, указанный далее. В имени файла можно использовать символы '?' и '*'
-Y	Архиватор не будет запрашивать у пользователя разрешения для выполнения различных действий, например для создания нового файла многотомного архива, создания каталогов

После дополнительных параметров следует имя файла архива, а за ним - список имен извлекаемых, добавляемых или удаляемых файлов. При указании имен этих файлов можно использовать символы '?' и '*'. Если вы не укажете список file_names, то будут подразумеваться все файлы, расположенные в текущем каталоге или архиве.

Программы-архиваторы очень удобны для создания резервных копий на дискетах. Если файл архива не помещается на одной дискете, архиватор позволяет создать многотомный архив, состоящий из нескольких файлов. Для этого надо указать дополнительный параметр V. Отдельные файлы многотомного архива можно записать на несколько дискет.

Следующая команда создает многотомный архив, из всех файлов, расположенных в текущем каталоге и всех его подкаталогах, за исключением файлов, имеющих имя TMP или расширение имени BAK. Файлы многотомного архива будут иметь размер немного больший, чем 1,44 Мбайт. Вы сможете записать их на 3-дюймовые дискеты.

```
ARJ A -R -X*.BAK -XTMP.* -V1440 !COLLAPS
```

Файлы созданного архива будут иметь имя !COLLAPS и различные расширения:

```
!COLLAPS.ARJ
!COLLAPS.A01
!COLLAPS.A02
!COLLAPS.A03
....
```

Восстановить файлы, записанные в этом многотомном архиве, можно либо предварительно скопировав их на жесткий диск компьютера или непосредственно с дискет. Например, для восстановления с дискет используйте следующую команду:

```
ARJ X -V A:\!COLLAPS
```

После восстановления файла архива пользователю будет выдан запрос на обработку следующего файла архива. Вставьте в дисковод следующую дискету и нажмите кнопку <Y>.

Резервное копирование документов в Windows 95

Операционная система Windows 95 предоставляет удобные средства для резервного копирования отдельных документов и целых каталогов на дискеты. Для этого достаточно открыть пиктограмму My Computer и перейти в каталог, файлы из которого надо записать на дискеты.

Затем переместите указатель мыши на пиктограмму того файла или каталога, который должен быть скопирован, и нажмите правую кнопку мыши. На экране появится небольшое меню.

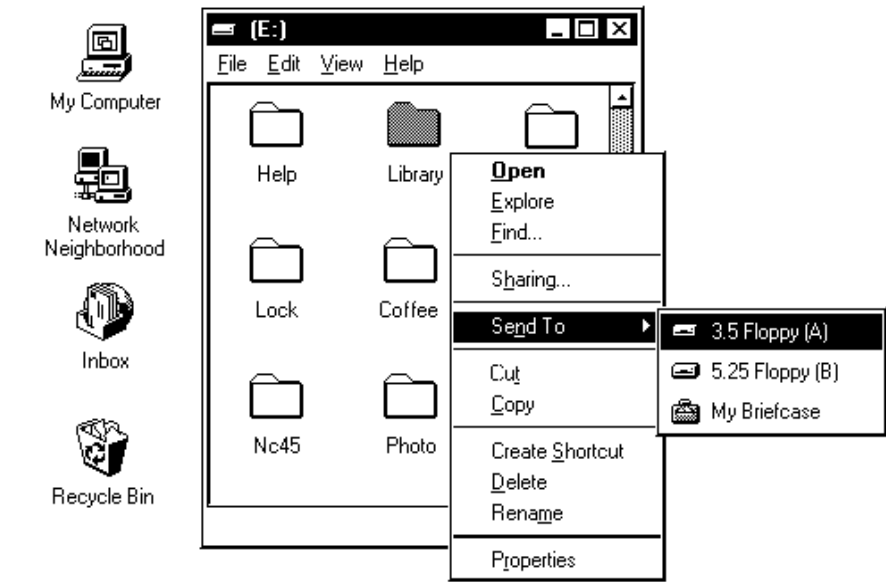


Рис. 2.3. Запись каталога Library на дискеты

Выберите из этого меню строку Send To, а затем в открывшемся временном меню укажите диск, на котором будет происходить копирование. На рисунке 2.3 мы показали, как надо выполнять копирование каталога Library на дискеты размера 3,5 дюйма.

После того как вы укажете диск, начнется процесс копирования. Если для копирования всех файлов каталога одной дискеты окажется недостаточно, операционная система попросит вас вставить следующую дискету.

К сожалению, продемонстрированный нами способ загрузки не позволяет скопировать на дискеты файлы, размер которых превышает объем самой дискеты. Поэтому скопировать, таким образом, очень большие документы невозможно.

Проверим, нет ли вирусов

Для проверки новых программ, которые вы записываете в свой компьютер, надо использовать антивирусные программы-полифаги последних версий. Они смогут обнаружить любые вирусы, известные на момент создания программы-антивируса. Желательно, чтобы используемые вами антивирусы выполняли эвристический анализ программ. Возможно, это позволит обнаружить новые, еще не известные вирусы.

Популярность антивирусных программ Aidstest и Doctor Web настолько велика, что они установлены практически на каждом компьютере. Поэтому сейчас мы проверим ваш компьютер с помощью этих программ и посмотрим, нет ли в нем вирусов.

Если у вас нет самых последних версий антивирусов, воспользуйтесь теми программами, которые у вас есть. Несмотря на то, что такая проверка будет неполной, она все же позволит обнаружить большое количество вирусов.

Поиск вирусов на жестком диске компьютера

В начале проверим все жесткие диски компьютера программой Aidstest. Введите в системном приглашении DOS следующую команду.

AIDSTEST *

Внимательно следите за сообщениями, выдаваемыми программой во время проверки компьютера. Если будет обнаружен вирус, Aidstest сообщит об этом.

Многие вирусы, которые не обнаруживает Aidstest, могут быть пойманы программой Doctor Web. Кроме того, Doctor Web позволяет выполнить эвристический анализ программ и загрузочных секторов. Поэтому повторите проверку с помощью Doctor Web.

DRWEB */CL/HL/AR/HA1/RV/UP

Антивирус Doctor Web проверит все жесткие диски компьютера, при этом он выполнит поиск вирусов не только непосредственно в выполнимых файлах, но и в файлах архивов, а также в сжатых выполнимых файлах. Если вирусы будут обнаружены, программа выведет на экран соответствующее сообщение.

Во всех примерах, приведенных в этом разделе, выполняется только поиск вирусов, ни один из обнаруженных вирусов не будет удален. Для этого надо запустить программу-антивирус еще один раз, загрузившись с системной дискеты.

Поиск вирусов на дискетах

Все новые дискеты, а также дискеты, которые вы отдавали кому-либо, необходимо проверить на заражение вирусами. Для этого используйте антивирусы-полифаги Aidstest и Doctor Web. Последовательно вызовите сначала одну, а затем другую программы. В следующем примере показано как проверить дискету, вставленную в дискетод A:

AIDSTEST A: /B

DRWEB A: /CL/AR/HA1/UP/NM/OF

Вирусы в файлах архивов

Чтобы увеличить объем свободного пространства на жестком диске и дискетах, многие пользователи архивируют редко используемые файлы. Для этого могут использоваться специальные программы-архиваторы, уменьшающие размер файлов за счет устранения избыточности данных, записанных в файле. Когда пользователю вновь требуется файл из архива, он снова использует программу-архиватор.

Файлы внутри архива хранятся в сжатом виде, исключая возможность поиска вируса по их сигнатурам. Поэтому, если вы записали в архив зараженную программу, она может остаться незамеченной для многих антивирусов.

Некоторые антивирусные программы, например Doctor Web, позволяют проверять файлы, записанные внутри архивов. Проверяя архивы, Doctor Web временно восстанавливает записанные в нем файлы и последовательно просматривает их.

Если вы обнаружили в своем компьютере вирусы, обязательно проверьте все файлы архивов, даже если ваша антивирусная программа не умеет работать с архивами. Самостоятельно восстановите файлы из всех архивов на диске, а затем проверьте их вашей антивирусной программой

Обычно, когда на одном компьютере работает несколько человек, они используют различные средства разграничения доступа к жестким дискам. Например Diskreet из пакета Norton Utilities, позволяет создать несколько логических дисков. Каждый пользователь может иметь доступ только к некоторым дискам, остальные для него будут полностью недоступны.

Вirus ArjVirus

Неопасный нерезидентный вирус. Выполняет поиск в текстовых каталогах и его подкаталогах файлов архивов, созданных программой-архиватором ARJ. Файлы архивов вирус открывает только по их расширению - ARJ.

Если файл архива будет обнаружен, вирус создает файл, имеющий случайное имя, состоящее из четырех символов от 'A' до 'V', с расширением COM. В этот файл вирус записывает 5 Кбайт своего кода и в конце дополняет его произвольным количеством байт

Затем вирус вызывает программу-архиватор ARJ, считая, что он расположен в одном из каталогов, перечисленных в переменной PATH. Для этого использует командный процессор:

```
C:\COMMAND.COM /C ARJ A <ArjFile> <ComFile>
```

В качестве параметра ArjFile указывается имя найденного вирусом файла-архива. Параметр ComFile содержит имя только что созданного исполнимого файла вируса. Такая команда добавляет в обнаруженный вирусом файл-архив новый исполнимый файл вируса. Затем исходный файл вируса удаляется.

Чтобы пользователь не увидел на экране информацию, обычно отображаемую программой-архиватором ARJ, вирус временно отключает весь вывод на экран монитора.

Основная идея вируса заключается в том, что пользователи восполнившие файлы из зараженного архива обнаружат в нем неизвестный исполнимый файл и запустят его из любопытства

Необходимо выполнять поиск вирусов на всех дисках. Лучше всего если это будет делать пользователь, имеющий доступ ко всем дискам компьютера. В противном случае каждый пользователь должен будет проверять доступные ему диски. Если кто-либо из пользователей обнаружит, что на диске, доступном ему, присутствует вирус, он обязательно должен сообщить об этом всем другим пользователям компьютера.

Если вы обнаружили вирус

Самую большую ценность представляют ваши данные, записанные в компьютере. Это могут быть текстовые документы, файлы электронных таблиц, базы данных, исходные тексты программ и т. д. Их стоимость может в много и много раз превышать стоимость самого компьютера и установленного в нем программного обеспечения.

Любое программное обеспечение, разрушенное вирусами, можно восстановить с дистрибутивов или резервных копий. А вот с данными дело обстоит значительно хуже. Если данные постоянно не копировались, они могут быть безвозвратно потеряны.

Поэтому обнаружив вирус, в первую очередь надо перезагрузиться с чистой дискеты и скопировать ваши данные с жесткого диска компьютера на дискеты, магнитные ленты или любые другие устройства хранения информации. Только после этого можно приступать к лечению компьютера.

Если обнаружен вирус, то возможно, он уже разрушил хранимую в компьютере информацию. Разрушения могут носить различный характер. Возможно, файлы с данными будут уничтожены полностью и вы даже не сможете их прочитать, а возможно они будут изменены незначительно и вы не сможете это сразу заметить.

Вирус Rogue.1208

Опасный резидентный вирус. Уничтожает файлы с расширением DBF, записывая в них первый байт 'R' и производя с остальным содержанием файла логическую операцию ИСКЛЮЧАЮЩЕЕ ИЛИ с числом 13, до первого символа, который имеет код 13. Уничтожает файлы CHKLIST ????. В месяц, когда сумма значения года и значения месяца равна 2000, вирус выводит на экран: "Now you got a real virus! I'm the ROGUE ...!"

Постарайтесь выяснить, какой именно вирус попал к вам в компьютер и что он делает. Получить подобную информацию можно из описаний вирусов, поставляемых вместе с антивирусными программами. Фактически все антивирусные программы имеют такие списки. Они могут быть выполнены в виде простых текстовых файлов или в виде специальных гипертекстовых баз данных.

Если вы обнаружили в компьютере вирус, он уже мог успеть распространиться, заразив другие компьютеры в вашей организации. Их необходимо проверить в обязательном порядке. Многие пользователи сегодня имеют компьютеры у себя дома. Они также могут оказаться заражены.

Необходимо проверить все дискеты, использовавшиеся для работы с зараженными компьютерами. Они могут оказаться заражены загрузочными и файловыми вирусами. Вирус может сохраниться на них, а затем снова заразить компьютер. Дискеты, зараженные вирусами, надо вылечить или отформатировать.

Как лечить компьютер

После того как вы попытались скопировать с компьютера все свои данные (документы, исходные тексты, файлы баз данных) пора начинать лечение компьютера и удаление заразивших его вирусов. Для вас существует как минимум три возможности удалить вирусы из компьютера.

Самый простой из них заключается в полной смене всего программного обеспечения, установленного в компьютере. Вы должны будете переустановить операционную систему и все остальные программы заново. Если вирус заразил загрузочную запись, то ее можно обновить, отформатировав логические диски компьютера, воспользовавшись для этого командой FORMAT. Однако даже форматирование не удалит вирус из главной загрузочной записи жесткого диска. Для этого следует воспользоваться командой FDISK

с недокументированным параметром /MBR, а затем снова создать на жестком диске разделы и логические диски.

Такие операции, как форматирование логического диска, удаление раздела или логического диска командой FDISK полностью уничтожают все файлы на данном диске. Поэтому предварительно удалять файлы нет никакой необходимости.

После того как вы заново создадите на жестком диске разделы и логические диски и отформатируете их, можно приступить к установке операционной системы и остальных программ. Полная установка программного обеспечения компьютера отнимает много времени. Чтобы ускорить этот процесс, по возможности устанавливайте программные продукты не с дискет, а с компакт-дисков.

Вы можете значительно облегчить восстановление работоспособности компьютера, если заблаговременно будете выполнять резервное копирование всей информации, записанной в компьютере. В этом случае после создания и форматирования логических дисков можно восстановить программное обеспечение с этих резервных копий. Как будет происходить это восстановление, зависит от средств, используемых вами при создании резервных копий.

Вторая возможность предполагает ручное удаление вирусов и восстановление поврежденных загрузочных секторов и файлов. Этот метод наиболее сложный и требует высокой квалификации. Мы расскажем о ручном восстановлении компьютера несколько позже в главе “Ручное восстановление операционной системы”.

И, наконец, последняя возможность предполагает применение специальных антивирусных программ. Антивирусные программы сами обнаружат и удалят вирусы, восстановив работоспособность компьютера. К сожалению, такое восстановление не всегда возможно, так как большая категория вирусов необратимо портит программы и данные, записанные на дисках компьютера. В этом случае необходимо заново установить программное обеспечение.

Сейчас мы очень кратко рассмотрим лечение компьютера антивирусными программами-полифагами Aidstest и Doctor Web. Более подробно об этих и других программах, позволяющих удалить вирусы из компьютера, читайте в следующей главе, которая называется “Лучшее средство”.

Лечение компьютеров антивирусными программами

Целый ряд резидентных вирусов, находясь в памяти компьютера, препятствует успешному лечению зараженных программ и загрузочных секторов. Поэтому желательно выполнять лечение только после загрузки компьютера с системной дискеты, свободной от вирусов. На эту дискету предварительно надо записать антивирусные программы-полифаги, например Aidstest и Doctor Web.

Программа Aidstest позволяет удалить обнаруженные ей вирусы. Для этого запустите Aidstest с параметром /F:

`AIDSTEST * /F`

Некоторые вирусы не могут быть обнаружены и удалены программой Aidstest, поэтому ее надо использовать совместно с антивирусом Doctor Web:

`DRWEB * /CL /UP /CU`

Программы Aidstest и Doctor Web могут лечить не только жесткие диски, но и дискеты. Для этого вместо параметра *, означающего работу со всеми жесткими дисками компьютера, надо указать имя дискового:

`AIDSTEST A: /F`

`DRWEB A: /CL /UP /CU`

3 ЛУЧШЕЕ СРЕДСТВО ПРОТИВ ВИРУСОВ

Проблема борьбы с вирусами приобрела настолько важное значение, что множество фирм, включая Microsoft, уделяют борьбе с ними все большее внимание. Среди зарубежных фирм, выпускающих антивирусное программное обеспечение, следует отметить McAfee, Central Point, IBM, S&S International, Symantec. Особенно хочется отметить отечественные антивирусные разработки АО “ДиалогНаука”, в которые входят такие известные программы как Aidstest, Doctor Web и ADinf.

Такое разнообразие ставит пользователя перед сложной проблемой выбора системы антивирусной защиты своего компьютера. Мы постараемся помочь вам, отметив критерии выбора, на которые следует обратить особое внимание. Чтобы дать вам представление о возможностях современных антивирусов, мы рассмотрим несколько таких средств, предназначенных для различных операционных систем - MS-DOS, Microsoft Windows, Microsoft Windows 95 и OS/2. Особое внимание мы уделим методике антивирусной защиты, позволяющей с наибольшей надежностью защитить вашу компьютерную систему.

Антивирусный комплект АО “ДиалогНаука”

В состав антивирусного комплекта АО “ДиалогНаука” входит несколько основных программ - Aidstest, Doctor Web, Doctor Web for WinWord, Advanced Diskinfoscope (ADinf) и ADinf Cure Module. Отдельно можно приобрести программно-аппаратный комплекс защиты от вирусов Sheriff.

Программы, входящие в состав антивирусного комплекта АО “ДиалогНаука”, используют все современные способы для борьбы с вирусами - поиск известных вирусов по их сигнатурам, эвристический анализ программ, позволяющий обнаружить неизвестные вирусы, контроль за изменениями на жестком диске.

Для поиска известных вирусов предназначены два антивируса-полифага. Это Aidstest и Doctor Web. Они позволяют обнаружить и удалить более чем 3000 известных на сегодняшний день вирусов. Полифак Doctor Web обнаруживает не только известные

вирусы. Эвристический анализатор Doctor Web может найти ранее неизвестные вирусы, которые еще не были проанализированы.

Новые вирусы появляются постоянно. Никакие законы и запреты не могут их остановить. Для успешного обнаружения и лечения вирусов программам-полифагам необходима разнообразная информация, которую можно получить только тщательным изучением зараженных программ. Поэтому успех практически любой антивирусной программы-полифага предполагает постоянное обновление версий программы или пополнение базы данных, содержащей информацию об известных вирусах.

Антивирусный комплект АО “ДиалогНаука” является в этом смысле наилучшим вариантом для отечественных пользователей. Специалисты АО “ДиалогНаука” в первую очередь занимаются вирусами, которые распространены в России и других странах бывшего СССР. Возможно, вирусные базы полифагов Aidstest и Doctor Web содержат меньшее количество вирусов, чем некоторые другие антивирусы, зато именно эти вирусы, скорее всего, могут заразить ваш компьютер.

Во многом это достигается за счет хорошо налаженных каналов поступления новых вирусов. Любой пользователь компьютера, в чьем распоряжении находится модем, может позвонить на станцию BBS АО “ДиалогНаука” и передать для изучения программы, зараженные новыми вирусами. Если переданная программа действительно заражена, то очередная версия Aidstest или Doctor Web будет его лечить.

Новые версии полифага Aidstest выходят постоянно (несколько раз в месяц) по мере появления новых вирусов. Версии полифага Doctor Web обновляются значительно реже. Чтобы Doctor Web смог лечить новые вирусы, достаточно получить файл-дополнение к вирусной базе программы. Эти файлы обычно выходят несколько раз в месяц. Получить их можно на станции BBS АО “ДиалогНаука” или непосредственно в офисе фирмы.

Удобнее всего купить подписку на антивирусный комплект АО “ДиалогНаука”. В этом случае вы сможете постоянно получать самые последние версии антивирусных программ. Владельцы модема могут связаться через него со станцией электронной почты BBS DialogueScience и получать антивирусы буквально не вставая из-за своего стола.

Кроме программ-полифагов в антивирусный комплект входит ревизор диска ADInf. Эта программа запоминает в собственных файлах (таблицах) различную информацию о программной среде компьютера - загрузочные секторы, контрольные суммы выполнимых файлов, расположение плохих кластеров, структуры каталога и т. д. Если какой-нибудь из этих параметров изменится, то очередная проверка компьютера ревизором ADInf сразу выявит изменения.

Интересной особенностью ADInf является обращение к файловой системе в обход операционной системы. Это позволяет легко обнаруживать стелс-вирусы, маскирующие свое присутствие в компьютере.

В дополнение к ADInf поставляется лечащий модуль ADInf Cure Module. Он удаляет обнаруженные вирусы из зараженных файлов. Интересно, что в отличие от полифагов

Aidstest и Doctor Web, модуль ADInf Cure Module удаляет даже новые вирусы. То есть он не нуждается в информации о каждом вирусе.

Чтобы удалить вирус ADInf Cure Module использует сведения полученные о файле до его заражения. Поэтому необходимо установить ADInf и ADInf Cure Module еще до заражения компьютера.

По настоящему полный заслон на пути вирусов ставит программно-аппаратный комплекс Sheriff. В дополнение ко всему Sheriff очень хорошо выполняет функции программы-монитора. Он немедленно реагирует на все несанкционированные действия программ, например, форматирование жесткого диска, изменение выполнимых файлов, изменение загрузочных секторов, блокируя эти операции и сообщая о них пользователю. Если для вашей работы нужен только чисто программный монитор, используйте программу VSafe из дистрибутива операционной системы MS-DOS.

Единственный метод борьбы с вирусами, не реализованный в антивирусном комплекте АО “ДиалогНаука”, это вакцинирование программ. Из-за низкой эффективности вакцинирования его использование совершенно нецелесообразно.

*Служба антивирусной скорой помощи, организованная АО “ДиалогНаука”,
высылает заказчику квалифицированных специалистов для лечения
компьютера в особо ответственных случаях*

Программы антивирусного комплекта работают в среде DOS, однако вы сможете их использовать и в других операционных системах, например Microsoft Windows и Microsoft Windows 95.

Программы Doctor Web, ADInf и ADInf Cure Module также работают и в среде операционной системы OS/2. Текущая версия Aidstest не совместима с OS/2.

Полифар Aidstest

Самой популярной антивирусной программой в России вот уже много лет является Aidstest, разработанный в конце 1988 года Лозинским Дмитрием Николаевичем. На момент создания книги вышло уже более 1400 версий программы. Aidstest умеет обнаруживать более 1500 вирусов в загрузочных секторах и выполнимых файлах. В том числе он успешно справляется с вирусами семейства DIR, вызвавшими эпидемию летом 1991 года и появляющимися вновь и вновь до сих пор.

Принципы, заложенные много лет назад в основу программы Aidstest, не позволяют ей обнаруживать и удалять полиморфные вирусы. Поэтому одной программы Aidstest явно недостаточно для обеспечения антивирусной безопасности компьютера. Вы обязательно должны пользоваться другими средствами комплекта. В первую очередь программой-полифагом нового поколения Doctor Web и ревизором ADInf.

Тем не менее, отказываться от Aidstest сегодня еще рано. Существует достаточно много вирусов, которые удаляет Aidstest, но которые не включены в вирусную базу Doctor Web. Возможно в скором времени вирусные базы Aidstest и Doctor Web будут объединены, тогда можно будет ограничиться использованием одной программы.

Полное описание программы Aidstest можно получить из документации. Сейчас мы приведем только самые главные параметры этой программы. Формат вызова Aidstest имеет следующий вид:

AIDSTEST путь [ключ]...[ключ]

Первый, обязательный, параметр программы **путь** определяет, какие файлы надо проверить. В качестве этого параметра вы можете указать имя логического диска, путь к каталогу или непосредственно имя файла для проверки. Если необходимо проверить все логические диски компьютера, укажите в качестве параметра **путь** символ '*'. Чтобы кроме логических дисков проверялись сетевые диски, компакт-диски и диски, образованные командой SUBST, вместо одного символа '*' укажите два.

После параметра **путь** следуют необязательные параметры, задающие различные режимы работы программы Aidstest. При вводе параметров не следует задавать символы квадратных скобок. Если вы ошиблись в задании параметров или не указали ни одного параметра, на экран выдается краткое описание программы. Ниже описаны только основные параметры программы.

Параметр	Описание
/E	Если видеоадаптер компьютера не русифицирован, укажите этот параметр. Aidstest будет пользоваться собственными русскими шрифтами
/F	Для лечения зараженных программ и загрузочных секторов укажите Aidstest дополнительный параметр /F. Те программы, которые невозможно восстановить, будут удалены
/G	По умолчанию Aidstest проверяет только выполнимые файлы, имеющие расширения COM, EXE и SYS. Параметр /G позволяет проверить все файлы на дисках компьютера, вне зависимости от их расширений. Если в компьютере обнаружен вирус, рекомендуется выполнить проверку всех файлов
/Q	В режиме лечения компьютера Aidstest удаляет зараженные файлы, которые нельзя восстановить. Чтобы перед удалением файлов у пользователя запрашивалось подтверждение, укажите параметр /Q
/S	Параметр /S необходимо указывать вместе с параметром /F для восстановления файлов, испорченных вирусами семейства DIR, в тех случаях, когда сам вирус отсутствует на диске

Как найти вирус

Программа Aidstest умеет обнаруживать вирусы без предварительной загрузки компьютера с чистой системной дискеты. Поэтому лучше всего записать программу Aidstest на жесткий диск компьютера и периодически проверять ей компьютер. Насколько часто нужно пользоваться Aidstest зависит от того, как и для чего используется компьютер. В большинстве случаев достаточно выполнять ежедневную проверку компьютера, включив вызов Aidstest в файл AUTOEXEC.BAT, а также отдельно проверять все новые файлы, записываемые на компьютер и все дискеты, которые в него вставляются. Особое внимание надо уделять проверке свободно распространяемого программного обеспечения, загруженного по электронной почте со станций BBS и FTP-серверов, а также дискетам, полученным от знакомых и друзей.

По мере появления новых вирусов выпускаются новые версии антивируса Aidstest. Что бы обеспечить надежную защиту компьютера, всегда используйте последние версии антивируса

При ежедневной проверке компьютера можно ограничиться проверкой выполнимых файлов, имеющих расширения COM, EXE и SYS. Следующая команда проверяет загрузочные секторы и выполнимые файлы на диске C:

AIDSTEST C:

Программа отображает на экране наиболее важную информацию и начинает проверять сначала загрузочные сектора указанного диска, а затем выполнимые файлы. По окончании проверки на экране отображается краткая статистическая информация:

Проверка "C:" (метка тома: PROGRAMM)

___ "C:" ___
Проверено файлов: 518
Заражено файлов: 0
- начальных секторов: 0
Следов вирусов DIR: 0

Если в ходе проверки на дисках компьютера или дискетах обнаружатся вирусы, на экране будут показаны имена зараженных файлов и названия заразивших их вирусов.

Проверка "A:" (метка тома: PROGRAMM)

Вирус в начальном секторе "FORM"
a:\C-639.COM - болен (Khizhnjak-639)
a:\COMMAND.COM - болен (V-475)
a:\FORMAT.COM - болен (Mini-129)

___ "A:" ___
Проверено файлов: 28
Заражено файлов: 3
- начальных секторов: 1
Следов вирусов DIR: 0

В этот раз Aidstest обнаружил на нашей дискете сразу четыре вируса. Один загрузочный - FORM и три файловых - Khizhnjak-639, V-475, Mini-129. Возможно, на дискете есть еще и другие вирусы, вы обязательно должны повторить проверку дискеты антивирусом Doctor Web.

После обнаружения на диске вирусов в выполнимых файлах повторите проверку еще раз, добавив в командной строке Aidstest параметр /G. На этот раз антивирус проверит все файлы на диске. Не забывайте выполнять такую проверку, так как иногда пользователи создают резервные копии файлов, изменяя их расширение. Например, резервная копия выполнимого файла MAYRAIN.EXE может называться MAYRAIN.BAK или MAYRAIN.EX_.

Лечение ко~~м~~пью~~те~~ра

Когда вирус обнаружен, надо решать что с ним делать. Вы можете удалить вирус с помощью антивирусной программы или удалить весь зараженный файл, восстановив его с дистрибутива или резервной копии.

Aidstest позволяет удалить обнаруженные им вирусы. Для этого надо указать дополнительный параметр /F. Если вы не укажете программе Aidstest такой дополнительный параметр, то она будет осуществлять только поиск вирусов.

В режиме лечения антивирус восстановит зараженные файлы и загрузочные секторы. Если зараженный файл испорчен и не может быть восстановлен, он будет удален. Чтобы перед удалением таких файлов, у пользователя требовалось подтверждение, добавьте параметр /Q.

Удалять вирусы из компьютера рекомендуется только после загрузки компьютера с чистой загрузочной дискеты. Это гарантирует, что вирус не получит управление и не установит в оперативной памяти резидентный модуль, который сможет помешать лечению.

Для загрузки с дискеты необходимо применять так называемую "холодную" перезагрузку, т. е. использовать кнопку сброса на корпусе ко~~м~~пью~~те~~ра или процедуру включения-выключения питания. Многие вирусы умеют о~~с~~т~~а~~ивать~~ь~~ся в памяти ко~~м~~пью~~те~~ра после того, как пользо~~в~~ате~~ль~~ наж~~м~~ет комбинацию клавиш <Alt + Ctrl + Del>

Существуют несколько вирусов, изменяющих данные, записанные в CMOS-памяти, таким образом, что компьютер всегда будет загружаться с диска С:.

К вирусам, изменяющим порядок загрузки компьютера, относятся некоторые модификации вируса EхеBug и вирус Mammoth.6000. Эти вирусы включают и выключают в CMOS-памяти признак наличия дисководов А: . Перед записью или чтением с дискеты вирусы включают признак наличия дисководов, а после отключают.

В результате при загрузке с чистой системной дискеты дисководы могут оказаться не установленными, и система в таком случае попытается загрузиться с жесткого инфицированного диска. Вирус первым получит управление, установит свою резидентную

копию в память, включит в CMOS-памяти признак наличия дисководов А: и передаст управление загрузочному сектору дискеты, вставленной в дисковод. В результате вирус получит управление даже при загрузке с чистой системной дискеты!

Перед перезагрузкой компьютера проверьте порядок загрузки компьютера, выбранный в CMOS-памяти. Сначала загрузка должна происходить с диска А: и только затем с диска С:.. Затем проверьте тип дисководов, указанный в конфигурации компьютера. Он должен соответствовать действительным параметрам дисководов, подключенных к компьютеру.

Чтобы просмотреть конфигурацию компьютера и порядок его загрузки, запустите программу BIOS Setup. Более подробно об этой программе вы можете прочитать в разделе "Восстановление файловой системы".

Ниже представлен пример использования антивируса Aidstest для обнаружения и лечения вирусов на диске С:.

AIDSTEST C: /F /Q

Программа проверит файлы на диске С:.. Все обнаруженные вирусы сказу будут удалены:

Проверка "А:" (метка тома: PROGRAMM)
Вирус в начальном секторе "FORM" - ОБЕЗВРЕЖЕН
а:\C-639.COM - болен (Khizhnjak-639) - ОБЕЗВРЕЖЕН
а:\COMMAND.COM - болен (V-475) - ОБЕЗВРЕЖЕН
а:\FORMAT.COM - болен (Mini-129) - ОБЕЗВРЕЖЕН

___ "А:" ___
Проверено файлов: 28
Заражено файлов: 3
- начальных секторов: 1
Следов вирусов DIR: 0

Исправлено файлов: 3
- строк каталогов: 0
Стерто файлов: 0

Полифар Doctor Web

Другая антивирусная программа-полифаг, входящая в состав антивирусного комплекта АО "ДиалогНаука", разработана Даниловым Игорем Анатольевичем. Также как и Aidstest, программа Doctor Web является полифагом, но при этом она основана совершенно на других принципах, благодаря чему позволяет обнаруживать полиморфные вирусы и успешно удалять их. Специальные методы позволяют Doctor Web обрабатывать зашифрованные вирусы.

В отличие от большинства антивирусных программ-полифагов, Doctor Web обнаруживает новые, неизвестные вирусы. Для этого применяется эвристический анализатор. Этот анализатор в автоматическом режиме изучает код проверяемых программ и загрузочных записей, пытаясь обнаружить в них участки кода, выполняющие характерные для вирусов действия.

Программа Doctor Web позволяет обнаружить и удалить опасный вирус OneHalf, широко распространившийся в последнее время. При этом Doctor Web восстанавливает зашифрованный вирусом жесткий диск компьютера. В зависимости от объема жесткого диска и того, насколько далеко зашел процесс его шифровки, на восстановление может потребоваться несколько десятков минут. В последнее время появились новые модификации вируса OneHalf, имеющие отличия в процедуре шифрования диска компьютера, поэтому надо использовать самые последние версии Doctor Web

Программа Doctor Web работает как в диалоговом, так и в пакетном режиме. Пакетный режим лучше всего использовать для проверки компьютера во время его загрузки, вызывая Doctor Web из файла AUTOEXEC.BAT. Чтобы Doctor Web начал работать в пакетном режиме, следует задать параметр /CL.

Полную информацию обо всех параметрах и режимах работы программы Doctor Web вы можете прочитать в документации антивирусного пакета АО “ДиалогНаука”. Сейчас мы перечислим только основные параметры программы:

Параметр	Описание
/AL	Проверка всех файлов на заданном диске
/AR	Проверка файлов, находящихся внутри архивов. Обеспечивается проверка архивов, созданных программами-архиваторами ARJ, PKZIP и RAR
/CL	Запуск программы в пакетном режиме
/CU[D][R][P]	Лечение файлов и системных областей дисков, удаление найденных вирусов. Если указан параметр D, тогда инфицированные файлы не лечатся, а просто удаляются с диска компьютера. Вместо удаления инфицированных файлов их можно переименовать. Для этого следует указать параметр R. В этом случае первый символ в расширении имени файла заменяется на символ 'V'. Если указан дополнительный параметр P, тогда перед удалением вирусов запрашивается подтверждение у пользователя

/DA	Проверка компьютера один раз в сутки. Этот режим рекомендуется использовать для запуска программы из файла AUTOEXEC.BAT
/DL	Удаление файлов, восстановление которых невозможно
/FN	Если видеоадаптер компьютера не русифицирован, укажите этот параметр. Doctor Web будет пользоваться собственными русскими шрифтами
/HA[<уровень>]	Эвристический анализ файлов и поиск в них неизвестных вирусов. Существует два уровня анализа: 0 - минимальный, 1 - максимальный. По умолчанию устанавливается минимальный уровень эвристического анализа
/HI	Поиск вирусов в адресном пространстве оперативной памяти от 0 Кбайт до 1088 Кбайт
/RV	Контроль за заражением проверяемых файлов активным резидентным вирусом
/TD<диск>:	Когда Doctor Web проверяет упакованные файлы и файлы архивов, он может создавать временные файлы. Вы можете самостоятельно задать диск, на котором создаются временные файлы, с помощью параметра /TD
/UP[N]	Проверка выполнимых файлов, упакованных программами DIET, PKLITE, LZEXE, EXEPACK, PROTECT, COMPACK, CRYPTCOM, а также файлов, вакцинированных антивирусом CPAV. Чтобы Doctor Web не отображал на экране названия программы архиватора, использованной для упаковки проверяемого файла, укажите дополнительный параметр N

Как найти вирус

Программа Doctor Web позволяет обнаружить вирусы без предварительной загрузки компьютера с чистой системной дискеты. Вы можете вызывать Doctor Web каждый раз во время загрузки компьютера, поместив вызов программы в файл AUTOEXEC.BAT. Лучше всего использовать Doctor Web совместно с ревизором диска ADInf. Подробнее об этом можно прочитать в разделе “Взаимодействие программ антивирусного комплекта”.

Для первоначальной проверки компьютера можно использовать следующую команду:
DRWEB * /CL /HA1 /HI /RV /UP /AR /OK

Полифаг Doctor Web проверит оперативную память компьютера, затем автоматически подключит все файлы вирусных баз-дополнений, расположенных в каталоге программы. Затем начнется последовательная проверка всех выполняемых

файлов на всех дисках компьютера. Также будут проверяться файлы внутри файлов архивов.

В памяти компьютера вирусов не обнаружено
Подключение файла WEB60109.308 :
Файл-дополнение подключен к вирусной базе программы.
Добавлено определений новых вирусов - 42
Поиск вирусов и инфицированных программ на диске C :
Метка тома: WORK DISK
c:\PILOT.ARJ - архив ARJ
c:\BALLON\SCREEN\SCR.ARJ - архив ARJ
c:\BALLON\REPORT.WEB - Ok
c:\BALLON\MENU\MENU.ARJ - архив ARJ
c:\NC45\BITMAP.EXE упакован EXEPACK
c:\NC45\RBVIEW.EXE /

После окончания проверки, Doctor Web отображает на экране отчет о проделанной работе. В нем указывается количество проверенных файлов и загрузочных секторов, количество обнаруженных вирусов и время проверки компьютера:

Отчет для диска C:
Проверено : файлов и загрузочных секторов - 245
Обнаружено: вирусов и инфицированных программ - 0
Время сканирования: 00:05:39

Если во время проверки будут обнаружены вирусы, программа сообщит об этом. Напротив названия каждого зараженного файла указывается имя обнаруженного в нем вируса.

Поиск вирусов и инфицированных программ на диске C :
BOOT SECTOR инфицирован Form
c:\TETRA\DWOL.EXE - Ok
c:\TETRA\DSORT.LST - Ok
c:\TETRA\REPORT.WEB - Ok
c:\TETRA\OVLOAD\KELA.EXE инфицирован TPE.Kela.4546
c:\TETRA\OVLOAD\EBBOI.COM инфицирован HelloUser.402
c:\TETRA\OVLOAD\APOC1.COM - Ok
c:\GAME\APOC1016.EXE - Ok
c:\GAME\GREEN.COM - Ok
c:\GAME\KLOM.EXE инфицирован XAM.278
c:\GAME\DOOM2DTH.EXE инфицирован Doom.666
c:\GAME\GKBEC.COM инфицирован Beer.3490
c:\NETLOG.EXE инфицирован Novell.3120

Вместе с антивирусом Doctor Web поставляется файл с описаниями известных вирусов VIRLIST.WEB. Перед тем как удалять обнаруженные вирусы, рекомендуется прочитать их описания. Файл VIRLIST.WEB может поставляться в архиве VIR-WEB.LZH. Для восстановления файлов из этого архива используйте архиватор LHA.

При проверке компьютера в режиме эвристического анализа, Doctor Web, может сообщить о том, что файл инфицирован неизвестным вирусом. Название неизвестного

вируса составляется из слова Virus и одного или нескольких терминов, описанных в следующей таблице:

Термин	Обнаружен
COM	Вирус, заражающий COM-файлы
EXE	Вирус, заражающий EXE-файлы
TSR	Резидентный вирус
BOOT	Вирус, заражающий загрузочные секторы дисков
CRYPT	Зашифрованный или полиморфный вирус

Названия обнаруженных таким образом вирусов могут выглядеть следующим образом:

D:\PROGRESS\VIDID\NCAA.EXE возможно инфицирован COM.CRYPT.Virus
D:\PROGRESS\FOXWOOD\README.EXE возможно инфицирован EXE.TSR.Virus
D:\FORMER\LOOM.EXE возможно инфицирован COM.EXE.TSR.CRYPT.Virus

Эти сообщения означают, что эвристический анализ данных файлов обнаружил подозрительные участки кода, характерные для вирусов. Такие файлы нужно передать специалистам для дальнейшего изучения.

Как лечить компьютер

Если проверка компьютера обнаружила вирусы, вам надо приступить к его лечению. Для этого необходимо загрузить компьютер с системной дискеты и запустить с нее программу Doctor Web. Системная дискета должна быть подготовлена заранее на компьютере, не зараженном вирусами, и на ней должна быть установлена защита от записи.

После перезагрузки компьютера с системной дискеты загрузите Doctor Web:

DRWEB */CL /NM /TDC: /UP /CU

Теперь полифар Doctor Web не только будет обнаруживать вирусы, а будет их удалять.

Поиск вирусов и инфицированных программ на диске C :
BOOT SECTOR инфицирован Form - исцелен!
c:\TETRA\OVLOAD\KELA.EXE инфицирован TPE.Kela.4546 - исцелен!
c:\TETRA\OVLOAD\EBBOI.COM инфицирован HelloUser.402 - исцелен!
c:\GAME\KLOM.EXE инфицирован XAM.278 - исцелен!
c:\GAME\DOOM2DTH.EXE инфицирован Doom.666 - исцелен!
c:\GAME\GKBEC.COM инфицирован Beer.3490 - исцелен!
c:\NETLOG.EXE инфицирован Novell.3120 - исцелен!

Если во время проверки компьютера, Doctor Web обнаружил зараженные файлы внутри файла архива, то он не сможет вылечить их автоматически. Архив надо раскрыть, а затем вылечить все зараженные файлы. После этого вы можете снова записать вылеченные файлы в архив.

Диалог с Doctor Web

Мы рассказали как работать с Doctor Web в пакетном режиме. Такой способ удобен при автоматической проверке компьютера. Для проверки в ручном режиме значительно удобнее пользоваться диалоговым режимом программы.

Чтобы запустить Doctor Web в диалоговом режиме не указывайте параметр /CL. Остальные параметры также можно не указывать, вы сможете их задать или изменить непосредственно во время работы программы.

Как подключить файлы-дополнения для вирусной базы

Новые вирусы появляются с завидной регулярностью. Для их удаления необходимо постоянно пополнять базу данных программы, содержащую информацию о вирусах. Программа Doctor Web позволяет подключать к этой базе данных внешние файлы-дополнения, содержащие сведения о новых вирусах.

Файлы-дополнения выпускаются постоянно, по мере поступления и изучения новых вирусов. Вы можете получить их через модем с BBS “ДиалогНаука”, по сети FIDO из эхо-конференции ADinf.Support, или по сети Relcom из телеконференции REL.FIDO.ADINF.SUPPORT.

В случае крайней необходимости можно получить файлы дополнений в текстовом виде через факсимильный аппарат, а затем ввести их в компьютер, набрав в любом текстовом редакторе. Если факсимильного аппарата у вас нет, файл дополнений в принципе можно записать на слух по телефону.

Файлы-дополнения имеют имена WEBymmdd.vvv. Символ *u* означает последнюю цифру года, *mm* - номер текущего месяца, *dd* - день месяца выпуска файла-дополнения, а *vvv* - номер версии программы, для которой предназначен файл. Если вы получили файл-дополнение по сети, то его надо сохранить в файле с соответствующим именем.

Чтобы подключить новые файлы-дополнения, запишите их в каталог программы Doctor Web. После запуска программы они подключатся автоматически. Вы можете выделить для файлов дополнений отдельный каталог и указать к нему путь в диалоговой оболочке Doctor Web.

Вирусы для текстового процессора Microsoft Word for Windows

Программа Doctor Web позволяет обнаружить на диске компьютера известные вирусы, распространяющиеся в среде текстового процессора Microsoft Word for Windows. Для этого следует ей указать на необходимость проверки файлов документов, имеющих расширения DOT и DOC.

Если такие вирусы будут обнаружены, воспользуйтесь для их удаления антивирусом Doctor Web for WinWord. Этот антивирус описан в следующем разделе “Антивирус Doctor Web for WinWord”. Антивирусная программа Doctor Web, предназначенная для работы в среде DOS, может только обнаружить вирусы в файлах-документах, но не удалять их.

Антивирус Doctor Web for WinWord

В разделе “Вирусы в файлах документов” мы рассказали о новом типе вирусов, заражающих файлы документов, подготовленные в текстовом процессоре Microsoft Word for Windows версии 6.0 и 7.0. В момент написания книги были известны всего несколько таких вирусов WinWord.Concept, WinWord.Nuclear, WinWord.Color.

Для борьбы с вирусами в текстовых файлах документов Даниловым Игорем Анатольевичем был разработан специальный антивирус Doctor Web for WinWord. Он может быть использован для обнаружения и удаления известных и неизвестных вирусов. Doctor Web for WinWord не является программой в полном смысле этого слова, скорее это документ, содержащий макрокоманды антивируса. В настоящее время он распространяется в файле с именем DRWEBWW.DOC.

В настоящее время Doctor Web for WinWord распространяется совершенно свободно. Вы можете получить это средство непосредственно в офисе АО “ДиалогНаука” или через модем со станции BBS “ДиалогНаука”

Чтобы установить Doctor Web for WinWord, достаточно запустить текстовый процессор Microsoft Word for Windows и загрузить в него файл DRWEBWW.DOC. В момент открытия файла среда текстового процессора будет автоматически проверена на заражение вирусами. Обнаруженные вирусы можно сразу же удалить.

Если вирусов не найдено, тогда вам будет предложено установить Doctor Web for WinWord. Согласитесь с этим предложением, в случае необходимости вы всегда сможете отключить антивирус, открыв файл DRWEBWW.DOC еще один раз. После окончания установки в главном меню Microsoft Word for Windows появится меню Dr.Web (рис. 3.1). Через это меню пользователь может настроить антивирус и выполнить проверку текстовых документов.

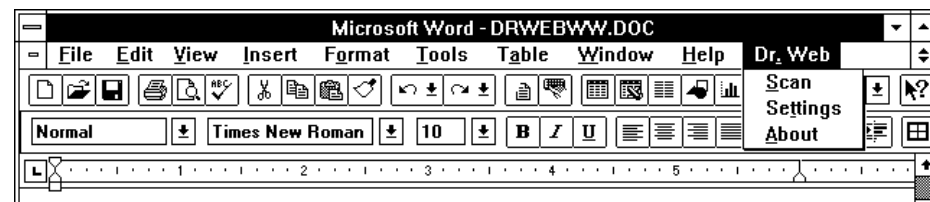


Рис. 3.1. Меню Doctor Web for WinWord

Настройка режимов работы Doctor Web for WinWord не должна вызвать у вас никаких затруднений. Откройте диалоговую панель настройки антивируса, выбрав из меню Dr.Web строку Settings. На экране появится диалоговая панель, показанная на рисунке 3.2.

Если вы установили у себя Doctor Web for WinWord, его можно настроить на поиск вирусов в открываемых файлах. Такая функция очень удобна, так как у вас отпадает необходимость частой проверки всех файлов документов. Даже если вы запишете на жесткий диск компьютера зараженный документ, вирус не сможет заразить вашу систему, так как он будет обнаружен в момент открытия файла.

Тем не менее, в любом случае желательно периодически проверять все файлы документов, хранимые в компьютере, даже если они не используются. В противном случае незамеченный зараженный файл может быть передан на другой компьютер, не защищенный Doctor Web for WinWord.

Антивирус Doctor Web for WinWord позволяет выполнять эвристический анализ макрокоманд проверяемых файлов. Для этого надо включить переключатель Strange macro (рис. 3.2). Такой режим позволяет обнаружить подозрительные макрокоманды, принадлежащие новым, ранее неизвестным вирусам.

Обнаружив подозрительные макрокоманды, Doctor Web for WinWord предлагает их удалить. Вы должны самостоятельно проверить эти макрокоманды и решить вопрос об их удалении.

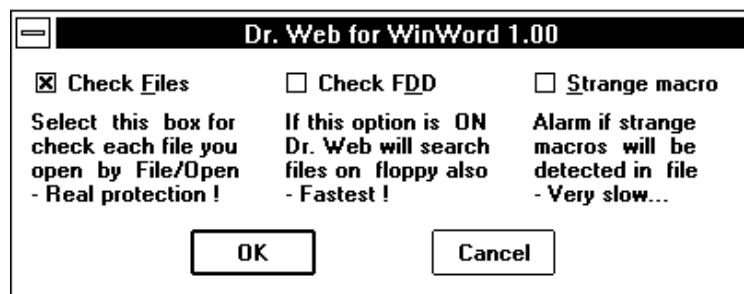


Рис. 3.2. Выбор режима работы Doctor Web for WinWord

Чтобы начать проверку дисков компьютера, выберите из меню Dr.Web строку Scan. Антивирус проверит, сколько дисков компьютера доступно и откроет диалоговую панель с кнопками, названия которых соответствуют именам этих дисков. Doctor Web for WinWord позволяет проверить не только жесткие диски компьютера, но также компакт-диски, сетевые диски и дискеты.

Перед тем как вы сможете проверять документы, записанные на дискетах, установите в диалоговой панели настройки антивируса переключатель Check FDD. Вставьте дискету, которую надо проверить, в дисковод и выберите из Dr.Web строку Scan. Теперь в открывшейся диалоговой панели появится кнопка для проверки дискет.

Файлы документов, поступающие вам от других пользователей, следует проверять на заражение вирусами. Обязательно проверяйте файлы, поступившее к вам по электронной почте и полученные со станций BBS.

Обнаружив вирус, Doctor Web for WinWord предлагает его удалить. Перед удалением вируса мы рекомендуем сделать резервную копию зараженного документа. После того как вы убедитесь в том, что вирус удален и документ не поврежден, удалите резервную копию зараженного документа.

После удаления вируса из файла документа он остается в формате файла стилей. Если вы решите сохранить такой документ в другом формате и выберете из меню File строку Save As, то увидите, что в открывшейся диалоговой панели Save As, список форматов Save as type будет недоступен. Чтобы исправить формат документа, откройте новый документ, выбрав из меню File строку New, скопируйте в него через универсальный обменный буфер Clipboard содержимое исходного файла, а затем сохраните новый документ. Теперь старый документ можно удалить и работать с новым документом.

Ревизор диска ADinf и лечащий модуль ADinf Cure Module

Использование антивирусных программ не может гарантировать полную защиту компьютера от заражения вирусами. Антивирусные программы-полифаги типа Aidtest и Doctor Web в первую очередь настроены на обнаружение уже известных вирусов и их клонов. В Doctor Web есть эвристический анализатор, обнаруживающий большинство новых вирусов, но все же существует небольшая вероятность появления вируса, который не будет обнаружен. Кроме того, даже если новый вирус будет обнаружен, вылечить его сразу не удастся. Поэтому в антивирусный комплект включена программа-ревизор ADinf, созданная Мостовым Дмитрием Юрьевичем.

Ревизор диска ADinf сохраняет в своих таблицах различную информацию о жестком диске компьютера - загрузочных секторах, сбойных кластерах, структуре каталогов и выполнимых файлах (рис. 3.3). Это позволяет выявить любой вирус, как только он проявит себя и попытается заразить новые файлы или загрузочные секторы.

Так как стелс-вирусы перехватывают обращения к дисковой подсистеме компьютера и скрывают присутствие вируса, ADinf считывает информацию с диска, минуя операционную систему. Для чтения диска ADinf обращается непосредственно к соответствующей функции BIOS, записанной в ПЗУ компьютера. В этом случае вирус не может перехватить обращение к диску, и ADinf получает достоверную информацию.

На этом, в частности, основан метод поиска активных стелс-вирусов. Ревизор ADinf считывает проверяемые файлы и загрузочные секторы двумя способами: через операционную систему и непосредственно через вызов BIOS. Полученные данные сравниваются. Если между ними обнаруживаются различия, значит в памяти находится активный стелс-вирус, скрывающий свое присутствие.

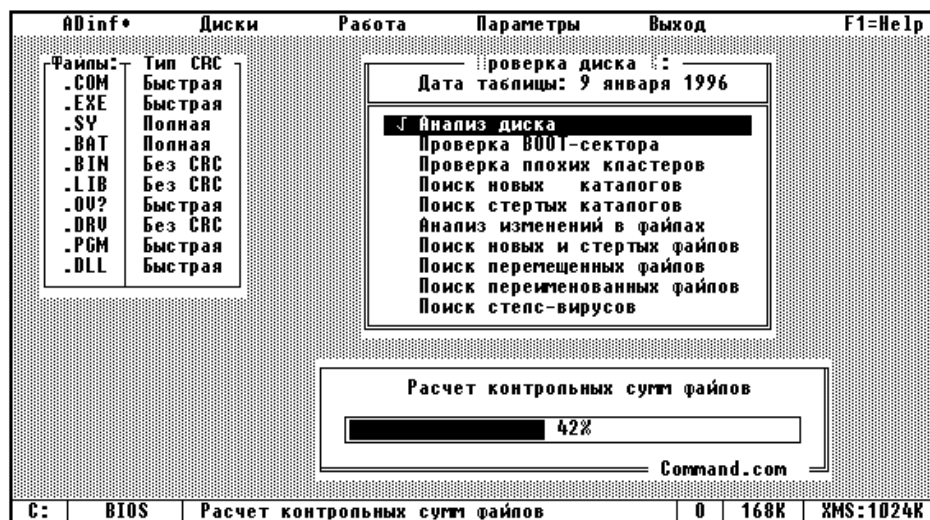


Рис. 3.3. Проверка диска ревизором ADInf

В состав антивирусного комплекта входит дополнительный модуль ADInf Cure Module, предназначенный для использования совместно с ревизором ADInf. ADInf Cure Module разработан Ладыгиным В. С., Зуевым Д. Г. и Мостовым Д. Ю. В нашей книге мы рассматриваем ADInf версии 10.5a и лечащий модуль ADInf Cure Module версии 3.03.

Дополнив ревизор ADInf лечащим модулем ADInf Cure Module, вы получаете возможность не только обнаружить появление вируса, но также и удалить его. Интересно, что ADInf Cure Module не содержит вирусной базы данных и может удалить даже новый, ранее неизвестный вирус. Для этого лечащий модуль использует информацию о зараженном файле, собранную им до того, как файл был поражен вирусом. Версии 3.03 и 3.04 ADInf Cure Module позволяют удалить вирусы из COM-, EXE-, SYS-, XTP- и BAT-файлов.

Когда книга готовилась к публикации, вышла новая версия ревизора ADInf 10.6 и лечащий модуль ADInf Cure Module версии 3.04. По сравнению с предыдущими версиями программ, в них добавлена возможность установки ADInf и ADInf Cure Module на сетевом диске.

Теперь при работе в локальной сети ADInf и ADInf Cure Module можно установить на сервере, что облегчит администратору смену версий программ. При запуске с сетевого диска ADInf по умолчанию ищет свой файл настроек и личные таблицы в каталоге C:\ADINF на локальной машине. Этот каталог можно изменить, указав дополнительный параметр -HOME:<путь>. Улучшена совместимость с новой операционной системой Windows 95 - изменен алгоритм работы с файлами при лечении, что обеспечивает сохранение длинных имен файлов.

Несколько слов о настройке ADInf

Программа ADInf позволяет настроить режим проверки компьютера, чтобы достичь лучшего результата. Настройка программы достаточно сложна и описана в документации к программе. Поэтому мы ограничимся кратким описанием самых важных возможностей настройки программы.

Во время проверки компьютера ADInf записывает полученную информацию в таблицы, расположенные в специальных файлах. Таблицы ADInf бывают двух типов - общие и личные. Общие таблицы создаются в корневых каталогах проверяемых дисков. Личные таблицы создаются в каталоге ADInf или в любом другом указанном пользователем каталоге. Несколько пользователей одного компьютера могут иметь собственные копии личных таблиц в своих каталогах и независимо контролировать диски. Выбрать работу с личными или общими таблицами можно в меню Параметры.

Режим проверки компьютера устанавливается в меню Параметры. Для этого надо выбрать строку Режимы работы. Можно включить быстрый режим поиска (режим fast) и режим поиска (режим info).

В быстром режиме не проверяются контрольные суммы файлов, и вы узнаете только о новых и стертых файлах и каталогах, а также о файлах, у которых изменилась длина. Таблицы с информацией о диске обновляться не будут. Режим поиска выполняет полную проверку диска без обновления информации в таблицах ревизора.

Для ежедневной проверки компьютера рекомендуется отключить быстрый режим и режим поиска. В этом случае будут проверяться контрольные суммы файлов, что позволит обнаружить изменения в их структуре.

Вы можете указать, как вычислять контрольные суммы файлов с различными расширениями. Для этого выберите из меню Параметры строку Настройка, а затем в открывшемся временном меню выберите строку Список расширений. Откроется временное меню, содержащее две строки - Расширения и Тип CRC. Первая строка позволяет изменить список расширений контролируемых файлов, а вторая позволяет выбрать тип контрольных сумм для файлов с данным расширением.

В ревизоре ADInf реализованы три типа контрольных сумм - Без CRC, Быстрая и Полная. Тип Без CRC, означает что контрольная сумма не будет рассчитываться. Быстрые контрольные суммы основаны на знании внутренней структуры исполняемых файлов с расширениями COM и EXE. Этот тип контрольных сумм надежно защищает выполнимые файлы от внедрения в них вируса, но некоторые изменения в выполнимых файлах, не связанные с внедрением вирусов, могут остаться незамеченными. Полные контрольные суммы рассчитываются на основе всего файла. Любые изменения файла будут обнаружены. Надо заметить, что полные контрольные суммы рассчитываются медленнее быстрых.

Наиболее важно правильно указать объекты (загрузочные записи, файлы и т. д.), контролируемые ревизором ADInf. Выберите из меню Параметры строку Настройки, а

затем из открывшегося временного меню строку Что контролировать. На экране появится меню Контроль (рис. 3.4).

Через это меню можно указать, какие файлы подлежат контролю - только с указанными расширениями или все, ввести список неизменяемых файлов, включить контроль загрузочных секторов, проверять вновь появившиеся плохие кластеры, проверять структуру каталогов, выполнять контроль таблицы параметров жестких дисков HDPT, а также выполнять автоматическую проверку на стелс-вирусы в новых и измененных файлах.

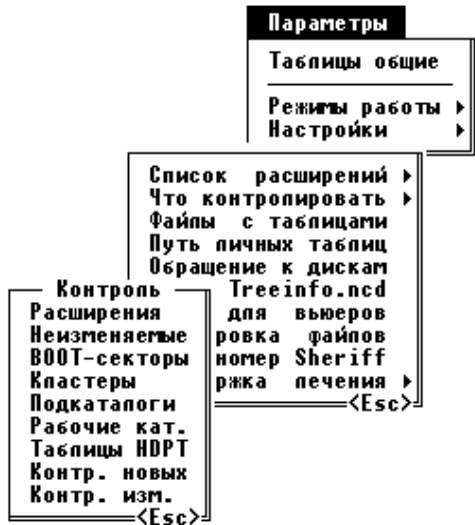


Рис. 3.4. Выбор вида контро ля

Мы рекомендуем обязательно включить контроль за всеми выполнимыми файлами и загрузочными секторами. Необходимо также включить проверку на стелс-вирусы в новых и измененных файлах. Это позволит ADInf сразу сообщить вам о появлении вирусов в компьютере.

Для каждого логического диска компьютера можно отдельно задать метод обращения к дискам. Выберите из меню Параметры строку Настройки, а затем из открывшегося временного меню строку Обращение к дискам. На экране появится список имен логических дисков компьютера. С помощью клавиш управления курсором и клавиши пробела для каждого диска можно указать метод обращения - BIOS, Int 13h, Int 25h.

Метод BIOS предполагает, что ADInf обращается к дискам компьютера, непосредственно вызывая процедуры, записанные в ПЗУ BIOS. Это позволяет преодолеть маскировку стелс-вирусов и прочитает именно ту информацию, которая записана на диске. Вирус не может в этом случае вмешаться и исказить данные, считанные с диска.

Некоторые вирусы пытаются маскироваться даже при чтении диска процедурами BIOS. Для этого они перехватывают специальное прерывание Int 76h, вырабатываемое контроллером жесткого диска по окончании некоторых операций, и искажают считанные данные фактически на уровне контроллера жесткого диска. Ревизор ADInf применяет специальные методы и не позволяют таким вирусам остаться незамеченными.

В некоторых ситуациях ADInf не может воспользоваться процедурами BIOS для доступа к дискам. Как правило, это происходит, если установлены драйверы дисков, например драйвер Disk Manager или драйверы SCSI-дисков. В этом случае выберите для этих дисков метод доступа Int 13h.

Если в вашей системе установлены программы динамического сжатия - DoubleSpace, DriveSpace, SuperStor или Stacker, тогда для этих дисков надо установить метод доступа Int 25h. Этот метод предполагает обращение к дискам средствами операционной системы DOS.

Методы доступа Int 13h и Int 25h оказываются для стелс-вирусов больше
возможны и для маскировки, поэтому предпочтительней пользоваться
методом доступа BIOS

Проверка компьютера

Перед проверкой компьютера выберите диски, которые надо проанализировать. Их названия следует выбрать из меню Диски. Для этого установите курсор на соответствующую строку меню с именем диска и нажмите клавишу <Insert> или клавишу пробела. Около названия диска появится знак плюс (рис. 3.5).



Рис. 3.5. Выбор дисков для проверки

Чтобы начать проверку компьютера, воспользуйтесь меню Работа, представленным на рисунке 3.6. Для проверки устройств, помеченных в меню Диски, выберите строку Проверить диск. Если проверить надо все диски компьютера, достаточно выбрать строку Проверить все. В этом случае не надо предварительно указывать проверяемые устройства в меню Диски.



Рис. 3.6. Проверка компьютера

Если ADInf обнаружит, что на диске произошли изменения, характерные для заражения вирусами, на экране появляется предупреждающее сообщение (рис. 3.7). Все найденные подозрительные изменения помечены символом ∇ . Для продолжения работы нажмите любую клавишу на клавиатуре компьютера. Диалоговая панель с предупреждающим сообщением закроется и вы сможете перейти к изучению результатов проверки диска (рис. 3.8).

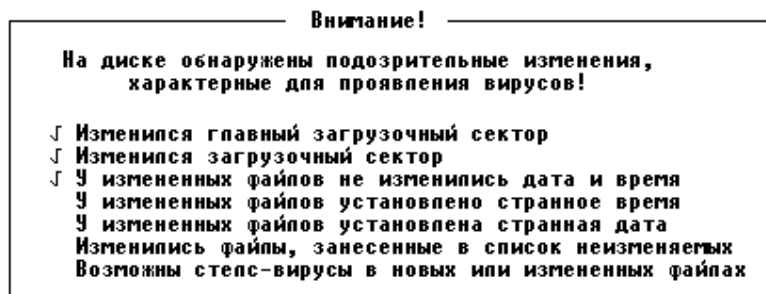


Рис. 3.7. Предупреждающее сообщение ADInf

Возможно, что изменения в файловой системе вызваны не заражением вирусами, а другими причинами. Например, изменение загрузочных секторов может быть вызвано установкой новой версии операционной системы. Странная дата создания файла (например, дата больше 2000 года) могут быть вызваны неправильной установкой часов компьютера. Изменение файлов, занесенных в список неизменяемых, может быть вызвано установкой новых версий этих программ.

Чтобы подробнее изучить обнаруженные программой ADInf изменения, выберите из списка “Изменения на диске” нужную позицию и нажмите клавишу <Enter>.

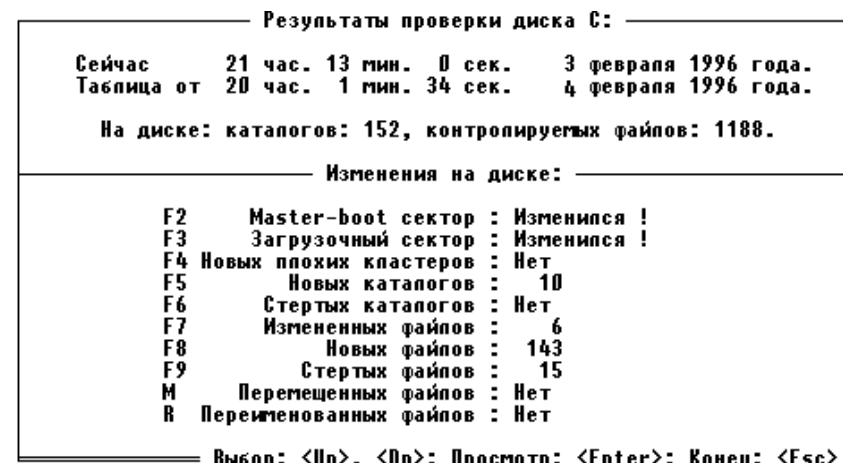


Рис. 3.8. Результаты проверки диска

Наиболее подозрительны изменения в секторе главной загрузочной записи (на рисунке она называется Master-boot сектор), загрузочном секторе и выполнимых файлах. Сообщения об их изменении ни в коем случае нельзя оставлять без внимания.

Чтобы подробнее изучить изменения в секторе главной загрузочной записи выберите первую строчку в списке “Изменения на диске” или нажмите клавишу <F2>. На экране появится диалоговая панель Master-boot сектор, содержащая информацию о главном загрузочном секторе (рис. 3.9). Строка в верхней части панели сообщает об изменении программы начальной загрузки - “Изменился загрузчик”. Если вы не устанавливали новой версии операционной системы, то, скорее всего, компьютер заражен загрузочным вирусом.

Ниже расположены две таблицы, отражающие состояние таблицы разделов в настоящий момент и во время предыдущей проверки. Более подробно об этих таблицах вы можете узнать в главе “Восстановление файловой системы”.

Master-boot сектор Изменился загрузчик!									
Прекняя таблица									
Sys	Boot	Side	Начало Cyl	Sect	Side	Конец Cyl	Sect	Относит. сектор	Количество секторов
6h	80h	1	0	1	63	203	63	63	822465
5h	0h	0	204	1	63	523	63	822528	1290240
0h	0h	0	0	0	0	0	0	0	0
0h	0h	0	0	0	0	0	0	0	0
Новая таблица									
Sys	Boot	Side	Начало Cyl	Sect	Side	Конец Cyl	Sect	Относит. сектор	Количество секторов
6h	80h	1	0	1	63	203	63	63	822465
5h	0h	0	204	1	63	523	63	822528	1290240
0h	0h	0	0	0	0	0	0	0	0
0h	0h	0	0	0	0	0	0	0	0

Выход: <Esc>

Рис. 3.9. Изменения в секторе главной загрузочной записи

Программа ADInf позволяет восстановить старую главную загрузочную запись, которая была сохранена во время предыдущей проверки компьютера. Используйте эту возможность, только если вы полностью уверены, что со времени последней проверки на компьютере не было установлено программное обеспечение, меняющее главную загрузочную запись. Главная загрузочная запись может быть изменена во время установки новой версии операционной системы, программы распределения доступа и некоторых систем защиты от копирования.

Перед тем как начинать восстановление сектора главной загрузочной записи или загрузочного сектора мы рекомендуем сделать резервные копии ваших файлов документов и баз данных, хранимых в компьютере

Если изменился загрузочный сектор диска, вы можете детально просмотреть изменения. Для этого надо выбрать из диалоговой панели Результаты проверки диска (рис. 3.8) строку Загрузочный сектор или нажать клавишу <F3>. На экране откроется новая диалоговая панель, показанная на рисунке 3.10.

Таблицы BOOT-сектора		старого	нового
Jump на загрузчик		не изменился	
Метка поставщика DOS		MSWIN4.0	MSWIN4.0
Размер сектора		512	512
Число резервных секторов		1	1
Число копий FAT		2	2
Входов в корневой каталог		512	512
Всего секторов		--	--
Байт описания носителя		F8h	F8h
Число секторов в FAT		201	201
Число секторов в дорожке		63	63
Число поверхностей диска		64	64
Число скрытых секторов		63	63
Общее количество секторов		822465	822465
Физический номер носителя		80h	80h
Признак расширенного BPB		29h	29h
Серийный номер носителя		530366163	539854634
Метка тома			
Тип файловой системы		FAT16	FAT16
Область загрузчика DOS		не изменилась	
		Выход: <Esc>	

Рис. 3.10. Изменения в загрузочном секторе

Особое внимание в этой диалоговой панели следует обратить на изменение команды перехода на программу загрузки операционной системы (Jump на загрузчик) и изменение самой программы загрузки (Область загрузчика DOS). Их изменение может быть вызвано заражением компьютера загрузочным вирусом.

Обнаружив с помощью ADInf изменения в секторе главной загрузочной записи, загрузочном секторе или в выполняемых файлах, проверьте компьютер с помощью полифазов Aidstest и Doctor Web. Ревизор ADInf сразу может восстановить старые загрузочные сектора, но если компьютер был заражен вирусами типа OneHalf или VolGU, можно потерять информацию, записанную на дисках компьютера

Загрузочный сектор, как правило, изменяется при установке новой версии операционной системы, некоторых систем распределения доступа и после форматирования диска командой FORMAT. Конечно, в этих случаях вируса в компьютере, скорее всего, нет и восстанавливать старый загрузочный сектор не надо.

С большим вниманием надо отнестись к изменениям в выполнимых файлах. Если ADInf обнаружит такие файлы, просмотрите их список. Для этого выберите в диалоговой панели Результаты проверки диска (рис. 3.8) строку Измененных файлов или нажмите клавишу <F7>. На экране появится диалоговая панель Изменившиеся файлы (рис. 3.11).

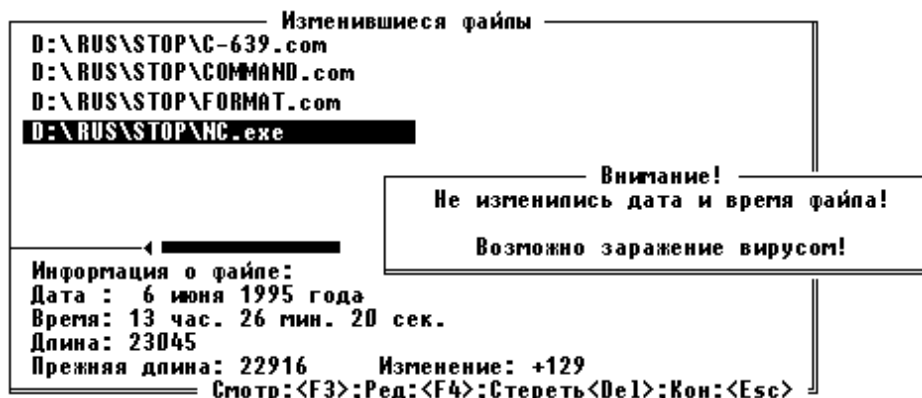


Рис. 3.11. Изменение выполнимых файлов

Просмотрите весь список изменившихся файлов, выбирая их один за другим. ADInf сообщит о каждом файле дату и время его последнего изменения, старую длину файла и его новую длину. Если изменение длины файла не сопровождается изменением даты его последней модификации, возможно файл заражен вирусом.

Особое внимание следует обратить на случаи, когда изменились файлы, занесенные в список неизменяемых. Обычно в этот список включаются основные файлы операционных систем, другие часто используемые выполнимые файлы. По умолчанию в списке неизменяемых файлов включены файлы COMMAND.COM, IBMBIO.COM, IBMDOS.COM, IO.SYS, NC.EXE, NCMAIN.EXE и WIN.COM.

Некоторые программы записывают в свой выполнимый файл различную информацию, например конфигурацию программы и т. д. Но обычно в этом случае меняется дата и время создания файла.

В любом случае рекомендуется проверить все измененные выполнимые файлы при помощи каких-нибудь программ-полифагов. Удобнее всего организовать взаимодействие ревизора ADInf и полифагов Aidstest и Doctor Web. ADInf может подготовить для этих программ список измененных, новых и перемещенных файлов, которые необходимо проверить. Более подробно о возможностях такого взаимодействия программ антивирусного комплекта АО "ДиалогНаука" мы расскажем в разделе Взаимодействие программ антивирусного комплекта.

Лечение зараженных файлов

Одно из преимуществ ADInf перед многими другими программами-ревизорами заключается в лечащем модуле ADInf Cure Module. Если ревизор ADInf обнаружил изменения в выполнимых файлах, характерные для заражения вирусами, а полифаги Aidstest и Doctor Web не могут обнаружить вирус, скорее всего, компьютер заражен новым вирусом, еще не включенным в вирусную базу этих полифагов. Запустите еще раз

полифаг Doctor Web, включив режим эвристического анализа. В этом режиме Doctor Web позволит обнаружить новый вирус, но не сможет удалить их.

Теперь можно воспользоваться лечащим модулем ADInf Cure Module. Он позволяет удалить большинство новых вирусов, еще не известных полифагам Aidstest и Doctor Web.

Лечение файлов надо выполнять, загрузившись с системной лечащей дискеты ADInf Cure Module. Эту дискету необходимо подготовить заранее во время установки ADInf Cure Module. Более подробную информацию о процессе лечения можно получить в документации на антивирусный комплект АО "ДиалогНаука".

Перед тем как загрузиться с лечащей дискеты ADInf Cure Module, установите на ней защиту от записи. В противном случае программа не будет работать

После загрузки компьютера с этой дискеты автоматически запустится программа ADInf Cure Module. После того как вы ответите на несколько вопросов, вы сможете выбрать изменившиеся файлы, которые необходимо вылечить. Программа ADInf Cure Module восстанавливает файл только в том случае, если результирующий файл точно соответствует файлу до его заражения. Если зараженный файл восстановить не удастся, ADInf Cure Module сообщит об этом.

В этом случае воспользуйтесь последними версиями полифагов Aidstest и Doctor Web. Если они также не обнаружат вирус, возможно изменения в файле связаны с заменой файла во время установки новых версий программ.

Рекомендуется дополнительно установить резидентный монитор, например VSafe - он входит в состав дистрибутива операционной системы MS-DOS и некоторое время поработать в таком режиме. Если компьютер заражен вирусом, он рано или поздно себя проявит. Об этом вам сообщит резидентный монитор. Если резидентный монитор будет срабатывать, сообщая о нарушении защиты, постарайтесь передать подозрительные файлы, обнаруженные ADInf, специалистам по вирусам для их дальнейшего исследования.

Взаимодействие программ антивирусного комплекта

Программы антивирусного комплекта являются не просто набором дополняющих друг друга программ, они могут и должны использоваться совместно. Рекомендуется следующая последовательность установки и использования комплекта.

Перед установкой программ антивирусного комплекта в компьютер проверьте его на заражение известными вирусами. Для этого воспользуйтесь антивирусными программами полифагами Aidstest и Doctor Web.

Затем установите программы антивирусного комплекта на жесткий диск компьютера - Aidstest, Doctor Web, ADInf и ADInf Cure Module, руководствуясь документацией комплекта или отдельных программ. Если вы работаете в среде операционной системы

Windows или Windows 95 и используете текстовый процессор Microsoft Word for Windows версии 6.0 или 7.0, установите антивирус Doctor Web for WinWord.

Ревизор диска ADInf позволяет создать список новых и измененных файлов, требующих проверки антивирусными программами полифагами Aidstest и Doctor Web. Вы можете создать специальный пакетный файл, в котором сначала вызывается ADInf, а затем антивирусы-полифаги. Вот пример такого файла.

```
@echo off

ADINF * /@C:\ADDTEST.LST /A

if errorlevel 50 goto end
if errorlevel 40 goto vir_in_mem
if errorlevel 30 goto end
if not exist C:\ADDTEST.LST goto end

DRWEB /@+C:\ADDTEST.LST /CL /HA1 /RV /HI /UPN /NS

if errorlevel 2 goto new_vir
if errorlevel 1 goto vir

AIDSTEST /@C:\ADDTEST.LST /G /NB

if errorlevel 3 goto end
if errorlevel 2 goto end
if errorlevel 1 goto vir

:no_vir
    echo Вирусы не обнаружены
    goto end

:vir_in_mem
    pause Обнаружен активный вирус, противодействующий ADInf
    goto end

:vir
    pause Внимание! Обнаружен известный вирус
    goto end

:new_vir
    pause Внимание! Подозрение на неизвестный вирус

:end
```

Для надежной проверки диска важно правильно настроить список расширений проверяемых файлов и режимы работы ADInf, чтобы не пропустить существенных изменений на диске. Настройка ADInf наиболее полно описана в документации на антивирусный комплект АО “ДиалогНаука”.

Если среди измененных файлов, антивирусы Aidstest или Doctor Web обнаружат вирусы, рекомендуется перезагрузить компьютер с ранее подготовленной системной дискеты, на которой записаны Aidstest и Doctor Web, и проверить все файлы и загрузочные записи на дисках компьютера.

Можно организовать более сложное взаимодействие антивирусов, чем в приведенном нами примере. Например, можно повторно вызывать антивирусы-полифаги для лечения зараженных файлов и выполнить заключительный вызов ADInf для окончательной проверки компьютера. Однако надо иметь в виду, что такое автоматическое лечение очень опасно. Перед лечением зараженных файлов и загрузочных записей рекомендуется провести анализ ситуации и как минимум сделать резервные копии ваших документов и файлов баз данных.

Программно-аппаратный комплекс Sheriff

Дополнительно к антивирусному комплекту АО “ДиалогНаука” можно приобрести программно-аппаратный комплекс защиты Sheriff. Совместное использование традиционных антивирусных программ и контроля с помощью аппаратных средств обеспечивают наибольшую безопасность системы.

Комплекс, разработанный Фоминым Юрием Николаевичем, включает адаптер защиты и управляющее им программное обеспечение. Адаптер защиты представляет собой плату расширения, предназначенную для установки в системную шину ISA. Плата имеет маленький формат и может быть вставлена в 8-разрядный разъем ISA.

Программно аппаратный комплекс можно использовать с операционными системами, совместимыми с MS-DOS (IBM PC-DOS, DR-DOS, Novell DOS), а также с Microsoft Windows версий 3.1 и 3.11, Microsoft Windows for Workgroups версии 3.11 и новой операционной системой Microsoft Windows 95.

Контроллер защиты контролирует доступ к контроллеру жесткого диска на уровне портов ввода/вывода и сообщает программному обеспечению Sheriff о выполнении любой программой или пользователем несанкционированных действий. Программное обеспечение блокирует дальнейшую работу компьютера, предотвращая возможную порчу программного обеспечения компьютера и записанных в нем данных.

Даже если контроллер жесткого диска подключен к компьютеру через системную шину VLB, PCI или EISA, адаптер защиты будет работать на таком компьютере.

Вот несколько основных возможностей и особенностей комплекса Sheriff:

- Блокирует выполнение операций, характерных для вирусов и про ясных программ. Sheriff предотв ращает формати рование же стки х дисков; запись в

область загрузочных секторов жестких дисков; запись в секторы, распределенные защищаемым файлам, элементов каталогов и таблицы размещения файлов; запись в секторы и логические диски, отмеченные как доступные только для чтения; обращение к дискам в обход специально предназначенного для этого прерывания; прямое обращение к портам контроллера жестких дисков

- Решает проблемы несанкционированного доступа, запрашивая пароль во время начальной загрузки компьютера. Если загрузить защищенный компьютер с дискеты, жесткий диск будет недоступен
- Содержит в себе систему разграничения доступа для нескольких пользователей, позволяющую определить для каждого пользователя пароль и персональные права доступа к ресурсам компьютера
- Защиту Sheriff можно отключить только при помощи специальной установочной дискеты. Другие способы отключения контроля связаны с полной потерей данных

Совместное использование Sheriff и других программ комплекта

Чтобы на компьютере, защищенном комплексом Sheriff, запустить остальные программы антивирусного комплекта, их необходимо настроить соответствующим образом. В противном случае защита сработает и компьютер окажется заблокирован.

Для настройки ADinf и ADinf Cure Module, откройте в ADinf меню Параметры и выберите из него строку Настройки. На экране появится временное меню. Выберите из него строку Сер. Номер Sheriff и введите пять первых цифр серийного номера вашего экземпляра Sheriff. Например, если Sheriff имеет серийный номер 123450981705763, надо ввести цифры 12345 (рис. 3.12).

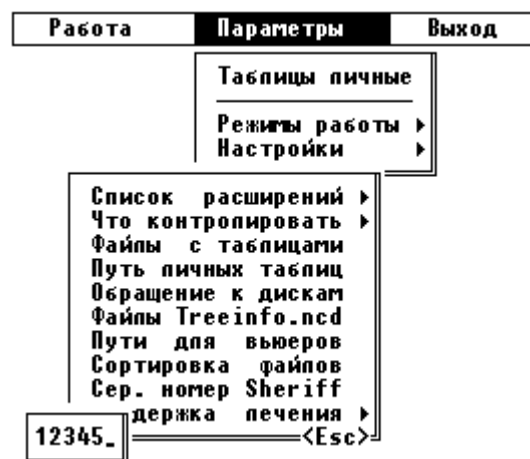


Рис. 3.12. Ввод серийного номера Sheriff

Если вы желаете воспользоваться программами Aidstest, Doctor Web, то в командной строке вызова этих программ надо добавить дополнительный параметр /Z и /SH соответственно, указав после него первые пять цифр серийного номера Sheriff:

AIDSTEST C: /Z12345

DRWEB C: /SH12345

Антивирусный пакет AVP

Антивирусный пакет Antiviral Toolkit Pro (AVP) создан фирмой КАМИ, основной разработчик - Касперский Евгений Валентинович. Пакет AVP позволяет обнаружить и удалить около 6000 различных вирусов. К сожалению, большое количество обнаруживаемых вирусов еще не является полной гарантией от заражения компьютера. Всегда найдется новый вирус, не входящий в вирусную базу программы.

Пакет AVP использует почти все средства для обнаружения вирусов. Он позволяет сканировать файлы, загрузочные записи и оперативную память компьютера в поисках известных вирусов. Анализатор кода может обнаружить большинство новых вирусов, но для их лечения надо получить обновления вирусной базы данных.

Антивирус AVP также позволяет вычислять контрольные суммы проверяемых файлов, а затем периодически проверять их. Расхождения в контрольных суммах файла может служить сигналом, что файл заражен вирусом. В отличие от ревизора ADinf, антивирус AVP не умеет обращаться к дискам компьютера непосредственно через функции BIOS. Поэтому многие активные стелс-вирусы могут оказаться незамеченными AVP.

Однако AVP не дает возможности удалить новые вирусы. В этом плане лучше использовать ADinf и лечащий модуль ADinf Cure Module, входящие в состав антивирусного комплекта АО "ДиалогНаука". ADinf Cure Module позволяет удалить большинство новых вирусов, еще не включенных в вирусные базы программ-полифагов.

Вместе с AVP поставляется антивирусный резидентный монитор Antiviral Monitor. Он позволяет обнаружить и сообщить обо всех проявлениях, которые могут быть вызваны компьютерными вирусами. Antiviral Monitor также позволяет выполнять автоматическую проверку всех запускаемых и открываемых файлов на заражение известными вирусами.

В настоящий момент фирма КАМИ не выпускает программно-аппаратных средств антивирусной защиты, подобных комплексу Sheriff, продаваемых вместе с антивирусным комплектом АО "ДиалогНаука". Поэтому если необходима антивирусная защита высокой надежности, лучше ориентироваться на программно-аппаратный комплекс Sheriff, и антивирусные программы из комплекта АО "ДиалогНаука".

Вместе с AVP можно купить компьютерную энциклопедию вирусов - AVP Virus Encyclopedia. Она содержит описания большого количества вирусов, структурированные по различным признакам. Для наиболее интересных вирусов можно просмотреть и прослушать выполняемые вирусами эффекты.



Рис. 3.13. Вирус Ambulance

Например, для вируса Ambulance энциклопедия AVP Virus Encyclopedia позволяет просмотреть эффект, иногда вызываемый этим вирусом. В нижней части экрана под звуки сирены движется автомобиль скорой помощи (рис. 3.13).

Антивирусны й пакет Microsoft Anti-Virus

В состав дистрибутива операционной системы MS-DOS версии 6.0 и более поздних версий входит программа Microsoft Anti-Virus. Комплект Microsoft Anti-Virus включает в себя не только антивирусы для операционной системы MS-DOS, но также и для Windows. Надо заметить, что этот антивирус не является разработкой самой фирмы Microsoft, а изготовлен фирмой Central Point Software Product.

Новая версия операционной системы Microsoft Windows 95 не содержит встроенных антивирусных средств, в том числе в ней отсутствует Microsoft Anti-Virus. Поэтому для Microsoft Windows 95 вы должны использовать другие средства защиты.

Процедуры установки и использования этих антивирусных программ описаны во втором томе серии "Персональный компьютер. Шаг за шагом". Поэтому мы повторим только самые основные сведения и больше внимания уделим методике использования Microsoft Anti-Virus и его сравнению с другими антивирусными средствами.

Антивирусная программа Microsoft Anti-Virus для MS-DOS выполняет функции полифага и ревизора. Она позволяет обнаружить известные вирусы и вылечить их. Кроме того, она запоминает основную информацию о выполнимых файлах и проверяет ее при последующих запусках.

В отличие от ревизора ADInf, антивирусная программа Microsoft Anti-Virus не умеет обращаться к дискам компьютера непосредственно через функции BIOS. Поэтому многие активные стелс-вирусы могут оказаться незамеченными.

Для запуска Microsoft Anti-Virus для MS-DOS, введите в командной строке DOS следующую команду:

```
MSAV.EXE
```

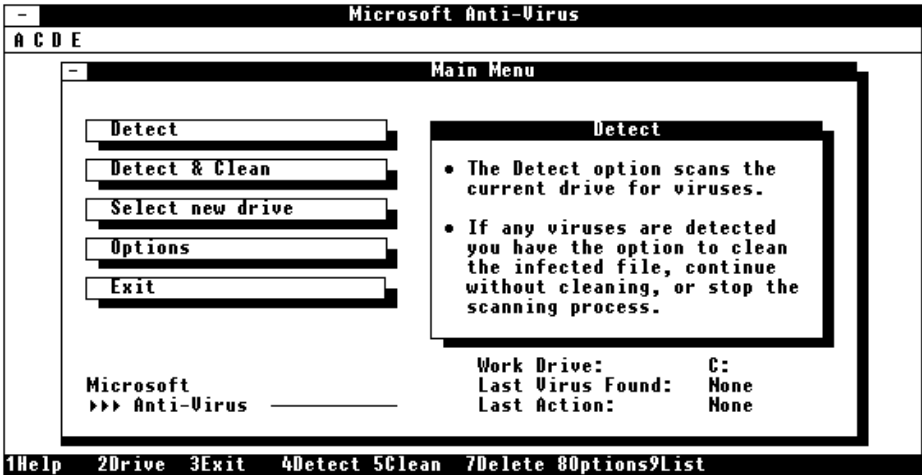


Рис. 3.14. Антивирусная программа Microsoft Anti-Virus для MS-DOS

На экране появится диалоговая оболочка программы (рис 3.14). В верхней части расположен заголовок программы, ниже него список дисков, которые можно проверить. В окне Main Menu находятся 5 кнопок, управляющие работой программы.

Кнопка	Назначение
Detect	Выполнить поиск вирусов
Detect & Clean	Выполнить поиск и удаление вирусов
Select new drive	Выбрать диск для проверки
Options	Установить режим работы Microsoft Anti-Virus
Exit	Закончить работу с Microsoft Anti-Virus

Чтобы изменить режим поиска вирусов, нажмите кнопку Options. На экране появится временная диалоговая панель с переключателями, показанная на рисунке 3.15.

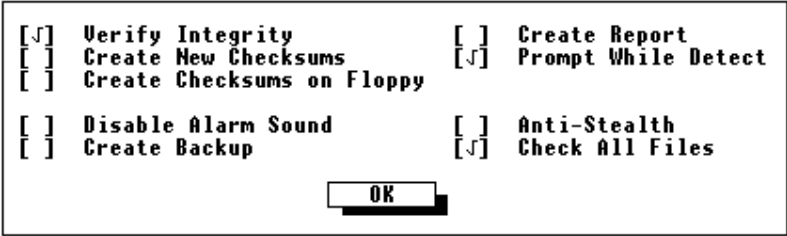


Рис. 3.15. Настрой ка Microsoft Anti-Virus

Переключатель	Режим работы программы
Verify Integrity	Антивирус сверяет информацию, записанную в файлах CHKLIST.MS (см. переключатель "Verify Integrity") с текущими характеристиками файлов. Если при проверке выявляются различия, на экран выдается предупреждающее сообщение
Create New Checksums	Во время проверки файлов на наличие вирусов в каждом каталоге создается файл CHKLIST.MS. В этом файле записываются сведения обо всех выполнимых файлах, содержащихся в каталоге (размер файла, дата создания, атрибуты). К выполнимым файлам относятся все файлы с расширениями EXE, COM, BAT, OV*, SYS, BIN, APP, CMD, PGM, PRG, DRV, DLL, 386, FON, ICO, PIF. При последующих проверках характеристики всех выполнимых файлов сверяются с данными из файлов CHKLIST.MS. Если обнаруживается несовпадение, антивирус отображает предупреждающее сообщение
Create Checksums on Floppy	Если включен этот переключатель и переключатель, "Create New Checksums", тогда во время проверки файлов, расположенных на диске, в каждом каталоге создается файл CHKLIST.MS
Disable Alarm Sound	Отключаются все звуковые сигналы
Create Backup	Перед восстановлением зараженных файлов создаются резервные копии инфицированных файлов. Файлы резервных копий создаются с расширением VIR
Create Report	Создавать файл отчета, содержащий информацию о результатах проверки диска. Файл создается в корневом каталоге проверяемого диска и имеет имя MSAV.RPT
Prompt While Detect	Если переключатель находится во включенном положении, то при обнаружении вируса или несоответствия информации, записанной в файле CHKLIST.MS, с параметрами проверяемых файлов дальнейшая проверка прерывается и на экране отображается предупреждающее сообщение "Virus Found" или "Verify Error" соответственно
Anti-Stealth	Выполняется проверка на наличие активных стелс-вирусов, маскирующихся на уровне операционной системы
Check All Files	Переключатель позволяет выполнить проверку всех файлов, расположенных на диске

Если вы постоянно работаете в среде Microsoft Windows, тогда вам лучше использовать для проверки компьютера Microsoft Anti-Virus for Windows.



Для проверки компьютера на наличие вирусов и восстановления пораженных файлов и системных областей можно воспользоваться приложением Microsoft Anti-Virus.

Чтобы запустить Microsoft Anti-Virus, переключитесь в Windows на приложение Program Manager. Затем установите указатель мыши на пиктограмму приложения Microsoft Anti-Virus, расположенную в группе Microsoft Tools, и сделайте двойной щелчок левой кнопкой мыши.

Если группа Microsoft Tools отсутствует, тогда запустите файл MWAV.EXE, он должен находиться в каталоге DOS. На экране появится главное окно "Microsoft Anti-Virus" (рис. 3.16).

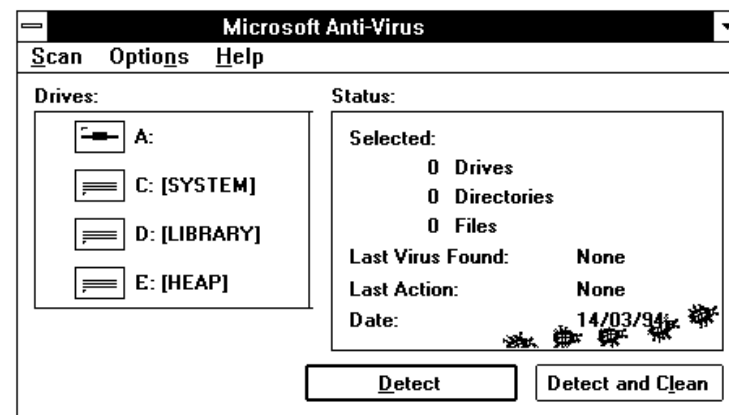


Рис. 3.16. Приложение Microsoft Anti-Virus

В группе Drivers отображаются пиктограммы всех дисковых устройств, к которым имеет доступ операционная система - накопители на гибких и жестких магнитных дисках, а также, если компьютер подключен к локальной сети, сетевые диски.

Выберите диски, которые надо проверить на наличие вирусов. Для этого достаточно последовательно щелкнуть указателем мыши по изображениям соответствующих устройств. Их названия выделяются цветом, после чего выполняется предварительный сбор информации об устройстве.

Информация о выбранных устройствах отображается в группе Status. В поле Selected выводится количество выбранных устройств Drivers, количество каталогов Directories и общее количество файлов на выделенных устройствах Files.

Чтобы начать проверку выбранных дисков, нажмите кнопку Detect. Если вирусы обнаружены и их надо удалить, нажмите кнопку Detect and Clean. Вы можете задавать

различные режимы проверки компьютера. Для этого выберите в меню Options строку Set Options. На экране появится диалоговая панель Options (рис. 3.17).

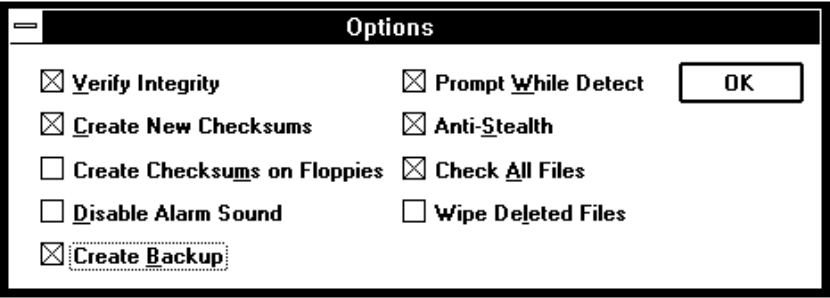


Рис. 3.17. Диалоговая панель "Options"

В этой диалоговой панели расположены девять переключателей, управляющих приложением Microsoft Anti-Virus for Windows. Переключатели и их назначение практически полностью соответствует переключателям, управляющим антивирусом Microsoft Anti-Virus. Добавлен только один переключатель Wipe Deleted Files. После его включения антивирус будет применять специальные приемы для удаления с диска файлов, зараженных вирусами. Восстановление таких файлов с помощью приложений, аналогичных Microsoft Undelete, будет невозможно.

Резидентный монитор VSafe

В состав Microsoft Anti-Virus входит резидентный монитор VSafe, позволяющий постоянно контролировать работу компьютера. После загрузки, он будет сообщать пользователю о любых подозрительных действиях программ, которые могут быть вызваны работой вирусов.

Запуск VSafe желательно выполнять в момент загрузки компьютера, поместив его вызов в конце конфигурационного файла AUTOEXEC.BAT, перед запуском командных оболочек типа Norton Commander или операционной системы Windows:

[VSAFE.COM](#)

Программе VSafe можно указать несколько параметров, устанавливающих режим его работы. Однако вместо этого есть возможность вызова специальной диалоговой панели, в которой выполняются все настройки программы. Если вы работаете в среде DOS, то для этого надо нажать комбинацию клавиш <Alt + V>. На экране откроется диалоговая панель, показанная на рисунке 3.18.

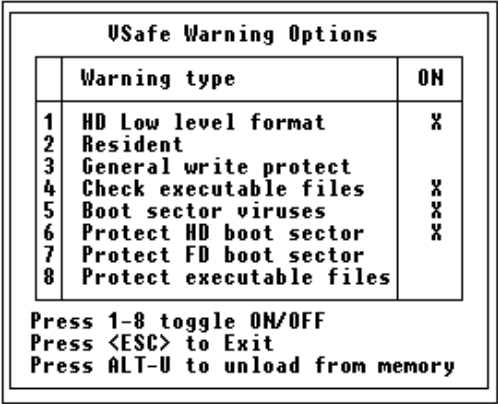


Рис. 3.18. Диалоговая панель VSafe Warning Options

В этой панели расположен ряд переключателей, управляющих работой монитора. Устанавливая те или иные переключатели, вы определяете какие операции будут контролироваться. Чтобы установить переключатель или сбросить его, надо нажать соответствующую цифровую клавишу. Например, чтобы изменить положение переключателя Resident надо нажать клавишу <2>.

Переключатель	Назначение
HD Low level format	Некоторые вирусы и троянские программы форматируют жесткие диски компьютера. Если переключатель установлен, то попытка отформатировать жесткий диск будет перехвачена и пользователь получит предупреждающее сообщение
Resident	Выдается предупреждение при попытке программы остаться резидентной в памяти компьютера
General write protect	Предупреждение выдается при любой попытке программы выполнить запись на диск
Check executable files	Проверяет целостность выполнимых файлов в момент их запуска. Сравнивается размер, дата создания и атрибуты файла запускаемого файла с информацией, записанной в файле CHKLIST.MS. Когда вы запустите зараженный файл, на экране появится предупреждение и вы сможете заняться лечением этого файла
Boot sector viruses	Устанавливается защита против вирусов, распространяющихся через загрузочный сектор

Protect HD boot sector	Сообщение выдается при попытке записи в загрузочный сектор или таблицу разделов жесткого диска. Изменения в загрузочный сектор и таблицу разделов жесткого диска, как правило, вносят вирусы
Protect FD boot sector	Выдается сообщение при попытке записи в загрузочный сектор дискеты (гибкого диска). Изменения в загрузочном секторе дискеты, как правило, вносят вирусы, которые уже находятся на компьютере
Protect executable files	Выдается предупреждение при попытке изменить выполнимые файлы. Как правило, при нормальной работе операционной системы изменения в выполнимые файлы не вносятся. Такие изменения могут служить сигналом, что данный файл заражен

Когда вы закончите установку переключателей, закройте панель VSafe Warning Options, нажав клавишу <Esc>. После перезагрузки компьютера положение переключателей восстановится.

Чтобы каждый раз при загрузке компьютера не менять положение переключателей, их положение можно задавать в командной строке VSafe. Сначала надо указать префикс параметра - символ слеша, затем номер переключателя и символ + или -, в зависимости от того надо включить или выключить переключатель.

Например, чтобы включить контроль за резидентными программами и включить проверку загрузочных секторов, измените вызов VSafe следующим образом:

[VSAFE.COM /2+ /6-](#)

Обнаружив, что какая-либо программа пытается нарушить установленную защиту, монитор VSafe немедленно сообщает об этом пользователю. На рисунке 3.19 представлено сообщение монитора о том, что файл MODE.COM изменен. Сообщение появляется в момент запуска файла. Такое изменение часто является результатом заражения программы файловым вирусом. Монитор VSafe позволяет предотвратить нарушение защиты, нажав кнопку Stop. В этом случае программа MODE.COM не будет запущена.



Рис. 3.19. Сообщение монитора VSafe

Если вы работаете в среде операционной системы Windows, вы также можете использовать монитор VSafe. Для этого надо запустить программу VSafe Manager for Windows.



Выполнимый файл VSafe Manager for Windows называется MWAVTSR.EXE и расположен в каталоге MS-DOS. Чтобы приложение VSafe Manager for Windows автоматически запускалось при каждом старте Windows, добавьте его в группу StartUp приложения Program Manager

При запуске приложения VSafe Manager for Windows на экране появляется окно приложения, показанное на рисунке 3.20.

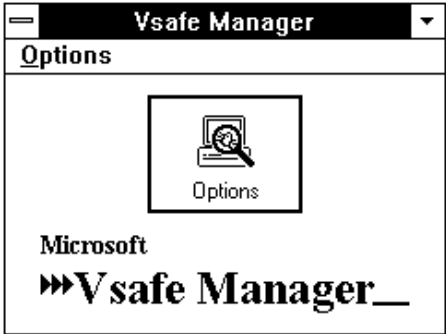


Рис. 3.20. Диалоговая панель Vsafe Manager

Нажмите кнопку Options. Появляется диалоговая панель Vsafe Options (рис. 3.21). В ней расположен ряд переключателей, управляющих работой приложения. Они соответствуют переключателям резидентного монитора VSafe, описанным выше. Через диалоговую панель Vsafe Options можно полностью управлять резидентным монитором VSafe.

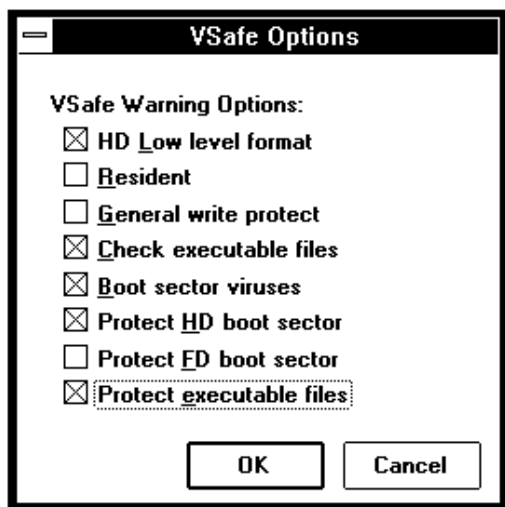


Рис. 3.21. Диалоговая панель Vsafe Options

Чтобы при последующих запусках Windows на экране не появлялась диалоговая панель Vsafe Manager, откройте в приложении Program Manager окно группы StartUp и щелкните один раз по пиктограмме Vsafe Manager. Затем нажмите комбинацию клавиш <Alt + Enter>. На экране появится панель Program Item Properties. Установите переключатель Run Minimized. Теперь при загрузке Windows приложение Vsafe Manager будет запускаться в виде пиктограммы.

К сожалению, резидентный монитор VSafe обманется некоторыми вирусами. Так вирус AntiC.1000, заражающий выполнимые файлы, может обнаружить в оперативной памяти резидентный монитор VSafe. В этом случае он выводит небольшой текст - "И даже VSafe тебе не поможет...". Чтобы антивирус не смог обнаружить факт заражения, вирус удаляет с диска файлы, имеющие расширение *.MS. В этих файлах хранится информация о контролируемых файлах и если она будет удалена, Microsoft Anti-Virus не сможет обнаружить в них изменения.

Чтобы отключить резидентный монитор, удалите пиктограмму Vsafe Manager из группы StartUp и удалите вызов программы VSAFE.COM из файла AUTOEXEC.BAT.

Антивирус Microsoft Anti-Virus позволяет удалить только известные вирусы, информация о которых есть в его базе данных. Новые вирусы появляются постоянно, поэтому версию антивируса необходимо постоянно обновлять.

К сожалению, Microsoft Anti-Virus не может не только удалить, но даже обнаружить полиморфные вирусы типа OneHalf. Из-за этого защита при помощи одного только антивируса Microsoft Anti-Virus недостаточна и необходимо дополнительно использовать другие средства.

Антивирус Norton AntiVirus for Windows 95

Как вы уже знаете, в дистрибутив операционной системы MS-DOS входит антивирусный пакет Microsoft Anti-Virus. В его составе несколько антивирусных программ для MS-DOS и Windows. Новая операционная система Microsoft Windows 95 не содержит в себе встроенных антивирусных средств. Поэтому мы включили в нашу книгу немного сведений о пакете Norton AntiVirus, предназначенном специально для этой операционной системы.

Так как новые вирусы появляются с завидным постоянством, то необходимо периодически обновлять вирусную базу Norton AntiVirus, содержащую описания известных вирусов. В противном случае при проверке можно пропустить новый вирус, заразивший компьютер.

Некоторые вирусы, созданные в России и не получившие широкого распространения за рубежом, могут не определяться программой Norton AntiVirus. Поэтому мы рекомендуем в первую очередь пользоваться отечественными разработками антивирусных программ

Операционная система Windows 95 имеет много новшеств по сравнению со старыми операционными системами MS-DOS и Windows. В частности, внесены изменения в файловую систему. Теперь пользователь может задавать для файлов длинные имена (до двухсот шестидесяти пяти символов). Некоторые старые программы, разработанные для прежних версий Windows, не работают с длинными именами файлов. Ряд антивирусных программ пользуются низкоуровневым доступом к жесткому диску и также не работают совместно с Windows 95.

Мы не стали описывать процедуру установки Norton AntiVirus for Windows 95, вы сможете найти ее в документации, а уделили основное внимание описанию возможностей этого пакета, его достоинствам и недостаткам.

После установки на компьютере Norton AntiVirus for Windows 95 версии 4.0 создается новая папка Norton AntiVirus, содержащая ряд приложений (рис. 3.22).

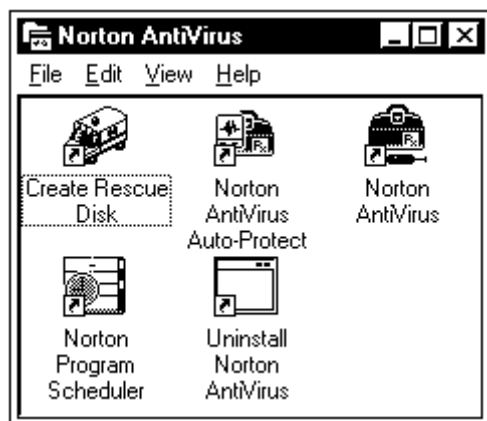






Рис. 3.22. Панка Norton AntiVirus

В следующей таблице мы перечислим пиктограммы пакета Norton AntiVirus и приведем их краткие описания.

Пиктограмма	Приложение
	Некоторые вирусы могут разрушить операционную систему компьютера таким образом, что она перестанет загружаться. Приложение Create Rescue Disk позволяет создать дискету, с которой вы сможете загрузить Windows 95 и восстановить ее работоспособность
	Приложение Norton AntiVirus Auto-Protect постоянно работает в фоновом режиме и проверяет все запускаемые программы на заражение известными вирусами. Кроме того, Norton AntiVirus Auto-Protect позволяет отслеживать все подозрительные действия и предупреждать о них пользователя
	Основное приложение пакета Norton AntiVirus. Выполняет поиск вирусов в компьютере. Приложение Norton AntiVirus позволяет выбрать режим проверки компьютера, просмотреть информацию об известных вирусах, просмотреть журнал, содержащий информацию о предыдущих проверках компьютера
	Приложение Norton Program Scheduler позволяет выполнять запуск Norton AntiVirus в автоматическом режиме. Например, вы можете указать время когда Scheduler должен запустить антивирус для проверки всех файлов на диске. Вместо Norton Program Scheduler вы можете воспользоваться приложением System Agent, входящим в состав Microsoft Plus! For Windows 95



Приложение Uninstall Norton AntiVirus позволяет отключить антивирусную защиту и удалить все файлы пакета с жесткого диска компьютера. Отключение антивирусной защиты увеличивает шансы вирусов заразить компьютер, поэтому если вы отказались от использования Norton AntiVirus, мы рекомендуем вам попробовать другие антивирусные программы, например, антивирусный комплект АО “ДиалогНаука”

Антивирус Norton AntiVirus

Запустите приложение Norton AntiVirus. На экране откроется главное окно Norton AntiVirus (рис. 3.23). В верхней части окна, под главным меню, расположен ряд кнопок, позволяющих настроить режим работы приложения, просмотреть информацию об известных вирусах, установить программу автоматического запуска Norton Program Scheduler и просмотреть журнал предыдущих проверок компьютера.

В средней части окна расположены две группы переключателей, при помощи которых можно выбрать проверяемые диски. В группе переключателей, расположенной слева, перечислены имена всех дисков компьютера и их метки (если такие есть). Чтобы проверить диск, необходимо включить переключатель, расположенный около него. Вы можете выбрать любую комбинацию проверяемых дисков, например, A:, C:, F: или C:, D:, E: и G:.

Вы можете указать не только отдельные имена проверяемых дисков, но и целые группы. Группа переключателей Drive types позволяет указать, что проверке подлежат все дисководы для гибких дисков, все жесткие диски и все сетевые диски. Вы можете проверить не только жесткие диски компьютера, но также все сетевые диски, к которым ваш компьютер имеет доступ и компакт-диски.

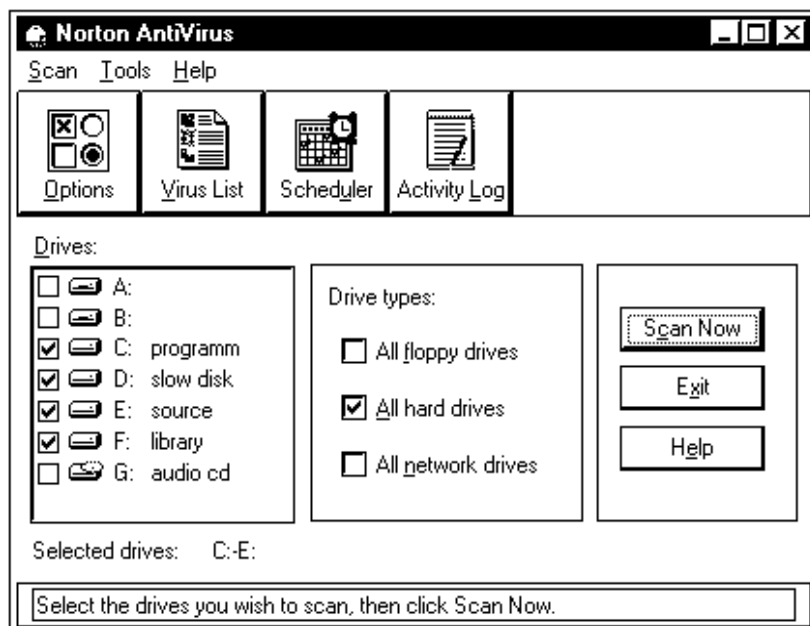


Рис. 3.23. Главное окно приложения Norton AntiVirus

С правой стороны окна Norton AntiVirus расположены три кнопки - Scan Now, Exit и Help. Они позволяют начать проверку компьютера, завершить приложение Norton AntiVirus, а также получить справочную информацию.

Чтобы начать проверку выбранных дисков, нажмите кнопку Scan Now. Антивирус выполнит проверку оперативной памяти и загрузочных секторов. Затем будут проверены основные файлы операционной системы. Если никаких нарушений не будет обнаружено, начинается проверка дисков (рис. 3.24).

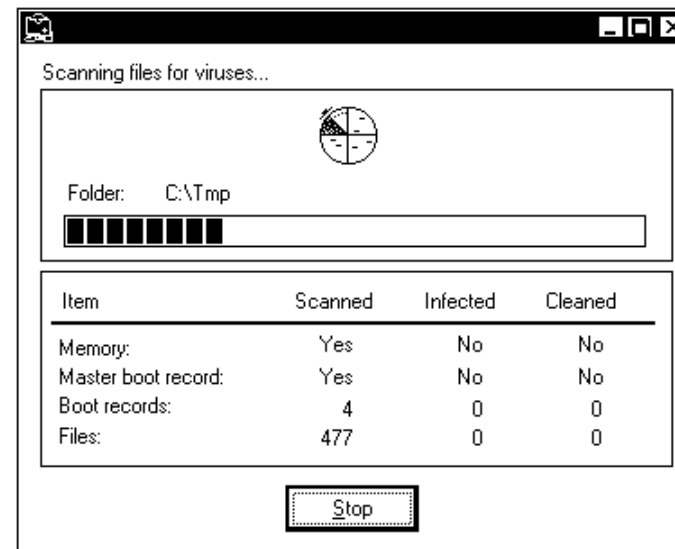


Рис. 3.24. Проверка диска C:

Ход проверки компьютера зависит от того, как настроен Norton AntiVirus. Зараженные файлы могут обрабатываться в автоматическом режиме или вручную. Более подробно о настройке Norton AntiVirus можно прочитать в следующей главе.

||

Для более опытных пользователей рекомендуется ручная обработка. В этом случае антивирус позволяет самому пользователю решать, что делать с обнаруженным вирусом (рис. 3.25) - удалить вирус, удалить сам зараженный файл или оставить файл без обработки. Вы можете просмотреть информацию о пойманном вирусе, нажав кнопку Info.

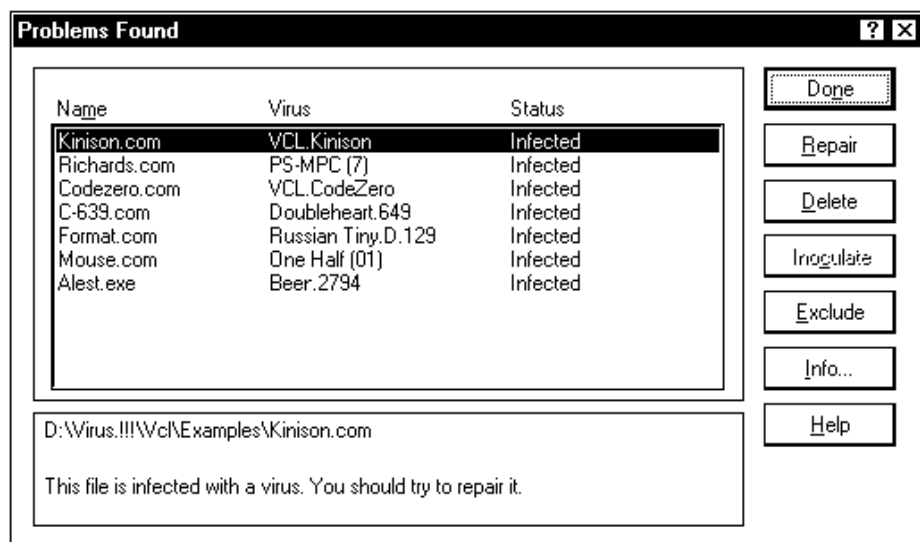


Рис. 3.25. Список обнаруженных вирусов

После того как вы обработаете все вирусы или нажмете кнопку Done, на экране появится диалоговая панель, содержащая статистические данные о проверке компьютера. Закрыв эту панель, вы вернетесь в главное окно программы.

Вirus Beer. 2794

Опасный резидентный шифрованный вирус, заражает выполнимые файлы в формате COM и EXE. Уничтожает файлы DISKDATA.DTL, VIRUSES.INF, DIRINFO, -V.MSG или A-DINF-_.____. Иногда проигрывает мелодию и выводит текст "Сейчас бы пивка"

Настройка режимов поиска вирусов

Перед тем как приступить к поиску вирусов на компьютере, следует настроить Norton AntiVirus. Для этого вы можете нажать кнопку Options или выбрать из меню Tools строку Options. На экране появится блокнот Options, содержащий несколько страничек - диалоговых панелей (рис. 3.26). Для выбора страницы следует нажать указателем мыши на закладки, расположенные в верхней части окна.

Сейчас мы дадим основные рекомендации по настройке всех режимов Norton AntiVirus.

Первая страница блокнота настроек, которую мы рассмотрим, называется Scanner (рис. 3.26). Она задает все основные параметры работы антивируса в режиме ручной проверки компьютера. Самая главная группа переключателей What to scan определяет,

где приложение будет искать вирусы. От того, насколько правильно вы установите эти переключатели, зависит эффективность проверки компьютера.

Первый переключатель Memoгу управляет поиском вирусов в оперативной памяти и позволяет обнаружить активные вирусы.

Переключатель Master boot record управляет поиском вирусов в главном загрузочном секторе жестких дисков компьютера. Желательно выполнять эту проверку всегда, так как главный загрузочный сектор - излюбленное место для вирусов.

Следующий переключатель Boot record включает поиск вирусов в загрузочных секторах жестких дисков и дискет. Имеет смысл установить этот переключатель, также как переключатель Master boot record, потому, что они оба отвечают за поиск загрузочных вирусов. Вы обязательно должны включить переключатель Boot record при поиске вирусов на дискетах.

Переключатель Within compressed files задает режим поиска внутри файлов архивов. Обычно такая проверка бывает полезна, так как вирусы могут попасть в архив во время его создания, когда вы записываете в него зараженный файл. Существуют вирусы, которые могут записать новый файл с вирусом в архив, и можно представить себе вирус, способный заразить файлы внутри архива.

В группе What to scan также расположен переключатель с зависимой фиксацией, который позволяет выбрать файлы для проверки. Вы можете задать проверку всех файлов на выбранных дисках или только файлов, имеющих определенные расширения. Чтобы проверить все файлы, этот переключатель надо перевести в положение All files. Если вам надо проверить только выполнимые файлы, переведите переключатель в положение Program files. По умолчанию будут проверены все файлы, имеющее расширения COM, EXE, OV?, SYS, DRV, APP, CMD, PGM, PRG, DLL и 386, но вы можете изменить этот список произвольным образом.

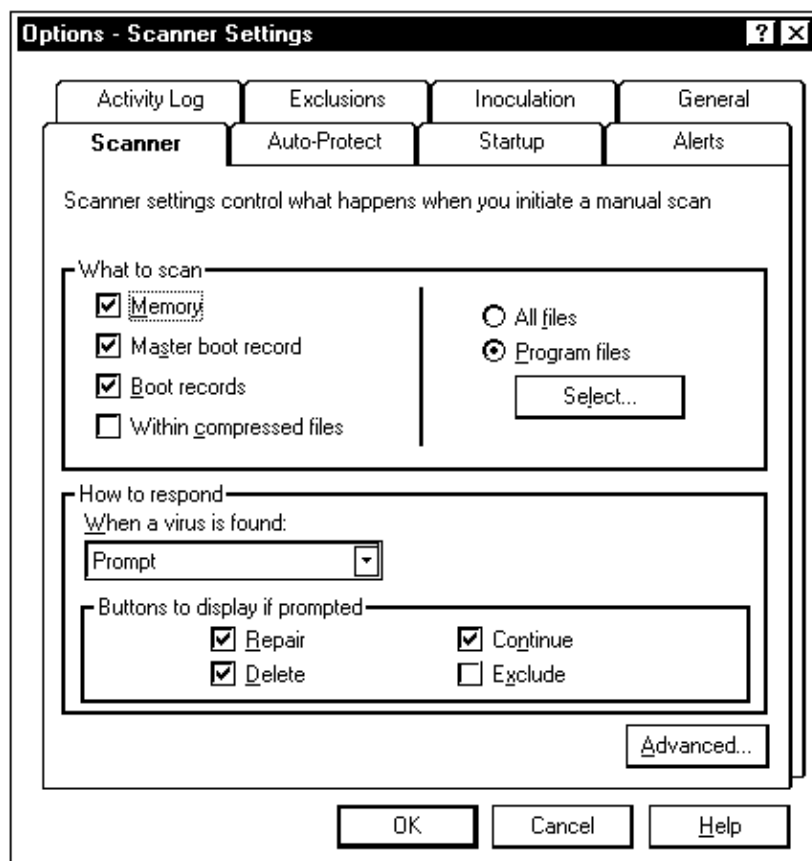


Рис. 3.26. Страница Scanner Setting

Если во время проверки компьютера Norton AntiVirus обнаружит вирус, он может выполнить различные действия, от сообщения пользователю до остановки компьютера. Для того чтобы определить поведение Norton AntiVirus при обнаружении вируса, предназначена группа How to respond.

Список When a virus is found содержит перечень возможных вариантов:

Строка из списка	Действие Norton AntiVirus при обнаружении вируса
------------------	--

Prompt	На экране появляется приглашение. Пользователю разрешается самостоятельно решить судьбу зараженного файла. Этот режим предполагает, что пользователь хорошо разбирается в программном обеспечении компьютера и в состоянии решить что делать с зараженным файлом или загрузочным сектором
Notify Only	Выводится сообщение об обнаружении вируса. Сам вирус не удаляется. В этом случае пользователь должен либо удалить зараженный файл самостоятельно, либо вылечить его, запустив Norton AntiVirus в другом режиме
Repair Automatically	В этом режиме все обнаруженные вирусы будут автоматически удаляться. К сожалению, не во всех случаях такое лечение будет успешным. Некоторые вирусы так заражают файлы, что они не подлежат лечению и должны быть восстановлены с резервной копии или с дистрибутива
Delete Automatically	Это очень опасный режим, в котором обнаруженный вирус будет удален вместе с зараженным файлом. Следует иметь в виду, что после удаления большинства файлов программное обеспечение компьютера скорее всего перестанет работать и вам может потребоваться устанавливать его заново
Shutdown Computer	Компьютер немедленно отключается. Этот режим можно использовать, если компьютер обслуживается специалистами, которых можно вызвать в случае вирусной атаки. Немедленное отключение компьютера, зараженного вирусами, и вызов специалиста во многих случаях позволят сохранить информацию, записанную в нем

Если вы выбрали строку Prompt, то при обнаружении вируса на экране появится диалоговая панель с кнопками, указывающими, что делать с зараженным файлом. Таких кнопок четыре: Repair - восстановить файл, удалив вирус, Delete - удалить зараженный файл, Continue - продолжить проверку компьютера и ни чего не делать с обнаруженным вирусом, Exclude - исключить файл из всех последующих проверок компьютера. Некоторые кнопки из перечисленных выше можно заблокировать, для этого следует выключить соответствующий переключатель в группе Buttons to display if prompted.

Некоторые дополнительные параметры режима проверки компьютера задаются в диалоговой панели Scanner Advanced Setting (рис. 3.27). Чтобы ее открыть, нажмите кнопку Advanced.

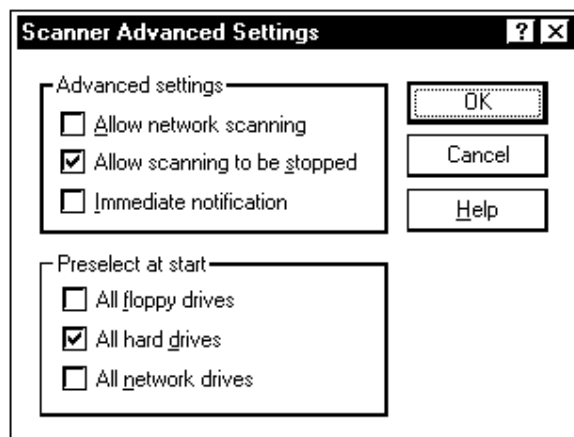


Рис. 3.27. Диалоговая панель Scanner Advanced Setting

Диалоговая панель Options - Startup Settings определяет, как будет проверяться компьютер при загрузке операционной системы (рис. 3.28). Ряд переключателей, объединенных в группу What to scan, указывают антивирусу, что конкретно он должен проверять.

Переключатель	Описание и рекомендации по использованию
Memory	Позволяет проверить, нет ли активных вирусов в оперативной памяти компьютера
Master boot record	Выполняет поиск загрузочных вирусов в главной загрузочной записи жесткого диска компьютера
Boot record	Проверяет загрузочные секторы в поисках загрузочных вирусов
System files	Проверяет основные файлы операционной системы
Programs run from AUTOEXEC.BAT	Выполняет поиск файловых вирусов в программах, запускаемых при загрузке компьютера из файла AUTOEXEC.BAT

Для повышения степени защиты компьютера вы можете установить все перечисленные в таблице переключатели, но время загрузки компьютера несколько увеличится. Если проверка компьютера при его загрузке будет выполняться слишком долго, ее можно прервать нажав комбинацию клавиш, установленную переключателем Bypass keys.

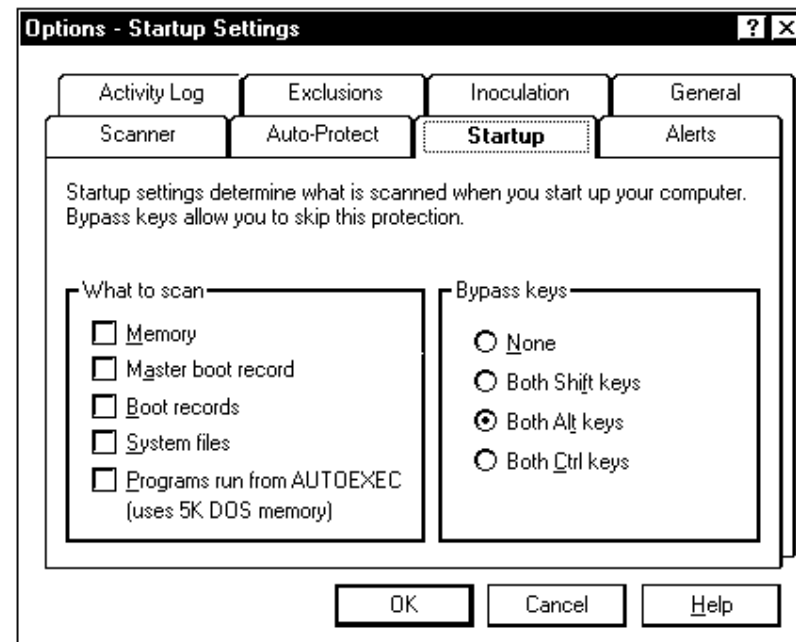


Рис. 3.28. Диалоговая панель Options - Startup Settings

Когда Norton AntiVirus обнаружит вирус, он может вывести для пользователя предупреждающее сообщение. Вы имеете возможность задать его сами. Для этого выберите диалоговую панель Options - Alerts Settings (рис. 3.29). Включите переключатель Display alert message и наберите текст сообщения в окне редактора, расположенном под этим переключателем. Дополнительно можно установить подачу звукового сигнала, включив переключатель Sound audible alert.

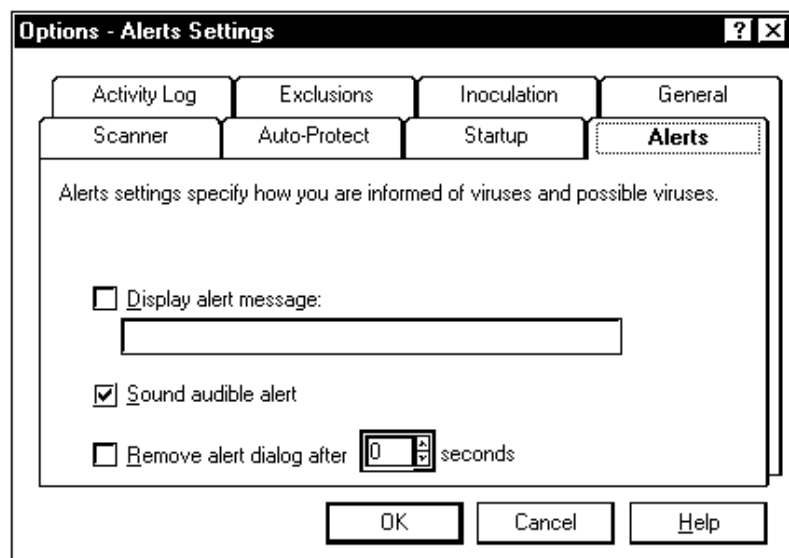


Рис. 3.29. Диалоговая панель Options - Alerts Settings

Если вы проверяете компьютер на наличие вирусов во время своего отсутствия, вы можете захотеть, чтобы предупреждающее сообщение отображалось на экране не дольше заданного времени. Поэтому установите переключатель Remove alert dialog after и укажите промежуток времени в секундах.

К сожалению, не всегда попытка лечения файла оказывается успешной. Иногда после удаления вируса вылеченная программа оказывается неработоспособной. Поэтому перед восстановлением файла обычно делают резервную копию. Если вылеченная программа оказывается неработоспособной, ее восстанавливают с резервной копией. Вирус в этом случае остается нетронутым.

Большинство антивирусных программ, в том числе и Norton AntiVirus, позволяет автоматически создавать резервные копии файлов программ перед их лечением. Вы можете управлять этой возможностью. Выберите диалоговую панель Options - General Settings (рис. 3.30).

Чтобы разрешить создание резервных копий, включите переключатель Back up file before attempting a repair, и введите расширение, которое будет присваиваться файлам копий. По умолчанию используется расширение VIR.

Таким образом, резервным копиям выполнимых файлов COM и EXE присваивается одинаковое расширение VIR. Отличить их можно просмотрев несколько первых символов из этих файлов. Выполнимые файлы программ в формате EXE начинаются символами MZ или ZM.

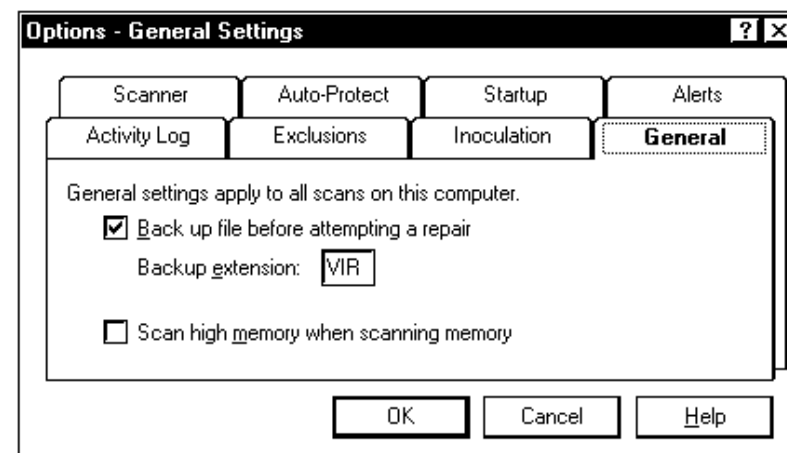


Рис. 3.30. Диалоговая панель Options - General Settings

В диалоговой панели Options - General Settings находится еще один переключатель Scan high memory when scanning memory. Он отвечает за проверку верхней области памяти во время теста оперативной памяти компьютера. Для повышения надежности защиты включите этот переключатель.

Антивирус Norton AntiVirus выполняет функции ревизора диска. Он позволяет записать необходимую информацию о загрузочных секторах и выполнимых файлах, а затем сверять ее. Если будет обнаружено совпадение, вероятнее всего загрузочный сектор или файл подверглись нападению вируса.

По умолчанию Norton AntiVirus записывает информацию только о загрузочных секторах и основных файлах операционной системы, но вы можете расширить этот список, выбрав диалоговую панель Options - Inoculation Settings (рис. 3.31). Для этого включите переключатель Inoculate program files.

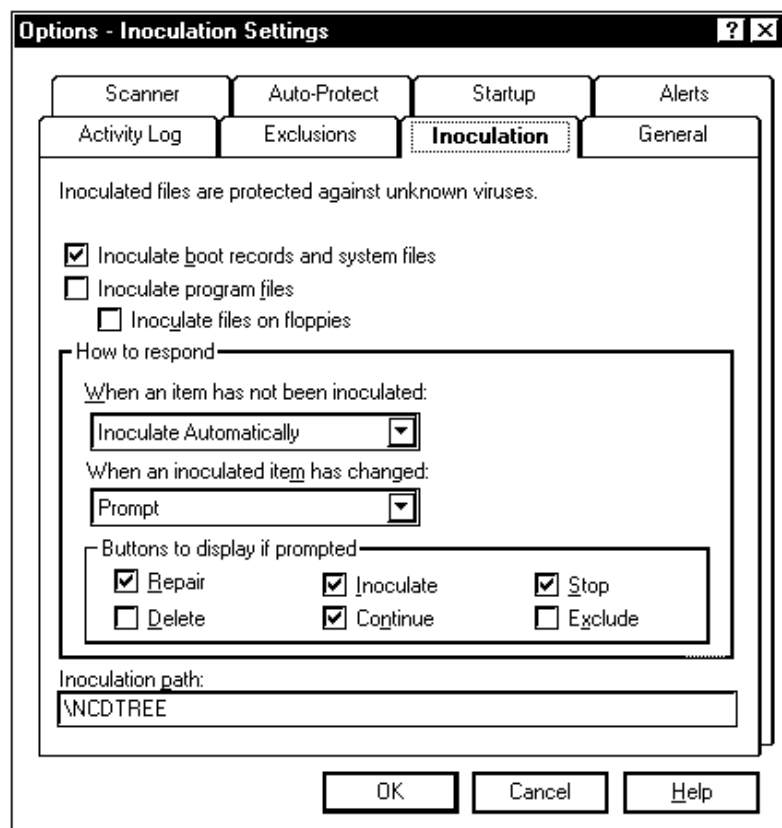


Рис. 3.31. Диалоговая панель Options - Inoculation Settings

Иногда требуется исключить ряд файлов из проверки на вирусы. Примером такого файла могут служить некоторые выполнимые файлы антивирусных программ, содержащие сигнатуры известных вирусов. Список таких файлов вы можете поддерживать, вызвав на экран диалоговую панель Options - Exclusions List Setting (рис. 3.32).

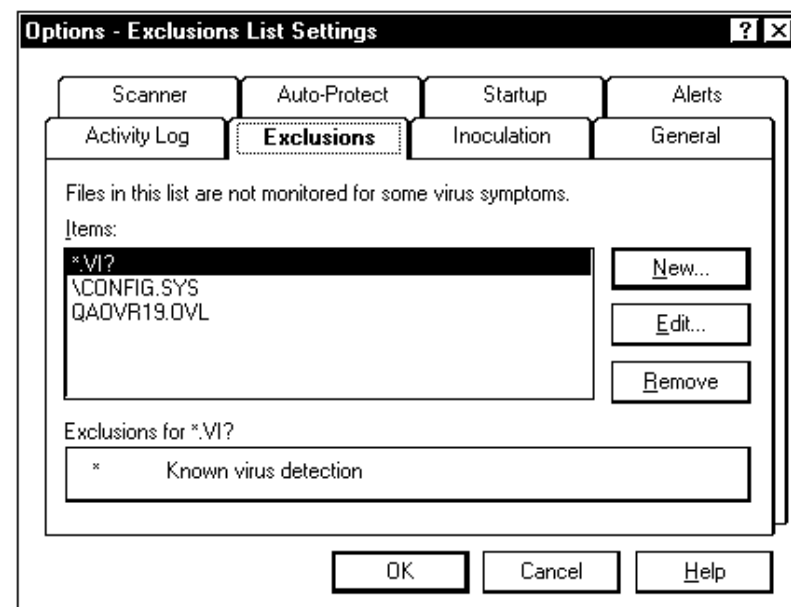


Рис. 3.32. Диалоговая панель Options - Exclusions List Setting

Вы можете добавлять новые имена файлов в список, изменять их и удалять из списка с помощью кнопок New, Edit и Remove.

Во время проверки компьютера Norton AntiVirus ведет журнал регистрации, в который записывает все основные события, такие как обнаружение вируса и т. д. Вы можете управлять ведением этого журнала через диалоговую панель Activity Log Settings (рис. 3.33).

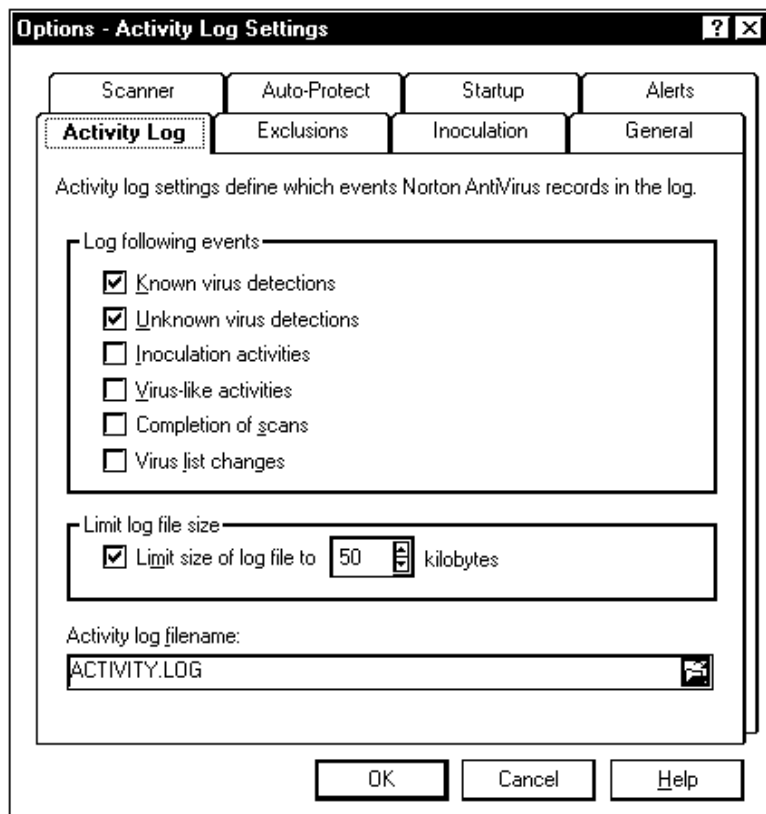


Рис. 3.33. Диалоговая панель Options - Activity Log Settings

Переключатели, расположенные в группе Log following events, определяют события, которые будут занесены в файл журнала. В группе Limit log file size можно указать максимальный размер файла журнала, а список Activity log filename - выбрать имя для файла журнала.

Впоследствии вы сможете просмотреть файл журнала, нажав кнопку Activity Log в главном окне приложения (рис. 3.33).

Автоматическая защита компьютера

В состав комплекта Norton AntiVirus for Windows 95 входит приложение Norton AntiVirus Auto-Protect. Будучи запущенным, это приложение постоянно работает в фоновом режиме, контролируя работу компьютера.

После запуска Norton AntiVirus Auto-Protect в нижней части экрана появляется небольшая пиктограмма, изображающая монитор с осциллограммой (см. правую

пиктограмму на рис. 3.34). Эта пиктограмма означает, что компьютер находится под защитой.



Рис. 3.34. Панка Norton AntiVirus Auto-Protect

Вы можете временно отключить Norton AntiVirus Auto-Protect и настроить режим его работы. Для этого сделайте двойной щелчок мышью по пиктограмме AntiVirus Auto-Protect. На экране появится диалоговая панель управления приложением (рис. 3.35), содержащая три кнопки. Кнопка Minimize позволяет закрыть эту диалоговую панель.

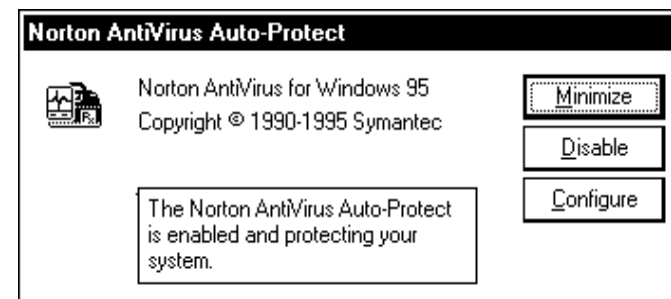


Рис. 3.35. Диалоговая панель Norton AntiVirus Auto-Protect

Чтобы временно отключить защиту компьютера с помощью Norton AntiVirus Auto-Protect, нажмите кнопку Disable. Защита будет отключена, а в нижней части экрана пиктограмма Norton AntiVirus Auto-Protect изменит свой внешний вид (рис. 3.36). Чтобы снова включить защиту, опять щелкните два раза мышью по перечеркнутой пиктограмме и в открывшейся диалоговой панели нажмите кнопку Enable.



Рис. 3.36. Панка Norton AntiVirus Auto-Protect

Norton AntiVirus Auto-Protect постоянно работает в фоновом режиме и проверяет все запускаемые программы на заражение известными вирусами. Кроме того, Norton AntiVirus Auto-Protect позволяет отслеживать все подозрительные действия и предупреждать о них пользователя.

Кнопка Configure служит для настройки автоматической защиты от вирусов. После того как вы на нее нажмете, на экране появится диалоговая панель Options - Auto-Protect Settings (рис. 3.37).

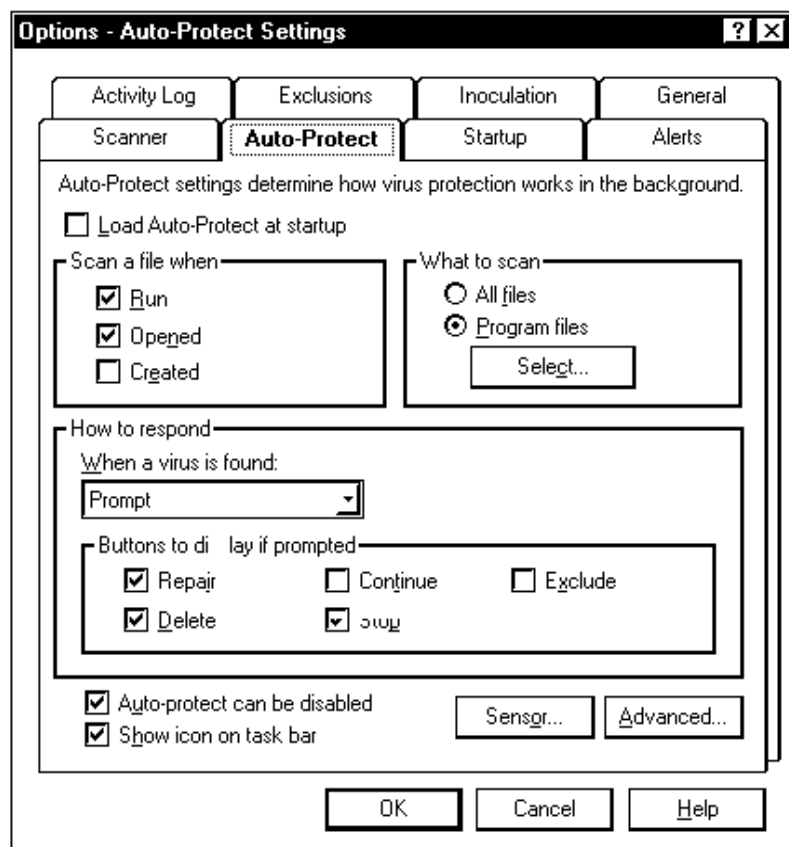


Рис. 3.37. Диалоговая панель Options - Auto-Protect Settings

Эта диалоговая панель почти соответствует уже рассмотренной нами панели основного приложения Norton AntiVirus (рис. 3.26). Она содержит описанные нами ранее две группы переключателей - Scan a file when и How to respond. Поэтому сейчас мы расскажем о дополнительных особенностях этой панели.

В первую очередь это переключатель Load Auto-Protect at startup. Если включить его, тогда Norton AntiVirus Auto-Protect будет автоматически запускаться каждый раз при загрузке компьютера.

Переключатель Auto-protect can be disabled позволяет заблокировать возможность временного отключения защиты. Для этого переключатель должен быть выключен. Вы можете воспользоваться этой возможностью, если на компьютере работают начинающие пользователи. Лучше всего использовать этот переключатель вместе с переключателем Show icon on task bar, который позволяет не отображать пиктограмму приложения в нижней части экрана.

Интересной особенностью приложения Norton AntiVirus Auto-Protect является то, что оно позволяет обнаруживать в выполнимых файлах не только известные, но также неизвестные вирусы. Для этого применяется специальная технология, которая называется Sensor technology. Нажмите кнопку Sensor. На экране появится диалоговая панель Auto-Protect Virus Sensor Settings (рис. 3.38).

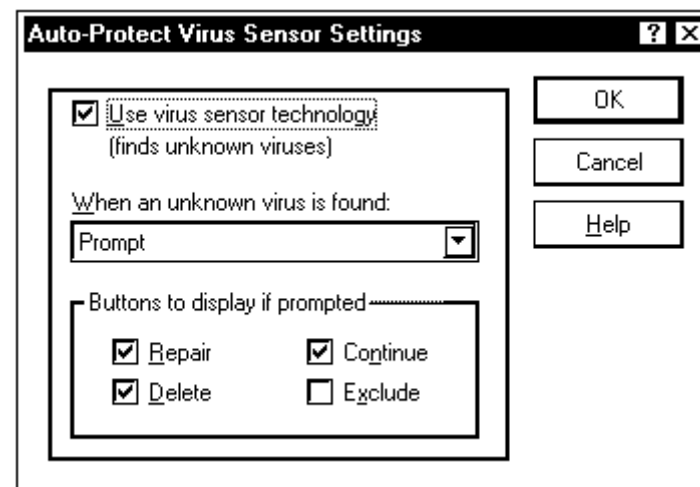


Рис. 3.38. Диалоговая панель Auto-Protect Virus Sensor Settings

Чтобы включить режим поиска неизвестных вирусов, установите переключатель Use virus sensor technology. Список When an unknown virus is found и группа переключателей Buttons to display if prompted, определяют реакцию антивируса в случае обнаружения неизвестного вируса.

Кроме проверки запускаемых файлов Norton AntiVirus Auto-Protect выполняет все функции обычного резидентного монитора. Он отслеживает все действия, которые могут стать причиной разрушения программного обеспечения компьютера и хранимых в нем данных, сообщая о них пользователю. Вы можете установить, в каких случаях Norton AntiVirus Auto-Protect будет сообщать вам о “нападении вирусов”. Для этого нажмите кнопку Advanced в диалоговой панели Options - Auto-Protect Settings. Откроется новая диалоговая панель Auto-Protect Advanced Settings (рис. 3.39).

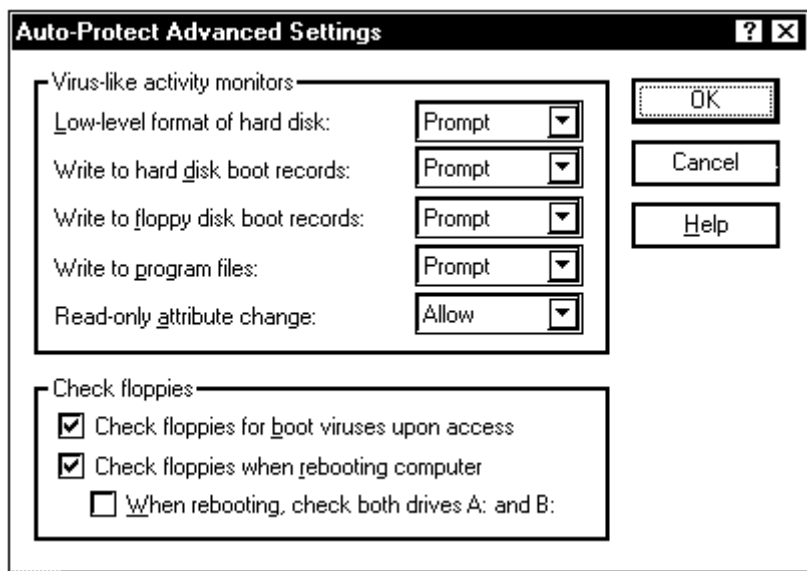


Рис. 3.39. Диалоговая панель Auto-Protect Advanced Settings

В группе Virus-like activity monitors перечислены ситуации, которые отслеживает приложение. Для каждой ситуации вы можете выбрать реакцию приложения Prompt - разрешить пользователю самому решить, выполнять ли данную операцию, Allow - разрешить выполнение операции, Don't Allow - запретить выполнение операции.

Вот список таких ситуаций с краткими описаниями и рекомендациями.

Переключатель	Описание и рекомендации
Low-level format of hard disk	Низкоуровневое форматирование жесткого диска. Очень опасная операция. Вызывает полную потерю всех данных на диске. Если монитор обнаружил попытку выполнить форматирование жесткого диска, практически наверняка компьютер заражен вирусом, троянской программой или логической бомбой. Вы должны отменить операцию форматирования и немедленно проверить компьютер на наличие вирусов

Write to hard disk boot record

Запись данных в загрузочные секторы жесткого диска. Обычно такая операция выполняется загрузочными вирусами при заражении жестких дисков компьютера. Однако изменение загрузочных секторов может быть вызвано значительно более прозаической причиной. Загрузочные секторы изменяются, когда вы изменяете метку диска командой LABEL и устанавливаете новую версию операционной системы. Если монитор сообщит о попытке изменения загрузочных секторов, вы должны самостоятельно проанализировать ситуацию и решить, не вызвано ли такое изменение вашими действиями. В случае если вы не форматировали диски, не меняли метку диска, не устанавливали новую версию операционной системы, то возможно компьютер заражен вирусом. Тогда отмените операцию записи загрузочного сектора и проверьте компьютер на наличие вирусов

Write to floppy disk boot record

Запись данных в загрузочные секторы дискеты. Обычно такая операция выполняется загрузочными вирусами при заражении дискеты. В тоже время изменение загрузочного сектора может быть вызвано форматированием дискеты, изменением ее метки, командой LABEL, записью на нее операционной системы командой SYS. Если монитор сообщит о попытке изменения загрузочного сектора дискеты, проанализируйте ситуацию и решите, не вызвано ли такое изменение вашими действиями. При необходимости проверьте компьютер на заражение вирусами

Write to program files

Запись данных в выполнимый файл. Эту операцию выполняет большинство файловых вирусов, заражая свои новые жертвы. Тем не менее, выполнение записи в выполнимый файл не может однозначно говорить о том, что компьютер заражен вирусом. Некоторые программы записывают в свой выполнимый файл различную информацию, например, свою конфигурацию. Если монитор сообщит о попытке изменения выполнимого файла, обратите внимание на файл в который выполняется запись. Если вы уверены, что это неизменяемый файл, скорее всего, компьютер заражен вирусом

Read-only attribute change

Изменение атрибута файла. Некоторые вирусы, заражая выполнимые файлы, предварительно снимают с них атрибут "только читаемый файл". Это может сигнализировать о вирусной атаке. Атрибуты файла могут меняться не только вирусами. Например, популярная программа Norton Commander позволяет устанавливать атрибуты файлов произвольным образом

Приложение Norton AntiVirus Auto-Protect имеет те же недостатки, что и остальные резидентные мониторы. Оно отнимает время на проверку программ во время их запуска, занимает ресурсы компьютера. Монитор может надоесть вам, постоянно сообщая об изменении выполнимых файлов и т. д. Мы рекомендуем пользоваться защитой Norton AntiVirus Auto-Protect во время запуска подозрительных или просто новых программ неизвестного происхождения.

Вирус Gloomy.2725

Заражае т выполнимые файлы в формате COM и EXE, резидентный. При каждом шестнадцатом запуске программы портит случайный сектор. Удаляет с диска файлы с именами ".MS" и ".*AS". Заменяет главную загрузочную запись на программу, которая после 511 загрузок компьютера форматирует диск. Содержит тексты "Gloomy Nutcracker (AB5) from the city of Brest(BY) with best wishes!" и "Only the Hope dies last!".*

Если на вашем компьютере установлена операционная система Windows 95, вы можете использовать монитор Norton AntiVirus Auto-Protect при запуске новых программ, а в качестве основных антивирусных программ пользоваться комплектом АО “ДиалогНаука”.

Антивирус для OS /2 - IBM AntiVirus/2

Малое количество вирусов, специально созданных для OS/2, не означает что компьютеры с этой операционной системой находятся в безопасности. Так как программы, разработанные для MS-DOS, могут работать в среде OS/2, то обычные вирусы MS-DOS все еще представляют опасность для компьютера, а также для установленного в нем программного обеспечения и, самое главное, опасность для данных пользователя.

В принципе для защиты от вирусов компьютера с установленной на нем операционной системой OS/2 можно применять обычные антивирусные средства, разработанные для операционной системы DOS. Однако в некоторых случаях это программное обеспечение не сможет нормально функционировать. Одной из причин служат отличия файловой системы OS/2. Если на жестких дисках компьютера имеются разделы OS/2 в формате высокопроизводительной файловой системы HPFS, не совместимой с FAT, то антивирусные программы DOS не смогут с ней работать.



Чтобы защитить компьютеры пользователей OS/2 от вирусов, фирма IBM выпустила в свет антивирус IBM AntiVirus/2, специально предназначенный для этой операционной системы.

Главное окно антивирусной программы IBM AntiVirus/2 представлено на рисунке 3.40. Как видите, интерфейс антивируса позволяет максимально упростить процедуру проверки компьютера. Для этого достаточно просто нажать кнопку Push here. Простота IBM AntiVirus/2 несомненно относится к достоинствам этого антивируса. Даже пользователь, имеющий поверхностные знания о вирусах, сможет успешно с ним работать.

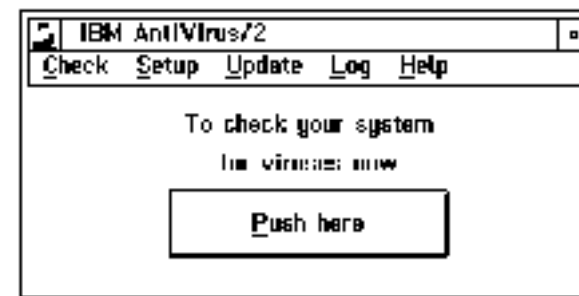


Рис. 3.40. Главное окно IBM AntiVirus/2

После запуска антивирус начнет последовательно просматривать файлы на жестком диске компьютера. Если будут обнаружены вирусы, на экране появится диалоговая панель с предложением удалить их (рис. 3.41). Пользователю предлагается несколько вариантов. Он может удалить вирус, восстановив зараженный файл или загрузочный сектор. Для этого следует выбрать из списка зараженные файлы, подлежащие восстановлению и нажать кнопку Disinfect.

Зараженные загрузочные секторы могут быть восстановлены, даже если из них невозможно удалить вирус. При этом зараженный загрузочный сектор заменяется программой IBM AntiVirus/2. Чтобы выполнить замену, нажмите кнопку Replace.

И наконец, зараженный вирусом файл можно удалить, воспользовавшись кнопкой Erase. Файлы, удаленные программой IBM AntiVirus/2, невозможно восстановить даже с помощью специальных программ, поэтому пользуйтесь этой операцией с большой осторожностью. Удаляя зараженный файл, надо иметь в виду, что возможно после этого программное обеспечение компьютера перестанет нормально работать и его придется переустанавливать с дистрибутивов или резервных копий. Проверяйте резервные копии программного обеспечения на заражение вирусами. В противном случае они могут быть испорчены.

Любой из перечисленных способов удаления вируса предпочтительнее работы на компьютере, зараженном вирусом. Никогда не проявляя себя внешне, вирус может планомерно уничтожать данные, записанные на диске

Чтобы отложить лечение зараженных файлов, достаточно нажать кнопку Close и диалоговая панель IBM AntiVirus/2 - Virus infection report будет закрыта, а вы вернетесь в главное окно программы.

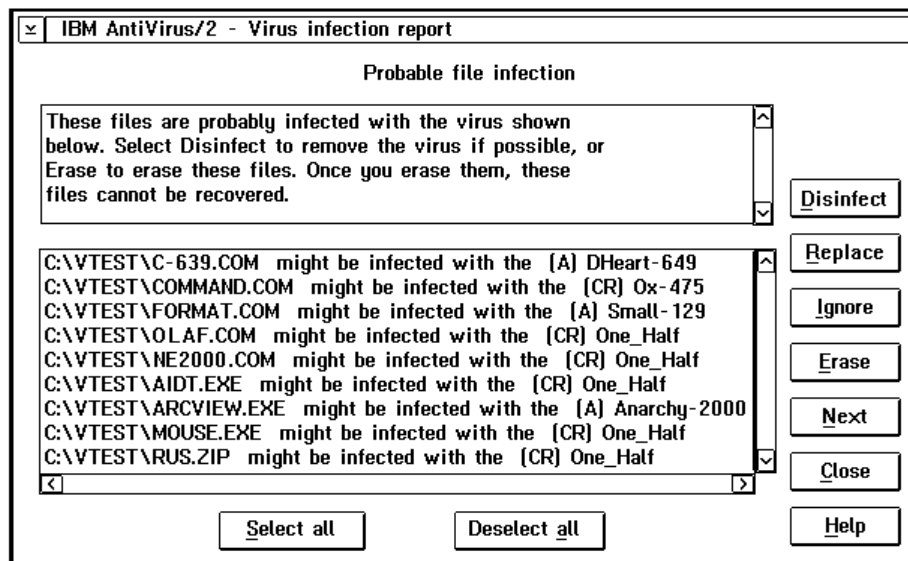


Рис. 3.41. Обнаружены вирусы

Программа IBM AntiVirus/2 позволяет задавать различные режимы проверки компьютера. Вы сами можете задать, какие диски и какие файлы будут проверяться. Для этого выберите из главного меню приложения Check строку Check system. На экране появится диалоговая панель Check system for viruses (рис. 3.42).

Органы управления группы позволяют указать диски и каталоги, которые должны быть проверены. Рекомендуется проверять все диски компьютера со всеми каталогами. Если компьютер подключен к сети, появляется возможность поиска вирусов на сетевых дисках.

Если компьютер используется в качестве почтовой станции, можно ограничиться проверкой только почтовых каталогов, в которые поступают новые файлы.

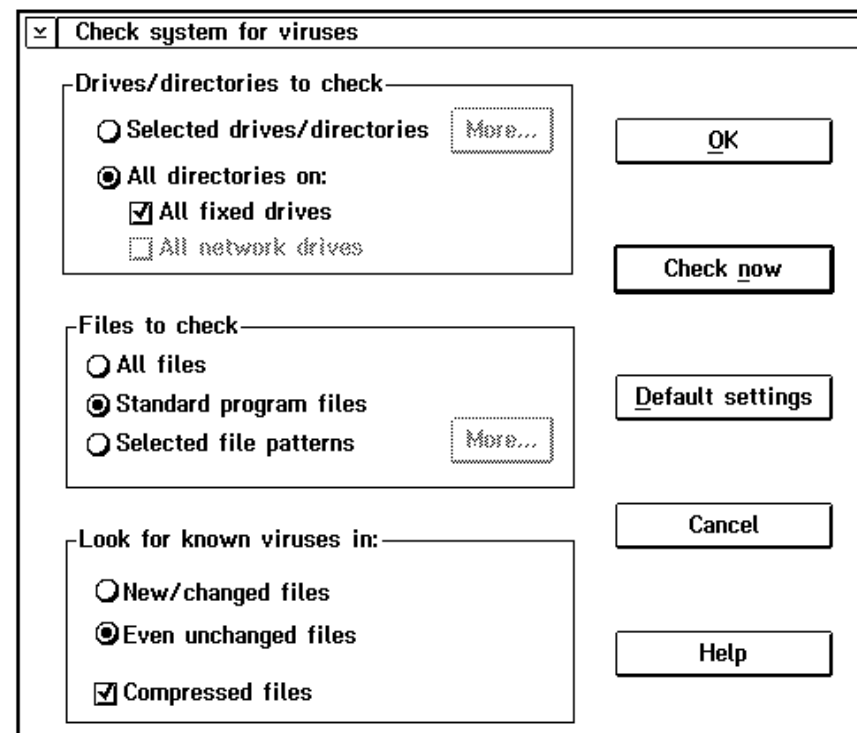


Рис. 3.42. Диалоговая панель Check system for viruses

Все ли файлы будут проверяться, определяется положением переключателя с зависимой фиксацией, размещенного в группе Files to check. Для ежедневной антивирусной профилактики можно проверять только программные файлы. Чтобы сократить время проверки, установите в группе Look for known viruses in переключатель New/changed files. В этом случае будут проверяться только новые и изменившиеся файлы.

Если вирус обнаружен, то лучше всего проверить все файлы в компьютере, включая файлы внутри архивов. Для этого установите переключатели в группе Look for known viruses in, как это показано на рисунке 3.42.

Так как практически все известные вирусы работают в среде MS-DOS, то контролю за программами, работающими в окне DOS, уделяется наибольшее внимание. Чтобы настроить режим контроля за программами MS-DOS, выберите из меню Setup строку Shield DOS. Откроется диалоговая панель Shield DOS (рис. 3.43).

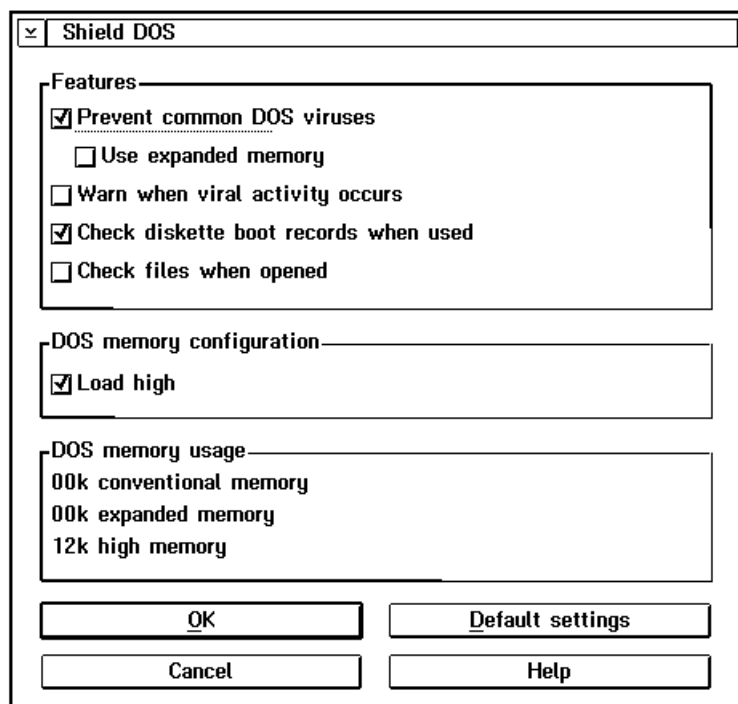


Рис. 3.43. Диалоговая панель Shield DOS

Основные параметры контроля устанавливаются в группе Features, содержащей несколько переключателей, описанных в следующей таблице:

Переключатель	Описание
Prevent common DOS viruses	Проверять заражение известными вирусами
Use expanded memory	Задействовать дополнительную память. Переключатель доступен только в том случае, если включен переключатель Prevent common DOS viruses
Warn when viral activity occurs	Антивирус сообщит пользователю, если вирус проявит активность
Check diskette boot records when used	Автоматическая проверка загрузочных секторов всех используемых дискет. Достаточно удобная функция. Немного замедляет работу с дискетами, зато позволяет обнаружить дискеты, инфицированные загрузочными вирусами

Check files when opened	Включает проверку файлов перед их запуском на выполнение
-------------------------	--

Мы рассказали, как проверить жесткие диски и диски, доступные через локальную сеть. Для проверки дискет нужно воспользоваться меню Check и выбрать из него строку Check diskettes. На экране появится диалоговая панель Check diskettes (рис. 3.44).

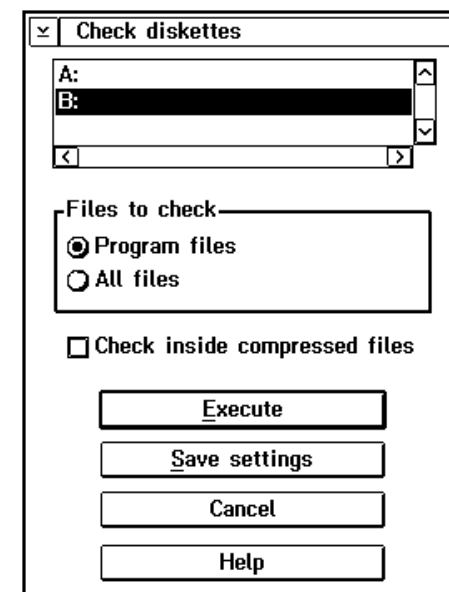


Рис. 3.44. Диалоговая панель Check diskettes

Чтобы IBM AntiVirus/2 успешно защищал компьютер от проникновения в него вирусов, необходимо постоянно обновлять вирусные базы данных программы. Это позволит обнаружить новые вирусы, появившиеся с момента выпуска программы. Обновление вирусной базы данных выполняется очень просто. Достаточно выбрать из меню Update строку Update и указать расположение файла с обновлениями вирусной базы данных.

4 ВИРУСЫ И ЛОКАЛЬНЫЕ СЕТИ

Сетевые технологии внедряются с невиданными темпами. В последнее время большинство фирм, имеющих хотя бы несколько персональных компьютеров, объединяют их в одноранговые локальные сети или локальные сети с выделенными серверами. Широкое распространение локальных сетей вызвано тем, что они позволяют поднять качество работы пользователей на новый уровень, при этом экономятся значительные материальные средства.

Локальные сети позволяют объединить ресурсы многих компьютеров, сделав их доступными для всех пользователей сети.

Например, фирма может приобрести один дорогостоящий лазерный принтер и подключить его к сети. В этом случае любой пользователь сможет печатать на нем так, как будто бы этот принтер подключен к его компьютеру.

Другая возможность, которая появляется при объединении компьютеров в сеть - совместное использование дисковой памяти. Можно установить на одном из компьютеров, подключенном к сети, диск большой емкости (скажем, несколько Гбайт) и предоставить доступ к этому диску для всех или некоторых пользователей. Так как локальные сети передают информацию очень быстро, пользователи могут работать с сетевыми дисками как с локальными, передавая информацию с одного компьютера на другой.

Однако у всякой медали есть обратная сторона. И если пользователи локальной сети могут легко передавать файлы друг другу, то вместе с ними также легко могут распространяться и компьютерные вирусы.

Novell.3120, Novell.3128

Опасные резидентные вирусы.

Если на рабочей станции загружена сетевая оболочка Novell NetWare, вирусы Novell.3120, Novell.3128 предпринимают попытку "взлома" системы защиты файл-сервера.

Содержат в своем теле следующие строки:

HYPervisor, SECURITY_EQUALS, SUPERVISOR, GROUPS_I'M_IN, PASSWORD, IDENTIFICATION, IDENTIFICATIONThe, Hypervisor, LOGIN_CONTROL, SYS:SYSTEM/SYS:LOGIN/, NET\$BIND.SYS, NET\$BVAL.SYS NET\$OBJ.SYS NET\$PROP.SYS NET\$VAL.SYS, SECURITY_EQUALS, SUPERVISOR, GROUPS_I'M_IN, PASSWORD, IDENTIFICATION, IDENTIFICATIONThe, LOGIN_CONTROL

В этой главе мы расскажем вам, как можно защитить локальную сеть персональных компьютеров от вирусного вторжения. При этом мы начнем с использования чисто административных мер (которые сами по себе являются достаточно эффективными), а закончим описанием методик применения специализированных сетевых антивирусных программ.

Разновидности локальных сетей

Так как методы защиты локальных сетей от вирусов сильно зависят от архитектуры сети, перед описанием конкретных приемов защиты и методик мы немного расскажем о том, какие бывают локальные сети.

Все существующие на данный момент локальные сети по своей архитектуре можно разделить на три группы.

К первой группе относятся небольшие одноранговые сети, объединяющие несколько компьютеров. Такие компьютеры называются рабочими станциями сети. В одноранговой сети все рабочие станции равноправны и равнозначны с точки зрения выполняемых ими функций. Каждая рабочая станция может предоставить в распоряжение всех пользователей сети свои ресурсы, например, принтер, диски или факс-модем.

Вторая группа локальных сетей - это сети с так называемым выделенным сервером (в сети может быть несколько выделенных серверов) или централизованные сети. В таких сетях один или несколько компьютеров выделяют свои ресурсы в коллективное пользование. При этом рабочие станции имеют доступ к сетевым принтерам и дискам, подключенным к серверу, но не к принтерам и дискам других рабочих станций. По своей идеологии эта группа сетей противоположна первой, объединяющей ресурсы рабочих станций.

Сети третьей группы на самом деле есть ни что иное, как комбинация одноранговых сетей с сетями второй группы, использующими выделенные серверы. При использовании такого конгломерата получается, с одной стороны, удобное взаимодействие между отдельными рабочими станциями, с другой - возможность обращения к централизованным ресурсам выделенных серверов (например, к серверам баз данных или почтовым серверам).

Одноранговые сети

К одноранговым сетям относятся такие средства, как Novell NetWare Lite, Microsoft Windows for Workgroups, Microsoft Windows 95, Lantastic и другие. Программное обеспечение перечисленных выше одноранговых сетей позволяет выделить ресурсы любой рабочей станции в коллективное пользование.

На рис. 4.1 показан пример небольшой одноранговой сети, состоящей из четырех рабочих станций. К одной из рабочих станций подключен лазерный принтер.

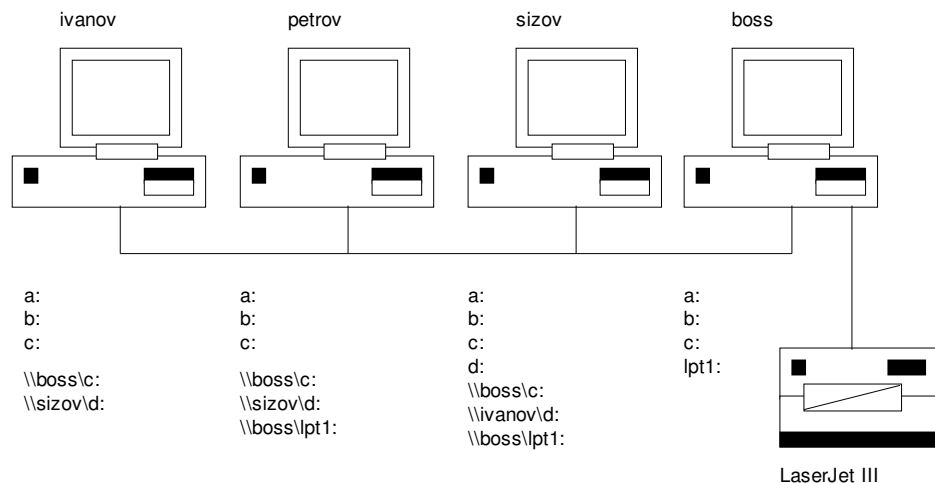


Рис. 4.1. Пример организации простейшей одноранговой сети

Каждый пользователь сети любого типа имеет свой идентификатор. В крупных сетях идентификаторы пользователей и пароли для подключения к сети назначает специально выделенный для этого человек - системный администратор или, как его еще называют, супервизор сети. В одноранговой сети пользователи сами выбирают и устанавливают свои идентификаторы.

Пользователи одноранговой сети самостоятельно выделяют ресурсы своих рабочих станций в коллективное пользование. При этом они могут указывать разрешенный вид доступа: полный доступ на чтение и запись, доступ только на чтение, никакого доступа. Дополнительно пользователь одноранговой сети может указать, что для получения доступа к ресурсам его рабочей станции другие пользователи сети должны указать пароль.

В примере, приведенном на рис. 4.1, рабочая станция пользователя с идентификатором ivanov имеет доступ к локальным ресурсам (диски a:, b: и c:), и к сетевым ресурсам рабочих станций boss (диск c:) и sizov (диск d:).

Пользователь с идентификатором petrov дополнительно имеет доступ к сетевому принтеру, подключенному к рабочей станции пользователя с идентификатором boss. Что же касается пользователя boss, то в данном случае он не подключен ни к одному сетевому ресурсу.

Как выглядят для пользователя рабочей станции сетевые ресурсы других рабочих станций?

Точно также, как и собственные, локальные.

Этот момент очень важен для понимания способа распространения вирусов в одноранговой сети.

После подключения к сетевому диску, расположенному на другой рабочей станции, пользователь получает в свое распоряжение еще одно дисковое устройство. И хотя физически это устройство может находиться в другой комнате или на другом этаже здания, с ним можно работать таким же образом, что и с локальным.

Необходимо, однако, помнить, что если вы записываете файл на такой сетевой диск, он немедленно становится доступным пользователю той рабочей станции, что предоставила этот диск в коллективное пользование.

Аналогично, если вы предоставили свой локальный диск в коллективное пользование, и не установили никакого ограничения доступа на запись, будьте готовы к тому, что на нем в любой момент могут появиться новые файлы (а также исчезнуть старые!).

Если сеть или диск или каталог доступны для вас на запись и ваша рабочая станция заражена вирусом, произойдет заражение сетевого диска или каталога

Поэтому если кто-нибудь запишет на ваш диск зараженную программу и вы запустите на выполнение, вирус может поразить ваш компьютер.

Более того, если вы имеете доступ на запись к другим сетевым дискам, вирус может заразить и те компьютеры, к дискам которых у вас есть доступ. Если же у вас есть доступ на запись ко всем дискам всех рабочих станций сети, начнется локальная вирусная эпидемия.

Сети с выделенными серверами

В сетях с выделенными серверами один или несколько компьютеров выполняют специальные функции. Они служат только для выделения ресурсов в коллективное пользование со стороны рабочих станций. Как правило, за экраном выделенных серверов пользователи не работают (часто к компьютерам, работающим в роли серверов, вообще не подключают ни клавиатуру, ни видеомонитор). Это повышает устойчивость сети и производительность серверов.

На рис. 4.2 показана конфигурация локальной сети с одним выделенным сервером.

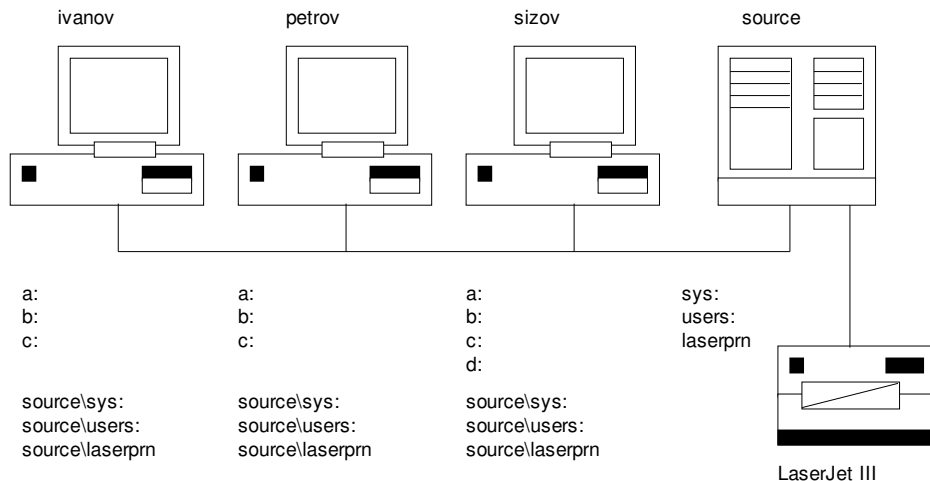


Рис. 4.2. Пример организации сети с выделенным сервером

В этой сети имеется три рабочих станции и сервер с именем source. Выделенный сервер создается (или как еще говорят, генерируется) системным администратором. Он определяет имя сервера, а также имена сетевых ресурсов и права доступа к ним.

В данном случае все пользователи имеют доступ к дисковым томам sys и users, а также к очереди печати laserprn. Эти сетевые ресурсы физически расположены на сервере, однако пользователи могут работать с ними почти также, как и с локальными ресурсами.

Сети с выделенными серверами не предоставляют пользователям возможность получения доступа к ресурсам рабочих станций. Поэтому непосредственное взаимодействие пользователей, работающих, например, над одним проектом, в таких сетях затруднено.

В результате для обмена файлами администратор создает на томах сервера каталоги, доступные всем пользователям на чтение и запись. Такие каталоги - потенциальный способ быстрого распространения вирусов по рабочим станциям сети.

Кроме того, на дисках сервера обычно находятся программы, предназначенные для запуска с рабочих станций. Если в них окажется вирус, он также может “перескочить” на диск рабочей станции, запустившей зараженную программу.

Вирусная защищенность одноранговых сетей зависит от пользователей. В противоположность этому, устойчивость к вирусам сети с выделенными серверами в значительной степени зависит от того, как системный администратор настроил права доступа пользователей к сетевым ресурсам. В нашей книге мы приведем конкретные рекомендации по такой настройке.

Комбинация одноранговых и централизованных сетей

Мы уже говорили, что пользователи централизованных сетей чувствуют себя в изоляции друг от друга. Даже если компьютеры находятся рядом, нет никаких средств для того чтобы выделить локальный диск одной рабочей станции в пользование другой.

Тем не менее, у централизованных сетей есть свои преимущества. Они более управляемы, так как находятся в полной власти системного администратора. Так как для сервера используется выделенный компьютер со специализированной сетевой операционной системой, быстродействие централизованной сети оказывается заметно выше, чем одноранговой.

С другой стороны, одноранговые сети очень удобны для объединения рабочих групп пользователей. Современные одноранговые операционные системы, такие как Microsoft Windows 95, содержат в себе средства, позволяющие не просто обмениваться файлами или печатать на принтере соседа, но выполнять коллективную работу над одним документом, передавать по сети содержимое универсального буфера обмена Clipboard, “разговаривать” с помощью экрана и клавиатуры или даже проводить видеоконференции.

Но системные администраторы не стоят перед выбором: установить им одноранговую сеть или централизованную. Можно использовать обе одновременно, дополняя высокую производительность централизованных сетей удобными средствами взаимодействия пользователей внутри рабочих групп, присущими одноранговым сетям.

На рис. 4.3 показана комбинированная сеть, в которой пользователи имеют доступ не только к сетевым ресурсам сервера, но и к ресурсам других рабочих станций.

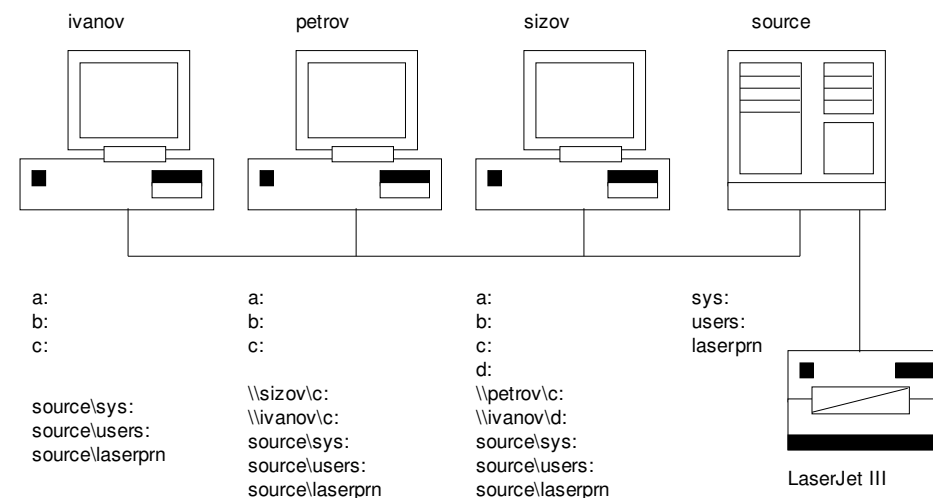


Рис. 4.3. Комбинирование централизованной и одноранговой сети

Следует заметить, что администрирование комбинированных сетей намного сложнее, чем централизованных, так как в системе присутствует такая неуправляемая компонента,

как пользователи рабочих станций. Выделяя в коллективное пользование ресурсы своих рабочих станций, пользователи могут сильно ослабить защиту системы от вирусов и от несанкционированного доступа.

В этом случае администратор должен сочетать меры по обеспечению безопасности централизованной сети с защитой рабочих станций и “воспитательной” работой среди пользователей.

Способы распространения вирусов в сетях

Распространение вирусов в одноранговых, централизованных и комбинированных сетях происходит по разному, однако результат практически всегда один и тот же - программы, расположенные на рабочих станциях и дисках сервера оказываются зараженными.

Рассмотрим особенности распространения вирусов в перечисленных выше типах компьютерных сетей.

Вирусы в одноранговых сетях

Распространение вирусов в одноранговых сетях возможно благодаря тому, что пользователи предоставляют доступ на запись к дискам своих рабочих станций.

Все происходит очень просто.

Рано или поздно один из пользователей приносит дискету, зараженную загрузочным или файловым вирусом. При активизации вирус просматривает все диски, доступные на запись, и заражает расположенные там программы.

Некоторые загрузочные вирусы, которые распространяются только через загрузочные секторы локальных дисков, не могут перейти через сеть на диски другой рабочей станции, даже если к этому диску имеется доступ на запись. Дело здесь в том, что для записи в загрузочные секторы необходимо использовать систему ввода-вывода, расположенную в BIOS, а эта система “не умеет” работать с секторами сетевых дисков. Способ записи вируса в загрузочные секторы, основанный на непосредственной работе с дисковым контроллером, также не подходит для сетевого диска, так как контроллер подключен к другой станции и его порты ввода-вывода абсолютно недоступны.

Однако комбинированные файлово-загрузочные вирусы закрепляются в загрузочных секторах локального диска рабочей станции и заражает файлы, расположенные на всех дисках, доступных для записи. В том числе, разумеется, и файлы, расположенные на сетевых дисках, принадлежащих другим рабочим станциям.

Если пользователь предоставил к своим дискам доступ только на чтение, но на них записаны зараженные программы, то другие пользователи смогут запустить такую программу. В результате этого их локальные диски окажутся зараженными.

Вирусы в централизованных сетях

Несмотря на то что в централизованных сетях пользователи не имеют доступа к ресурсам других рабочих станций, имеется по крайней мере две возможности для распространения вирусов.

Во-первых, вирус может попасть с одной из рабочих станций на диски сервера, доступные для записи, заразив записанные там программы. Когда пользователь другой рабочей станции запустит зараженную программу непосредственно с диска сервера или вначале перепишет ее на локальный диск и затем запустит ее там, рабочая станция окажется зараженной. Таким образом, через некоторое, возможно очень небольшое время, вирус попадет с сервера на все рабочие станции сети и заразит их.

Во-вторых, существует принципиальная возможность создания такого вируса, который сумеет подобрать пароль системного администратора и записать себя даже на диски, защищенные от записи. И все это несмотря на то, что современные сетевые операционные системы имеют достаточно мощную и надежную систему разграничения доступа. Однако известно: что один человек сделал, другой может сломать.

Несмотря на то, что система паролей потенциально обладает высокой устойчивостью, усилия пользователей могут свести всю защиту на нет. Например, для того чтобы облегчить себе жизнь, они не задают пароли вообще или указывают в качестве пароля свое имя или фамилию, год рождения и т. п.

Следите за тем, чтобы пользователи задавали пароли для подключения к сети

Между тем существует список наиболее распространенных паролей, который доступен через электронные доски объявлений и, конечно же, имеется в распоряжении разработчиков вирусов. Таким образом, при подборе пароля вирусу не нужно перебирать громадное количество случайно выбранных комбинаций символов, а достаточно пройти по указанному списку. Вероятность успеха при этом достаточно велика.

Login-2971/2967, Login-2972/2968

Резидентный вирус.
Заражает программы с расширением имени COM и EXE.
При заражении COM-файла записывает четыре лишних байта.
Плагиат на самый известный классический вирус M2C. Содержит многочисленные куски вируса M2C, ставшие после модификации “оригинального варианта” абсолютно бессмысленными. Собственное творчество автора направлено на определение чужих паролей в локальной сети. Для этого во время работы программы LOGIN.EXE перехватываются коды символов, введенных с клавиатуры, которые затем накапливаются. В результате эти коды оказываются в зараженных файлах.

Правильно настроив права доступа пользователей и саму систему управления доступом, системный администратор может значительно уменьшить опасность поражения вирусами дисков сервера. Существенную помощь в защите сервера могут оказать специальные антивирусные программы и аппаратные средства защиты, которые мы рассмотрим в нашей книге.

Вирусы в комбинированных сетях

Как и следовало ожидать, в комбинированных сетях вирусы могут распространяться как непосредственно между рабочими станциями, так и через диски серверов. При этом вирусы могут попадать на диски, доступные для записи или же они могут предпринимать попытки подбора паролей для получения доступа к дискам, защищенным от записи.

Взяв на себя ответственность по сопровождению комбинированной сети, для предотвращения возникновения вирусной эпидемии системный администратор должен защищать от вирусов не только сервер, но и рабочие станции.

Вирус в оперативной памяти сервера

Так как вирус является программой, для активизации он должен быть загружен в оперативную память, после чего вирусу должно быть передано управление.

Когда вирус “живет” на рабочей станции, так и происходит. Пользователь запускает зараженную программу или загружает операционную систему с дискеты, зараженной загрузочным вирусом, в результате чего вирус тем или иным способом оказывается в оперативной памяти рабочей станции.

Если же пользователь запускает зараженную программу непосредственно с диска сервера, вирус опять-таки попадает в оперативную память рабочей станции, с которой был выполнен запуск.

Таким образом, обычный вирус, не рассчитанный специально для работы под управлением сетевой операционной системы, может изменить только содержимое файлов, расположенных на доступных для записи дисках. Но он *не может* изменить загрузочные секторы на дисках сервера, так как для этого вирус должен попасть в оперативную память сервера как программа и получить управление.

Тем не менее, возможно создание таких вирусов, которые запускают себя как процесс в среде сетевой операционной системы. Такие вирусы наиболее опасны, так как им доступны все ресурсы сервера.

Например, взломав тем или иным способом пароль супервизора, вирус может записать себя в системный каталог сервера Novell NetWare в виде nlm-программы и указать ее имя в файле автоматического конфигурирования startup.ncf. При этом вирусная nlm-программа будет получать управление каждый раз при загрузке сервера.

Современные сетевые операционные системы, такие например, как Microsoft Windows NT, допускают удаленный запуск процедур. Эта возможность также может быть использована специализированными сетевыми вирусами для распространения или для нанесения повреждений.

Защита от вирусов одноранговых сетей

В этом разделе мы рассмотрим методику защиты от вирусов наиболее распространенных одноранговых сетей Novell NetWare Lite, Microsoft AddOn for Workgroups, Microsoft Windows for Workgroups версии 3.11 и Microsoft Windows 95.

Для защиты одноранговых сетей необходимо использовать комбинацию административных мер со специализированным антивирусным программным обеспечением.

Задача защиты одноранговой сети может быть разделена на две задачи:

- защита рабочих станций от проникновения в них вирусов извне;
- предотвращение быстрого и бесконтрольного распространения вирусов с одной рабочей станции на остальные.

Что касается способов решения первой задачи, то тут можно принимать те же меры, что и для защиты компьютеров, не подключенных к сети. Это установка специализированного антивирусного программного обеспечения, отключение НГМД (непопулярная, но достаточно эффективная мера), жесткий контроль за новым программным обеспечением с помощью антивирусных программ (даже если они не предназначены специально для работы в сети).

Проверяйте все новые программы, перед тем как устна вливать их в сетевые кати логи. Исполъзуйте для этого специальные антивирусные средства

Одноранговые сети обычно не позволяют создавать бездисковые рабочие станции, так как соответствующие сетевые программы должны находиться на локальных дисках рабочих станций. Однако администратор сети (или кто-то из технического персонала) может отключить НГМД или вовсе изъять их из компьютера. В этом случае пользователь не сможет вставить никакую дискету в компьютер, в том числе дискету с зараженной программой.

Надежнее всего отключить НГМД аппаратно, однако для такого отключения нужно открывать корпус компьютера. В качестве альтернативы мы предлагаем отключение при помощи программы BIOS Setup. Дополнительно администратор сети должен назначить пароль для запуска этой программы, чтобы пользователь не смог самостоятельно подключить НГМД.

Бездисковые рабочие станции или станции с отключенными накопите лями на гибких магнитны х дисках представляют собой серьезное препятст вие для проникновения вирусов в сеть

Казалось бы, работать на компьютере с отключенным НГМД неудобно, но это только на первый взгляд. К тому же все зависит от того, какая именно работа выполняется. Если несколько пользователей обращаются к общей базе данных, расположенной на диске

одной из рабочих станций, записывая в нее информацию или извлекая ее оттуда с целью просмотра или печати, НГМД не нужен.

Другое преимущество рабочих станций с отключенными НГМД - невозможность кражи секретной или конфиденциальной информации недобросовестными сотрудниками. Здесь только нужно учесть, что в настоящее время появились дисковые устройства, подключаемые к параллельному или последовательному порту компьютера. Их можно использовать для чтения или записи. Кроме того, к указанным выше портам нетрудно подключить малогабаритный компьютер типа Notebook, организовав несанкционированную передачу данных с помощью, например, такой распространенной программы, как Norton Commander. Однако обсуждение проблем обеспечения безопасности такого рода выходит за рамки нашей книги, посвященной борьбе с вирусами. Тем не менее, в ответственных случаях можно отключить неиспользуемые параллельные и последовательные порты с помощью все той же программы BIOS Setup. Практически все современные версии BIOS позволяют это сделать.

Вторая задача (предотвращение распространения вируса в сети), решается прежде всего правильной организацией доступа пользователей к сетевым ресурсам. Существенную помощь в этом также окажут антивирусные средства, позволяющие обнаружить вирус на ранней стадии его появления, предотвратив дальнейшее распространение.

Основное правило распределения доступа заключается в том, что не следует предоставлять пользователям права доступа, которые не нужны им для выполнения работы.

Никогда и ни при каких обстоятельствах не предоставляйте обычным пользователям права записи во все сетевые каталоги и особенно в корневые каталоги сетевых томов

Администратор должен тщательно продумать права доступа для сетевых каталогов. При этом следует по возможности не предоставлять пользователям права на запись, особенно для каталогов, содержащих загрузочные файлы программ. Очевидно, если пользователь имеет права на запись в сетевой каталог, содержащий программы, то при возникновении на его рабочей станции вирусов, они заразят файлы в сетевом каталоге.

Приведем конкретные рекомендации по административным мерам защиты наиболее распространенных одноранговых сетей.

Novell NetWare Lite

Сеть Novell NetWare Lite достаточно распространена ввиду простоты установки и сопровождения. Эта сеть нетребовательна к ресурсам и неплохо работает даже на дешевых компьютерах с процессором i80286 и объемом оперативной памяти 1 Мбайт. Сетевое программное обеспечение Novell NetWare Lite поставляется на дискетах. Для каждой рабочей станции вы должны приобрести отдельный комплект дискет.

Полностью процедура установки и настройки сети Novell NetWare Lite приведена в 4-том нашей серии книг “Персональный компьютер. Шаг за шагом”, который называется “Сети компьютеров в вашем офисе”. Однако для удобства мы расскажем о том, как в сети Novell NetWare Lite выполняются процедуры создания пользователей и определение прав доступа к сетевым ресурсам. Именно эти вопросы наиболее важны для организации защиты от вирусов административными методами.

После установки Novell NetWare Lite на диске C: рабочей станции создается каталог NWLITE, в котором есть два подкаталога с именами NLCNTL и TUTOR, а также файлы самой оболочки NetWare Lite.

В каталоге C:\NWLITE имеется файл startnet.bat, который предназначен для запуска сетевой оболочки. Вот его содержимое:

LSL
NE2000
IPXODI.A
SHARE
SERVER
CLIENT

В этом файле запускается несколько резидентных программ. Вначале запускается программа lsl.com. Эта программа реализует так называемую спецификацию открытого интерфейса связи (Open Link Interface - OLI) - стандартную спецификацию для одновременной работы в одной сети нескольких коммуникационных протоколов. Программа lsl.com служит связующим звеном между драйвером сетевого адаптера (в нашем случае драйвером является программа ne2000.com) и коммуникационным протоколом IPX.

После lsl.com загружается драйвер сетевого адаптера ne2000.com, затем программа ipxodi.com. Программа ipxodi.com реализует коммуникационный протокол IPX (параметр A указывает, что программа ipxodi.com должна загружать модули, отвечающие только за базовые возможности IPX).

Далее происходит запуск утилиты MS-DOS share.exe. Эта утилита нужна для безопасной работы с файлами в мультипользовательском режиме.

В конце файла startnet.bat запускаются программы server.exe и client.exe. Если рабочая станция должна выполнять только функции сервера, не запускайте программу client.exe, если только клиента - не запускайте программу server.exe.

Файл startnet.bat запускается, как правило, автоматически при загрузке операционной системы MS-DOS из файла autoexec.bat, однако пользователи могут запускать его вручную при необходимости.

Для того чтобы защитить рабочую станцию от нападения вирусов, полученных из сети, следует выделять дисковые ресурсы своей станции по возможности только для чтения. Особенно это относится к каталогам, в которых находятся загрузочные файлы программ.

Если пользователь зараженной рабочей станции имеет доступ к вашим дискам только на чтение, такой же доступ есть и у вирусов. Поэтому он не повредит ваши файлы.

Для выделения ресурсов рабочей станции в коллективное пользование и управления доступом других пользователей к этим ресурсам вы должны запустить программу net.exe, которая расположена в каталоге NWLITE. В ответ на сообщение следует ввести имя пользователя - SUPERVISOR.

При этом вы будете подключены к сети как системный администратор. На экране появится меню утилиты net.exe (рис. 4.4).



Рис. 4.4. Главное меню утилиты net.exe

С помощью этого меню вы можете, в частности, создавать сетевые каталоги, подключать к сети новых пользователей и определять их права доступа.

Прежде всего надо создать пользователей и определить их права. Для этого выберите в меню строку Supervise the network (управление сетью). Появится меню Supervise the network (рис. 4.4), в котором вам надо выбрать строку Users.

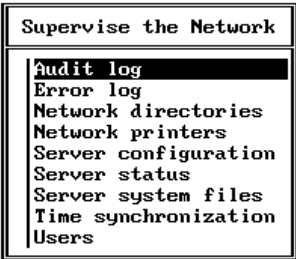


Рис. 4.4. Меню Supervise the network

После этого на экране появится меню Users. В нем будет только один пользователь с именем SUPERVISOR. Нажмите клавишу <Insert> и введите имя нового пользователя. Имя должно состоять не более чем из 15 символов. Завершите ввод клавишей <Enter>.

Затем на экране появится диалоговая панель Account Information for User..., где вместо многоточия будет указано имя создаваемого пользователя. В поле User's full name задайте полное имя пользователя.

Содержимое поля Supervisor privileges определяет, обладает ли пользователь привилегиями супервизора сети. Если в этом поле находится значение Yes, пользователь обладает правами супервизора.

Обычно в небольшой сети, состоящей из нескольких компьютеров, для упрощения обслуживания сети всем пользователям предоставляются права права супервизора. Однако с точки зрения устойчивости сети к вирусам этого нельзя делать ни в коем случае. Помните - права пользователя автоматически переходят к вирусу.

|| *Предоставляйте пользователям минимально возможные права доступа*

В поле Password вы сможете задать пароль для пользователя. Если пользователь забыл свой пароль, супервизор может его изменить, нажав в поле Password два раза клавишу <Enter>. Не пренебрегайте паролем, особенно для дисков и каталогов, доступных на запись. Несмотря на потенциальную возможность создания вирусов, “подсматривающих” или подбирающих пароль, большинство вирусов не умеют этого делать.

Подготовив все поля, нажмите клавишу <Esc> и подтвердите свое желание сохранить сделанные изменения. Для этого выберите строку Yes в появившемся меню Save changes.

Предоставляя доступ другим рабочим станциям к собственным каталогам и дискам, не забудьте указать минимально необходимые права доступа.

Для создания сетевых каталогов, доступных другим пользователям, вы должны запустить программу net.exe и войти в сеть как супервизор. В главном меню утилиты выберите строку Supervise the network. В появившемся меню выберите строку Network directories. Вы увидите список существующих сетевых каталогов Network Directory Server (рис. 4.5).

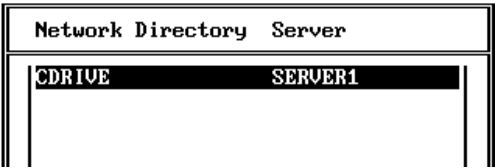


Рис. 4.5. Список существующих сетевых каталогов

Для создания нового каталога нажмите клавишу <Insert>. Появится меню серверов NetWare Lite. Выберите нужный вам сервер и нажмите клавишу <Enter>. Вам будет предложено ввести имя сетевого каталога, которое должно состоять не более чем из 15 символов.

После ввода имени каталога вы окажетесь в диалоговой панели, с помощью которой нужно описать создаваемый сетевой каталог (рис. 4.6).

Information for Network Directory DDRIVE on Server SERVER1	
Actual directory path (48 max):	D: [REDACTED]
Default access rights	: ALL
Users with nondefault rights	: (Press Enter to see list)

Рис. 4.6. Описание создаваемого сетевого каталога

В поле Default access rights укажите права доступа к каталогу, присваиваемые пользователям по умолчанию. Вы можете указать ALL для предоставления полного доступа к каталогу (чтение и запись), READ для разрешения доступа на чтение и NONE для полного запрещения доступа к каталогу. По возможности избегайте предоставления полного доступа.

Если некоторые из пользователей должны иметь в данном каталоге права, отличные от прав, заданных по умолчанию, воспользуйтесь полем Users with nondefault rights.

Microsoft AddOn for Workgroups

Сеть Microsoft AddOn for Workgroups, так же как и сеть Novell NetWare Lite, позволяет объединить компьютеры с процессором i80286 и с объемом оперативной памяти 1 Мбайт. Дополнительно программное обеспечение Microsoft AddOn for Workgroups позволяет получить доступ рабочим станциям MS-DOS к серверам на базе Microsoft Windows for Workgroups и Windows NT. В силу этого сети Microsoft AddOn for Workgroups получили достаточно широкое распространение. Полное описание приемов работы в среде этой сети вы найдете приведена в 4 томе нашей серии книг “Персональный компьютер. Шаг за шагом”.

Методика защиты этой сети от вирусов полностью аналогична методике защиты сети Novell NetWare Lite. Рабочие станции сети должны быть защищены обычными несетевыми антивирусными средствами, такими, например, как антивирусный комплект АО “ДиалогНаука” или аппаратное устройство защиты Sheriff. Кроме того, необходимо ограничить доступ пользователей к сетевым каталогам, особенно на запись.

Отдавая в коллективное пользование локальный диск или каталог рабочей станции, вы должны запустить программу net.exe с параметром share:

```
net share Name=Drive:[\Path]
```

Параметр Name определяет имя, под которым пользователи сети увидят ваш каталог. Нужно также указать локальный диск Drive, на котором этот каталог расположен, и путь к каталогу Path.

Например, для того чтобы предоставить доступ к каталогу d:\src, можно использовать следующую команду:

```
net share source=d:\src
```

Полный формат параметров команды share для распределения дисков представлен ниже:

```
net share ShareName=Drive:[Path][\remark:"Text"][/saveshare:no]
[/read[:Pwd1]][/full[:Pwd2]]
```

Здесь ShareName - сетевое имя, которое будет видно пользователям других рабочих станций.

Дополнительно при распределении диска или каталога вы можете указать параметры /remark, /saveshare:no, /read и /full.

Параметр /remark позволяет задать произвольный текстовый комментарий Text, описывающий ресурс. Если указать параметр /saveshare:no, каждый раз при запуске рабочей станции вам придется заново отдавать ее ресурсы в коллективное пользование запуском программы net.exe с параметром share.

Вы можете ограничить доступ пользователей (и, соответственно, вирусов) к дискам вашей рабочей станции, указав при распределении параметры /read и /full с паролем или без пароля.

По умолчанию предоставляется доступ только на чтение (которому соответствует параметр /read), причем без пароля. Для предоставления полного доступа к диску или каталогу вы должны указать параметр /full (с паролем или без).

Например, следующая команда предоставляет полный доступ к каталогу d:\src только после предъявления пароля:

```
net share source=d:\src /remark:"Source Code Lib" /full:pwdfull
```

Microsoft Windows for Workgroups версии 3.11

Одноранговая сеть Microsoft Windows for Workgroups версии 3.11 также получила широкое распространение, так как она обеспечивает удобные средства интеграции рабочих групп пользователей, встроенные непосредственно в графическую среду Windows.

Приложение File Manager, которое поставляется в составе дистрибутива Microsoft Windows for Workgroups, позволяет выделять ресурсы рабочей станции в коллективное пользование и подключаться к сетевым ресурсам. Для этого достаточно просто нажать нужную кнопку на полосе инструментальных средств Toolbar (рис. 4.7).

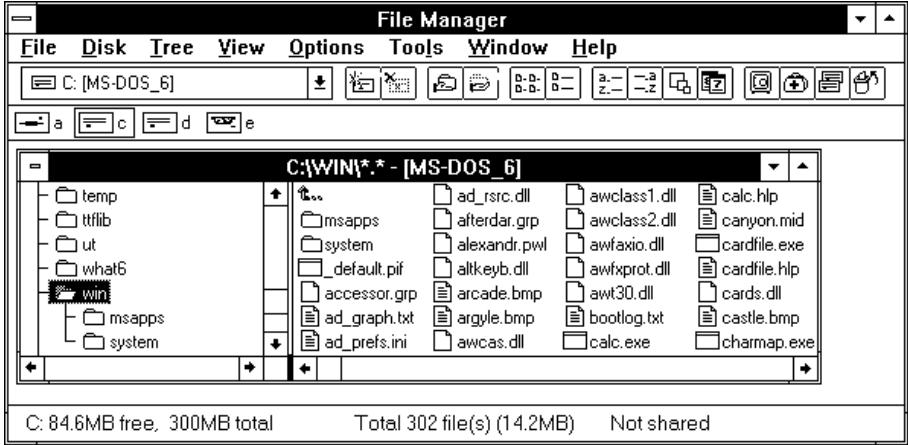







Рис. 4.7. Главное окно приложения File Manager операционной системы Microsoft Windows for Workgroups версии 3.11

Ниж е мы перечислили назначение некоторых кнопок, имеющих в основном отношение к дисковым сетевым ресурсам.

Кнопка	Описание
	Подключение к сетевому диску (т. е. к диску, расположенному на другой рабочей станции сети)
	Отключение от сетевого диска
	Предоставление локального диска рабочей станции в коллективное пользование. Диск будет доступен для всех пользователей сети (возможно, после предъявления пароля)
	Отмена коллективного доступа к диску
	Запуск приложения Microsoft Antivirus for Windows

Обратите внимание, что среди других кнопок есть кнопка для запуска антивирусного приложения Microsoft Antivirus for Windows. Это приложение поставляется в составе MS-DOS.

Для предоставления локального диска или каталога в коллективное пользование нажмите соответствующую кнопку.

После этого на экране появится диалоговая панель Share Directory (рис. 4.8).

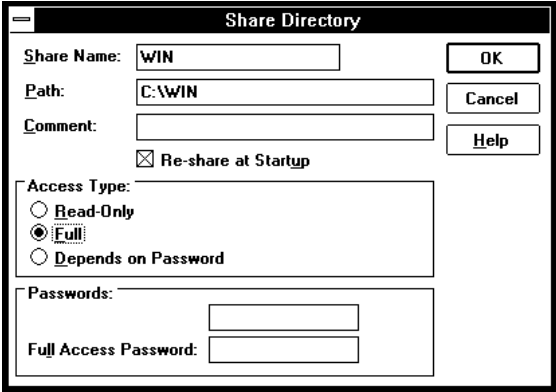


Рис. 4.8. Диалоговая панель Share Directory, предназначенная для выделения диска или каталога в коллективное пользование

В поле Share Name следует задать произвольное имя, под которым этот каталог будет виден другим пользователям.

Группа переключателей Access Type позволит вам определить права доступа к создаваемому сетевому ресурсу.

Если включить переключатель Read-Only, пользователи получают доступ только на чтение. Включив переключатель Full, вы можете предоставить полный доступ (на чтение и на запись). И, наконец, если включить переключатель Depends on Password, вы сможете задать два пароля: один для доступа только на чтение, другой - для полного доступа. Те пользователи, которые знают только пароль на чтение (а также вирусы, не умеющие подбирать пароль), не смогут использовать сетевой диск для записи.

Не следует предоставлять пользователям права доступа в сетевые каталоги, содержащие исполнимые файлы или дистрибутивы программных продуктов

Пароль указывается в группе полей Passwords. В зависимости от установки переключателей Access Type в этой группе может быть одно или два поля для ввода, соответственно, пароля на чтение и на запись. После ввода следует подтвердить пароли, указав их еще раз в диалоговой панели Confirm New Password (рис. 4.9).

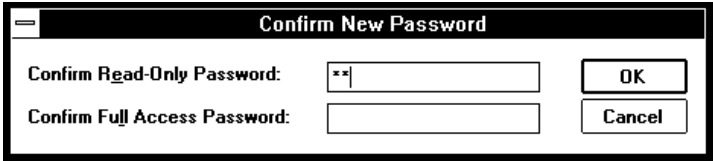


Рис. 4.9. Повторный ввод пароля для проверки

Microsoft Windows 95

Новая операционная система Microsoft Windows 95 предназначена для замены операционных систем Microsoft Windows версии 3.1 и Microsoft Windows for Workgroup версии 3.11. В нее встроены средства организации одноранговой сети, поэтому любой пользователь может выделить ресурсы своей станции в коллективное пользование.

Способ такого выделения очень прост - достаточно сделать щелчок правой клавишей мыши по пиктограмме ресурса и в появившемся контекстном меню выбрать строку Sharing.

На экране появится блокнот, в котором нас будет интересовать страница Sharing, показанная (для диска C:) на рис. 4.10.

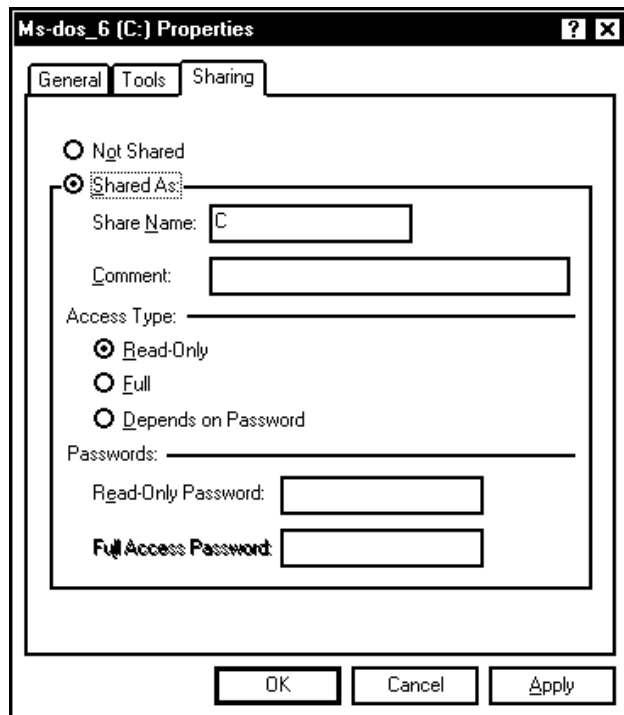


Рис. 4.10. Страница Sharing, с помощью которой можно задать атрибуты доступа для сетевого каталога или диска

Для ограничения доступа к диску следует воспользоваться переключателями из группы Access Type. Вы можете предоставить полный доступ к ресурсу (включив переключатель Full), только на чтение (при помощи переключателя Read-Only) или в зависимости от пароля (Depends on Password). Перечисленные варианты доступа полностью соответствуют тем, что используются в Microsoft Windows for Workgroups.

Если вы собираетесь разрешить доступ к своему диску на запись, укажите в поле Full Access Password пароль. В противном случае вирусы смогут беспрепятственно проникнуть на ваш диск с любой рабочей станции.

Заметим, что если пользователь получил доступ к вашему диску на запись, предоставив необходимый пароль, а затем запустил зараженную программу, вирус “перескочит” на ваши диски. Поэтому чисто административные меры борьбы с вирусами необходимо комбинировать с использованием специального антивирусного программного обеспечения, установленного на все рабочие станции одноранговой сети.

Защита централизованных сетей

В централизованных сетях с файл-серверами Novell NetWare или IBM Lan Server необходимо защищать от проникновения вирусов, с одной стороны, рабочие станции, с другой - файл-серверы.

Что касается методов защиты рабочих станций, то они уже были нами описаны. Здесь вы можете использовать ту же методику, что и для защиты персональных компьютеров, не объединенных в сеть.

Novell-708

Резидентный вирус.

Заражает только программы с расширением имени COM. Пытается обращаться к программному интерфейсу Novell NetWare.

Защита файл-сервера может выполняться как административными мерами, так и с помощью специальных антивирусных программ, работающих в среде сетевой операционной системы.

Административные меры подразумевают правильное распределение прав доступа пользователей к сетевым каталогам, расположенным на дисках сервера. Необходимо также принимать специальные меры предосторожности при подключении к сети пользователей с правами администратора. Последнее особенно важно из-за того что администраторы имеют права на запись в любые каталоги, поэтому если на рабочей станции администратора находится активный вирус, он может заразить все программные файлы, расположенные на сервере.

В настоящее время несколько производителей предлагают специальные антивирусные программы, которые запускаются на файл-сервере и работают, как правило, в фоновом режиме, постоянно проверяя сетевые каталоги. Дополнительно такие программы могут сканировать все файлы, которые записываются на диски сервера или читаются с них, однако такой режим работы, очевидно, уменьшает производительность системы. Используя программные средства защиты от вирусов, необходимо постоянно пополнять базу данных вирусов или получать новые версии антивирусных средств. В

противном случае возможно поражение сервера новым вирусом, информация о котором раньше отсутствовала у разработчика антивирусных средств.

Novell-3120

*Резидентный вирус с элементом и стилем технологии.
Заражает программы с расширением имени COM и EXE. Пытается
обращаться к программному интерфейсу Novell NetWare.*

Аппаратные средства защиты (и только они) помогут вам в том случае, если вирус сумел “подсмотреть” или подобрать пароль системного администратора. Например, вы можете защитить аппаратно тома сервера от записи. Если в этом случае вирус (или системный администратор) попытается изменить содержимое какого-либо файла на таком томе, защита сработает и сервер будет заблокирован.

Далее мы рассмотрим особенности защиты от вирусов сетей Novell NetWare и серверов с серверами IBM LAN Server.

Защита сети Novell NetWare версии 3.12

Сеть Novell NetWare версии 3.12 очень распространена в России благодаря ее высокой надежности и быстродействию, а также удобству в администрировании. В 3-й книге “Персональный компьютер. Шаг за шагом” мы подробно рассмотрели процесс ее установки, настройки и использования, поэтому здесь мы ограничимся только самыми минимальными сведениями, нужными для организации защиты серверов Novell NetWare и всей сети в целом от вирусов.

Пользователи сети Novell NetWare и их права

Пользователей сети Novell NetWare можно разделить на обычных, администраторов групп и системных администраторов (супервизоров).

Системный администратор обладает неограниченными правами, в то время как администратор групп может подключать к серверу новых пользователей (или создавать новые группы пользователей). Администратор групп может наделять правами созданные им группы пользователей и отдельных пользователей в рамках прав, предоставленных ему системным администратором. Группы могут объединять любых пользователей, имеющих сходные права доступа к тем или иным сетевым ресурсам.

Именно системный администратор должен определять стратегию распределения прав в сети. При этом, если в сети много пользователей и групп, он может делегировать часть своих прав администраторам групп. На системном администраторе должна лежать и работа по организации защиты сети от вирусов.

Предоставление доступа к сетевым каталогам

Основной принцип, которому должен следовать системный администратор, вырабатывая стратегию предоставления доступа заключается в том, что пользователям не следует предоставлять прав, которые не нужны им для работы. Если следовать этому принципу, можно избежать многих неприятностей, связанных с потерей или искажением данных,

хранящихся на сервере. В том числе, с потерями или искажениями, вызванными вирусами.

Кроме этого, следует убедиться в том, что те права, которые запрашиваются пользователями, действительно им нужны. Вполне возможно, что в ряде случаев хватило бы и меньших прав.

Наиболее грубая ошибка системного администратора заключается в предоставлении кому бы то ни было прав на запись в системные каталоги LOGIN, PUBLIC, SYSTEM. К каталогу SYSTEM никто, кроме системного администратора, не должен иметь доступ ни на чтение, ни тем более на запись.

Никогда не предоставляйте пользователям права доступа на запись в каталоги LOGIN, PUBLIC, SYSTEM. Обычный пользователь не должен иметь никаких прав на доступ к каталогу SYSTEM

Представьте себе, что системный администратор предоставил всем пользователям право записи в каталог LOGIN. Если на одной из рабочих станций появится активный вирус, он заразит файл LOGIN.EXE, который используется для подключения пользователей к сети. Теперь когда любой другой пользователь подключится к сети или просто просмотрит список серверов при помощи программы SLIST.EXE, расположенной в том же каталоге, вирус заразит его рабочую станцию. Через некоторое (очень небольшое) время вирусная эпидемия охватит всю сеть.

Если же к сети подключится системный администратор, имеющий права на запись во все сетевые каталоги, вирус моментально проникнет на все диски файл-сервера.

Системный администратор должен подключаться к сети только с проверенной на отсутствие вирусов рабочей станции, иначе вирус проникнет во все сетевые каталоги

Описанная выше ситуация не является гипотетической. Мы столкнулись с ней в одной фирме, которая вызывала нас для антивирусной профилактики через службу “Компьютерной скорой помощи”®, которая создана в АО “ДиалогНаука”.

Случай с каталогом LOGIN можно обобщить. Любой программный файл, доступный для записи, служит потенциальным средством распространения вируса в сети. Поэтому мы настоятельно рекомендуем защищать от записи все каталоги, содержащие программные файлы.

Лучше всего если системный администратор выделит для данных, которые изменяются пользователями (например, для файлов баз данных) отдельные каталоги. В этих каталогах пользователи могут иметь права доступа на запись. Системный администратор должен следить за тем, чтобы в таких каталогах не появлялись программные файлы, так как они могут оказаться зараженными вирусами.

В последнее время появились вирусы, поражающие файлы документов, например, doc-файлы, создаваемые текстовым процессором Microsoft Word for Windows. По

большей части системный администратор не может хранить такие файлы в защищенных от записи каталогах, так как пользователи постоянно редактируют свои документы. В этом случае необходимо применять специальные антивирусные средства на рабочих станциях, например, Doctor Web for WinWord.

```
Novell-528

Резидентный вирус.
Заражае только ко программы с расширением имени COM.
При завершении программы дважды исполняется функция
программного интерфейса Novell NetWare "Add Trustee to directory" с
именами "WORK:" и "SYS:". Эта функция предназначена для добавления
прав доступа к сетевым каталогам.
```

Для предоставления прав доступа к сетевым каталогам системный администратор должен запустить программу SYSCON.EXE, которая находится в каталоге PUBLIC. Детальное описание этого процесса выходит за рамки нашей книги, однако мы сделаем некоторые замечания. При необходимости вы можете обратиться к 3 тому нашей серии книг “Персональный компьютер. Шаг за шагом”.

Полный список прав доступа к каталогам и файлам, которые системный администратор может предоставить пользователям, показан на рис. 4.11.

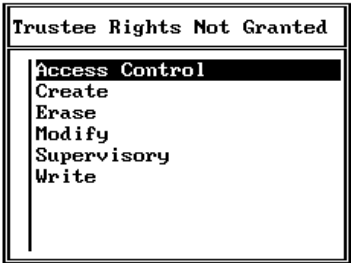


Рис. 4.11. Права доступа к сетевым каталогам и файлам

Ниже мы приведем обозначение и краткое описание видов доступа к файлам и каталогам.

Вид доступа	Обозначение	Что разрешено
Access Control	A	Изменение прав доступа к каталогу или файлу
File Scan	F	Просмотр содержимого каталога
Create	C	Создание каталогов или файлов в данном каталоге
Erase	E	Удаление каталогов или файлов из данного каталога

Modify	M	Изменение содержимого файлов (перезапись)
Supervisory	S	Права супервизора (можно делать любые операции над файлами, расположенными в каталоге)
Write	W	Запись в файл

Для обычных пользователей достаточно указывать следующие виды доступа: File Scan, Create, Erase, Modify, Write. Для администраторов групп дополнительно можно указать права Access Control.

Если каталог содержит программные файлы, для него не следует разрешать доступ Write, Modify, Erase, Create.

Предоставление доступа к отдельным файлам

Программа FILER.EXE, расположенная в каталоге PUBLIC, позволяет системному администратору устанавливать права доступа к отдельным файлам (рис. 4.12).

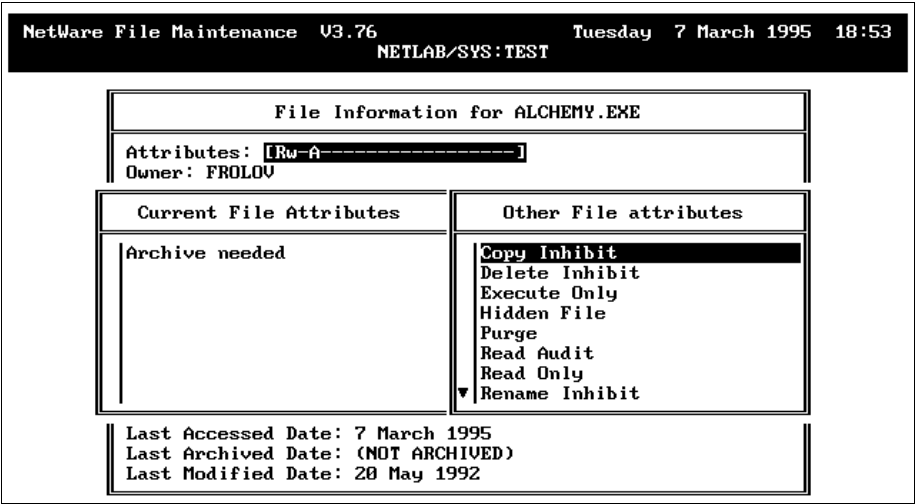


Рис. 4.12. Просмотр и изменение атрибутов файла

В частности, для защиты файла от нападения вирусов вы можете установить для него атрибут Read Only.

Системные администраторы знают о существовании очень интересного атрибута Execute Only, который можно установить, но нельзя снять (во всяком случае, нет никаких документированных средств для снятия этого атрибута). Напомним, что файл, отмеченный атрибутом Execute Only, можно запустить, но нельзя прочитать как обычный файл.

Было бы очень заманчиво использовать атрибут Execute Only для защиты файлов от нападения вирусов, однако мы должны отметить два момента.

Во-первых, атрибут Execute Only можно устанавливать только для программ DOS, не использующих оверлейную структуру и не выполняющих прямое чтение загрузочного файла. В то же время многие программы дописывают к концу ехе-файла данные, которые они затем читают в процессе своей работы.

Kkyuzz.1413

При стирте программы, имя которой заканчивается на LI.EXE, вирус Kkyuzz.1413 обращается к программному интерфейсу Novell Netware. Когда вводится слово "kkyuzz" с использованием буферизованного ввода (функция 0Ah прерывания Int 21h), вирус удаляет свой код из памяти.

Как следствие вы не можете защитить атрибутом Execute Only загрузочные файлы приложений и библиотек динамической компоновки операционных систем Microsoft Windows и OS/2. Эти файлы содержат специальные данные (ресурсы) которые читаются из файла при необходимости при выполнении приложений. Для доступа к ресурсам используются команды прямого чтения, которые не будут работать при установленном атрибуте Execute Only.

Используйте атрибут доступа Execute Only только вместе с атрибутом Read Only

Во-вторых, атрибут можно использовать только в паре с атрибутом Read Only, так как иначе вирус сможет “снять” атрибут Execute Only, просто уничтожив файл и записав на его место новый, но уже без атрибута Execute Only.

Вы можете спросить: как вирус запишет файл, ведь он не сможет его прочитать?

Дело в том, что вирусу не нужно читать программный файл. Во многих случаях он сможет восстановить этот файл, пользуясь, например, его образом в оперативной памяти. Когда операционная система DOS запускает файл с атрибутом Execute Only, она “читает” его в оперативную память. А там этот файл уже поджидает вирус. Сделав реконструкцию файла по образу в памяти, он может записать такой файл на место защищенного. Именно поэтому атрибуты Execute Only и Read Only необходимо использовать вместе.

Проверка паролей и прав пользователей

Периодически системный администратор должен проверять целостность защиты серверов. При этом следует выполнить анализ прав доступа на избыточность, а также проверить, для всех ли пользователей задан пароль.

Проще всего выполнить такую проверку, запустив программу SECURITY.EXE из каталога SYSTEM. Параметры указывать не нужно.

Периодически проверяйте права пользователей сети на избыточность

Программа SECURITY.EXE проверит права всех пользователей и выведет на экран рабочей станции замечания. Подробное описание этих замечаний вы найдете на стр. 258 в

3 томе библиотеки “Персональный компьютер. Шаг за шагом”. На все замечания следует обязательно отреагировать, так как их появление говорит о потенциальном снижении устойчивости системы защиты сервера Novell NetWare к преднамеренным или непреднамеренным действиям пользователя или к нападению вирусов.

Вход системы много администраторов

Как мы уже говорили, вход системного администратора в сервер сопряжен с риском заражения расположенных на этом сервере сетевых каталогов, так как использованная для входа рабочая станция может быть заражена вирусом.

По возможности следует избегать входить в сеть с именем пользователя, для которого не существует никаких ограничений для записи в сетевые каталоги. Поэтому при нормальной каждодневной работе пользователь, отвечающий за сеть, не должен подключаться к серверам как системный администратор. Для выполнения таких работ, как подключение других пользователей и управления доступом вполне достаточно привилегий администратора групп. К тому же, вы можете разрешить администратору групп читать содержимое всех сетевых каталогов, предоставив доступ на чтение к корневым каталогам сетевых томов.

Однако рано или поздно системному администратору придется подключаться к сети как супервизору. В этом случае мы рекомендуем сделать следующее.

- Проверьте рабочую станцию, которая будет использоваться для подключения, на присутствие вирусов. Для этого можно использовать, например, антивирусный комплект АО “ДиалогНаука”
- Подготовьте чистую системную дискету, с которой можно выполнить загрузку DOS. Запишите на эту дискету все файлы, необходимые для получения доступа к серверу (программы LSL.COM, IPXODI.COM, NETX.EXE и драйвер сетевого адаптера). Запишите на эту же дискету несколько антивирусных программ, например, Aidstest и Doctor Web. Используйте самые последние версии указанных программ. Вы можете также записать на эту дискету программу LOGIN.EXE
- Загрузите рабочую станцию с дискеты, подготовленной указанным выше образом, и войдите в сеть пользователем с правами системного администратора
- Выполните поиск вирусов в сетевых каталогах сервера, используя перечисленные выше антивирусные программы

Такая процедура защитит диски сервера от нападения вирусов, которое будет особенно опасным, если рабочая станция системного администратора окажется зараженной.

Сетевые антивирусные программы для Novell NetWare

Разными фирмами были созданы многочисленные антивирусные программы, специально предназначенные для работы в среде сетевой операционной системы Novell NetWare. Эти программы представляют собой NLM-модули, загружаемые оператором с консоли Novell

NetWare или через файл startup.ncf (играющий ту же самую роль, что и файл autoexec.bat в операционной системе DOS).

В чем удобство таких антивирусных программ? Мы уже говорили, что сканирование сетевых каталогов можно с успехом выполнять при помощи обычных антивирусных программ, предназначенных для отдельных компьютеров, не объединенных в сеть, и рабочих станций, например, при помощи программы Doctor Web. Однако такое сканирование приходится выполнять вручную. Кроме того, для получения доступа ко всем сетевым томам и каталогом в процессе сканирования приходится подключаться к сети с именем высокопривилегированного пользователя (что опасно само по себе).

WorkNet.708

*Резидентный вирус.
Пытается обращаться к программно му интерфейсу Novell NetWare.
Содержит строку "WORK:NET:".*

В то же время специальная сетевая антивирусная программа работает в среде сетевой операционной системы как фоновый процесс, имеющий доступ к любым сетевым ресурсам сервера, на котором она была запущена. Поэтому проверка сетевых каталогов выполняется в автоматическом режиме без вмешательства системного администратора.

Дополнительно все современные сетевые антивирусные программы, предназначенные для запуска в среде сетевой операционной системы, способны автоматически проверять файлы, которые записываются пользователями в сетевые каталоги или читаются с них. В этом случае будут пресекаться попытки пользователей записать на диски файл-сервера программы, зараженные вирусами. Если же окажется, что зараженная программа была записана на сервер раньше (до установки и запуска антивирусной программы), она будет обнаружена при попытке ее запуска или копирования на диск рабочей станции или в другой сетевой каталог.

Результаты сканирования записываются в журнал, который доступен для просмотра системному администратору или другому лицу с аналогичными правами доступа.

Как только вирус будет обнаружен, системный администратор (или другой пользователь, идентификатор которого указывается при настройке антивирусной программы) получает сообщение. Одновременно делается запись в журнале. Доступ к зараженному файлу блокируется, что предотвращает распространение вируса по сети. Дополнительно все зараженные программы могут автоматически переписываться в отдельный каталог для последующего анализа (например, для поиска источника заражения).

Эффективность обнаружения вирусов в значительной степени зависит от актуальности вирусной базы данных, входящих в состав антивирусных средств, а также от способности обнаруживать полиморфные вирусы. Простое сканирование с поиском вирусов по набору сигнатур обычно дает плохие результаты, поэтому современные

сетевые антивирусные программы используют эвристические методы обнаружения вирусов.

Постоянно обновляйте версии анти вирусных программ (не реже одного раза в неделю или в месяц). Помните, что каждый день появляется несколько новых вирусов

Среди наиболее известных антивирусных программ для Novell NetWare можно назвать следующие: Norton AntiVirus for NetWare, NetShield for NetWare, Central Point AntiVirus for NetWare, LANDesk Virus Protect, Dr. Solomon's Toolkit for NetWare, SWEEP for Novell NetWare. В самом ближайшем будущем появится антивирусная программа Doctor Web for Novell NetWare, которая войдет в антивирусный комплект АО "ДиалогНаука".

Выбор велик, хотя можно ожидать, что программа Doctor Web for Novell NetWare будет у нас более эффективна, так как ее вирусная база постоянно обновляется и значительную часть этой базы составляют "отечественные" вирусы.

Как правило, все сетевые антивирусные программы для Novell NetWare состоят из двух компонент: NLM-модуля, который запускается на сервере, и набора программ для рабочей станции, рассчитанных на использование в среде DOS или Microsoft Windows.

Для примера мы расскажем вам о двух сетевых антивирусных программах: Norton AntiVirus for NetWare и NetShield for NetWare.

На рис. 4.13 показана работа NLM-модуля программы Norton AntiVirus for NetWare версии 2.01.

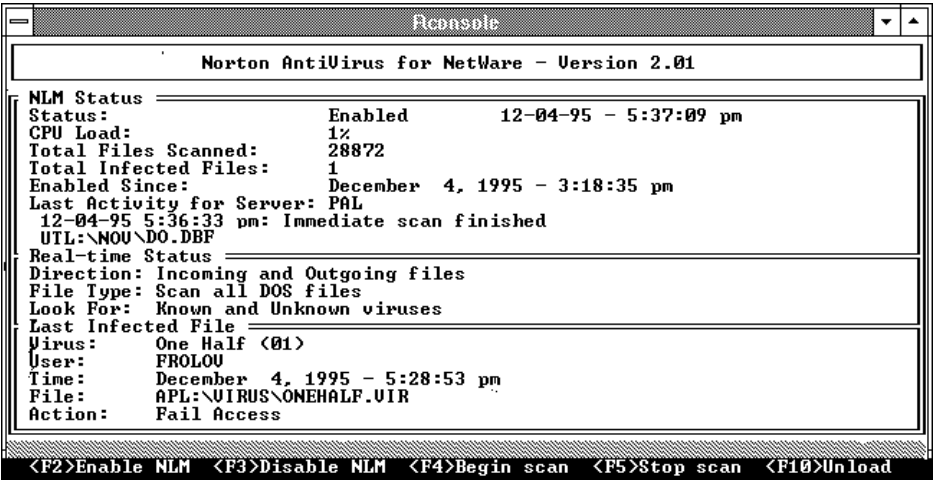


Рис. 4.13. Работа NLM-модуля программы версии 2.01

Запустив этот модуль на сервере (например, с помощью программы удаленного доступа к консоли RCONSOLE.EXE) вы можете управлять ее работой с помощью клавиш <F2>, <F3>, <F4>, <F5> и <F10>.

Клавиши <F2> и <F3> предназначены, соответственно, для разрешения и блокирования работы NLM-модуля. Нажав клавишу <F4>, можно запустить процесс сканирования, который будет выполняться в автоматическом режиме. Клавиша <F5> позволяет остановить сканирование, а клавиша <F10> - выгрузить NLM-модуль антивирусной программы из памяти.

Заметим, что для выполнения любых действий с NLM-модулем антивирусной программы Norton AntiVirus for NetWare требуется указать имя пользователя, запустившего этот модуль и пароль. Таким образом, если программа была запущена системным администратором, никто другой не сможет ее заблокировать или выгрузить из памяти, отключив таким образом антивирусную защиту файл-сервера.

Окно NLM-модуля антивирусной программы Norton AntiVirus for NetWare разделено на три части.

В области NLM Status отображается текущее состояние модуля (разблокирован или заблокирован, процент загрузки центрального процессора сервера, общее количество проверенных файлов и т. д.

В области Real-time Status отображаются текущие параметры модуля.

И, наконец, в области Last Infected File приведены сведения о последнем обнаруженном зараженном файле. Здесь вы можете увидеть название найденного вируса, идентификатор пользователя, который сделал попытку записать зараженный файл на сервер, дату этого события и путь к зараженной программе, а также действия, выполненные антивирусной программой.

Для управления NLM-модулем антивирусной программы Norton AntiVirus for NetWare системный администратор может использовать специальное приложение, предназначенное для работы в среде Microsoft Windows версии 3.1, главное окно которого показано на рис. 4.14.

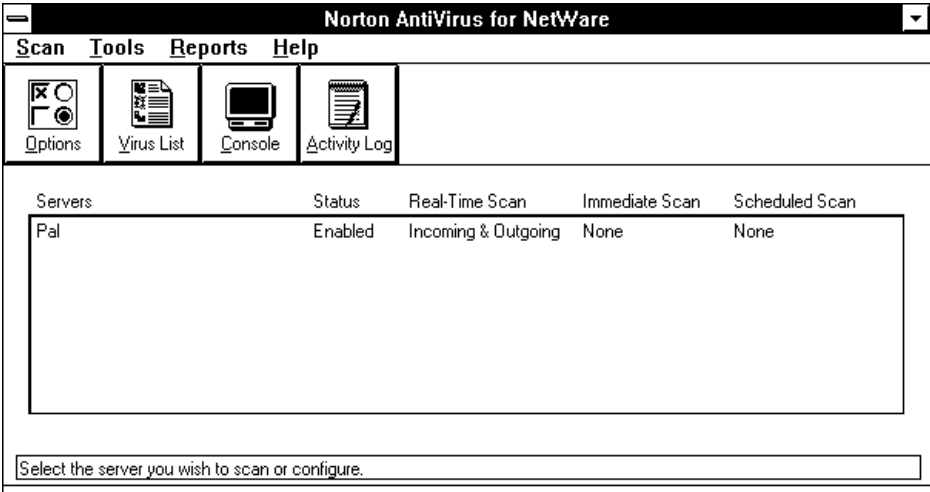


Рис. 4.14. Главное окно приложения, предназначенного для управления антивирусной программой Norton AntiVirus for NetWare версии 2.01

Доступ к самым нужным функциям приложения можно выполнять при помощи меню а также органа управления Toolbar, содержащего четыре кнопки Options, Virus List, Console и Activity Log.

Нажав кнопку Console, системный администратор может определить текущее состояние NLM-модуля антивирусной программы, не прибегая к услугам программы RCONSOLE.EXE (рис. 4.15).

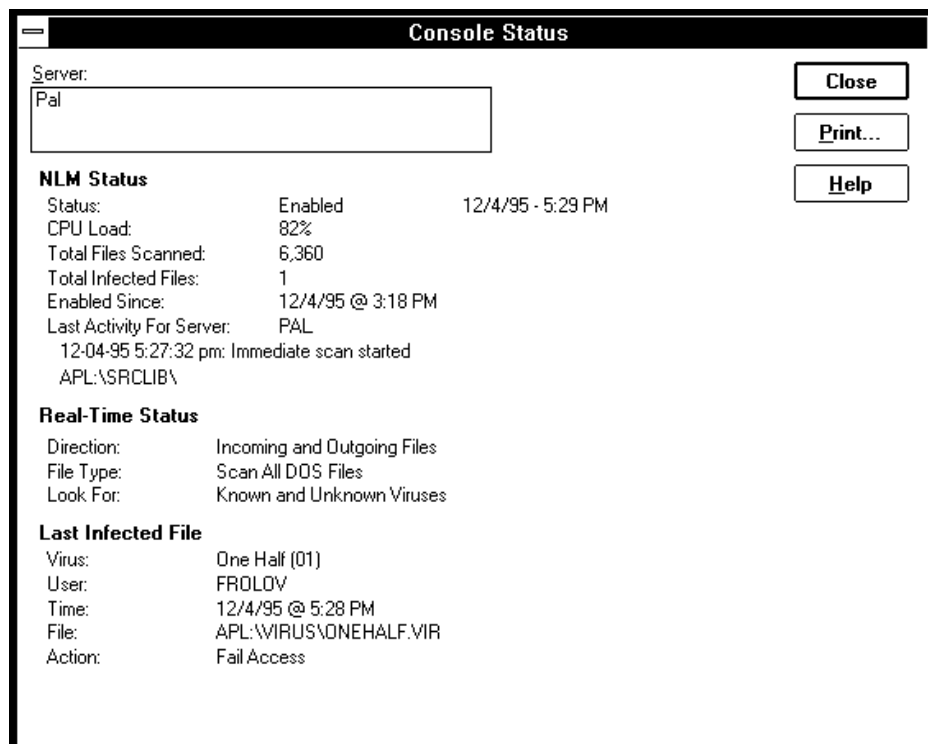


Рис. 4.15. Просмотр текущего состояния NLM-модуля антивирусной программы Norton AntiVirus for NetWare

Нажав в главном окне приложения кнопку Activity Log, можно просмотреть содержимое журнала на предмет обнаружения вирусов (рис. 4.16).

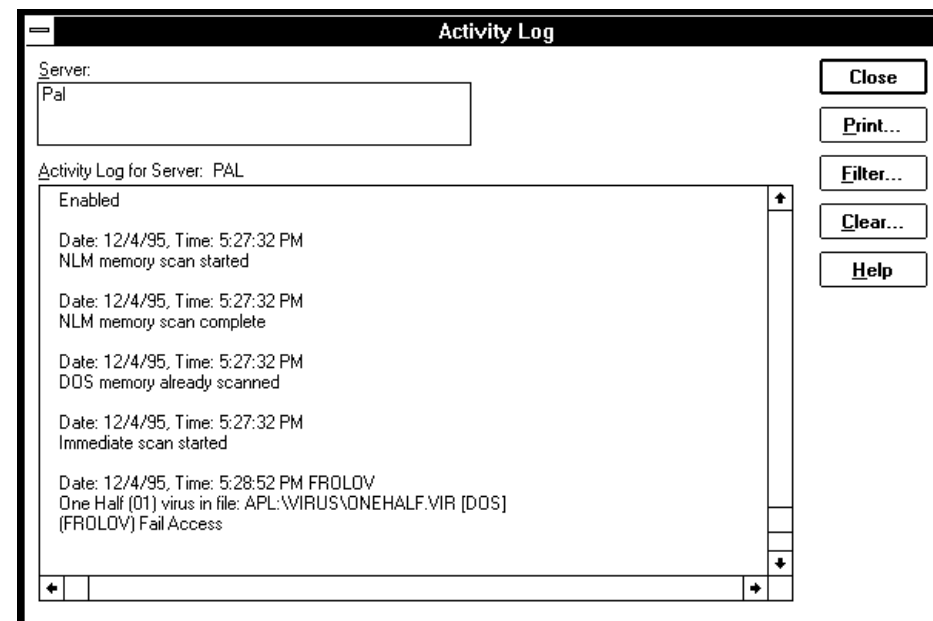


Рис. 4.16. Просмотр журнала

Управляющее приложение позволяет указать для NLM-модуля антивирусной программы Norton AntiVirus for NetWare многочисленные параметры, определяющие режимы ее работы (рис. 4.17).

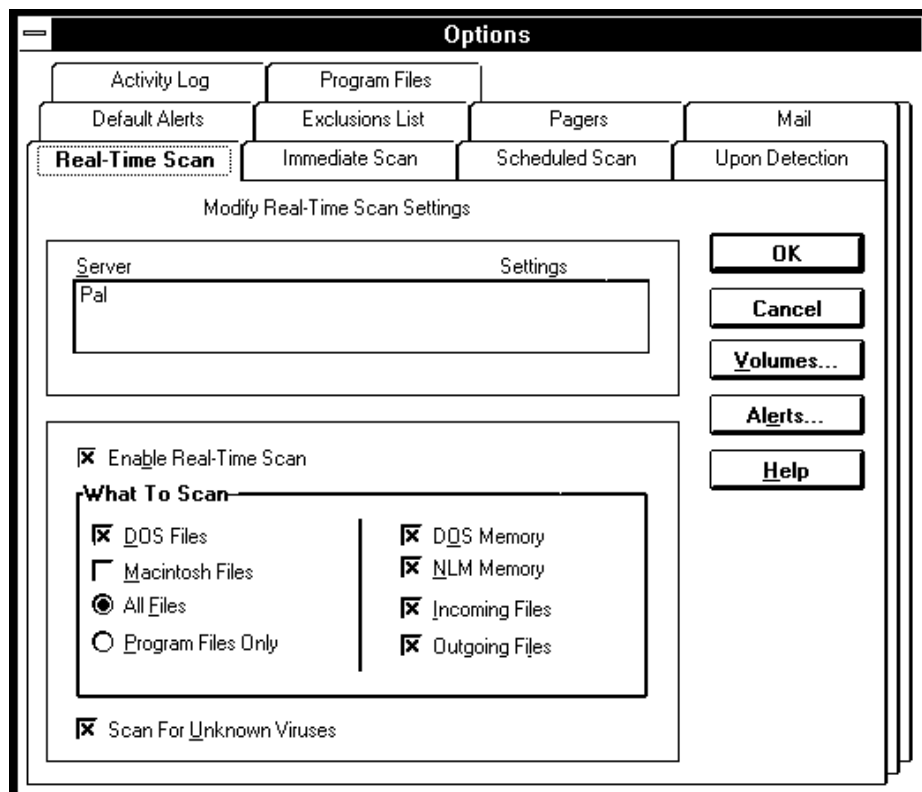


Рис. 4.17. Блокнот настройки параметров NLM-модуля антивирусной программы Norton AntiVirus for NetWare

Выбрав страницу Real-Time Scan, вы можете указать, какие файлы должны сканироваться (файлы программ DOS, программные файлы или все файлы, файлы, которые пользователи записывают в сетевые каталоги или переписывают на диски рабочих станций из сетевых каталогов и т. д.). Дополнительно можно сканировать на предмет наличия вирусов память сервера, в которую загружаются NLM-модули, а также память, выделенную операционной системе DOS.

NetBIOS-4340

Резидентный вирус.

Заражает программы с расширением имени COM и EXE.

При определенных обстоятельствах пытается разместиться в памяти дополнительного резидентного модуля, который должен что-то делать в локальной сети с использованием программного интерфейса NetBIOS.

Содержит довольно много ошибок. После 1 августа стирает я вылечить все зараженные файлы.

Страница Default Alerts позволяет указать, кому должно направляться извещение при обнаружении вируса (рис. 4.18).

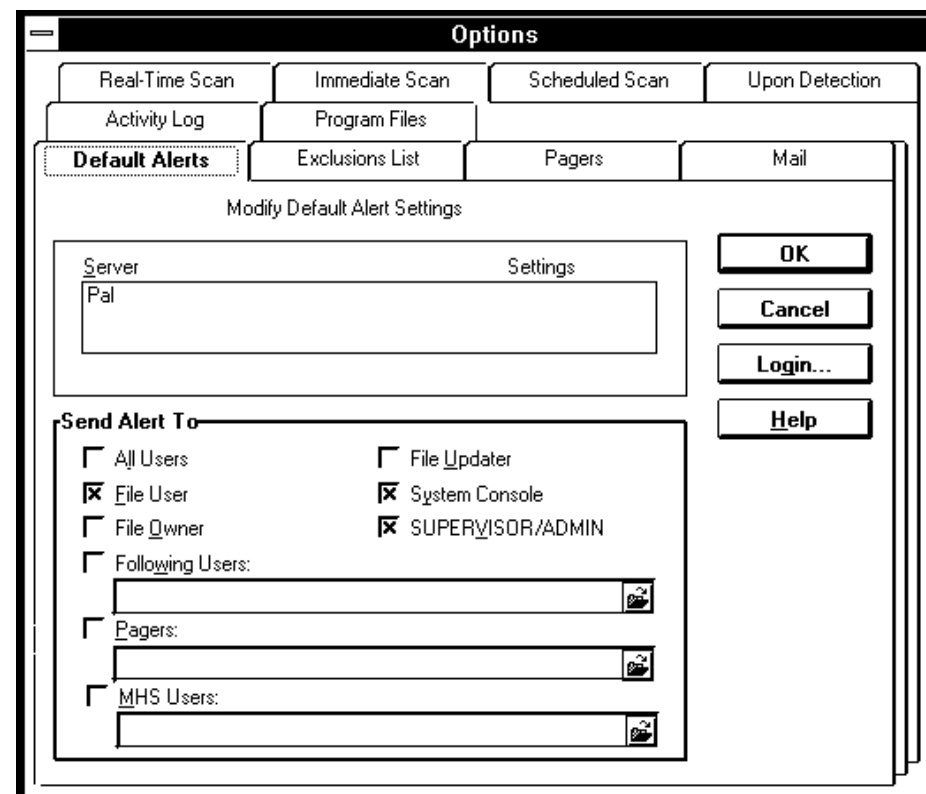


Рис. 4.18. Выбор действий при обнаружении вируса

Такое извещение может быть направлено всем или только некоторым пользователям, владельцу файла, пользователю, выполняющему обновление файла или системному администратору. Сообщение о том, что в сетевых каталогах обнаружен вирус, может быть выведено на системную консоль сервера Novell NetWare, отправлено по почте MHS или даже передано на пейджер.

Кнопка Virus List в главном окне управляющей программы Norton AntiVirus for NetWare предоставляет доступ к базе данных, содержащей описания вирусов и, что очень важно, рекомендуемые действия при обнаружении вирусов (рис. 4.19).

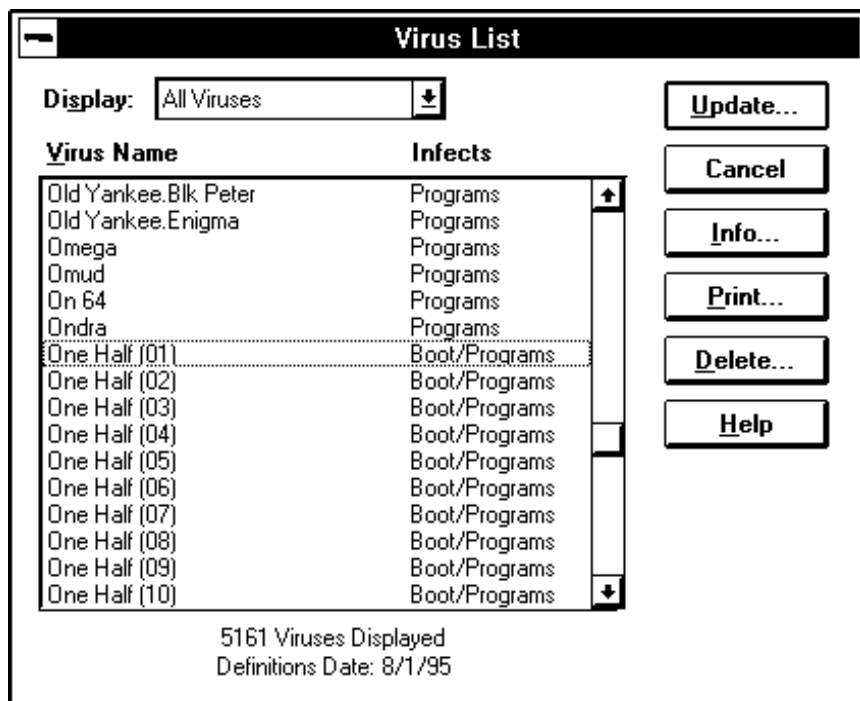


Рис. 4.19. База данных с информацией о вирусах

Для получения подробной информации о каком-либо вирусе вы должны найти его имя в этом списке и нажать кнопку Info. При этом на экране появится диалоговая панель Virus Information, показанная на рис. 4.20.

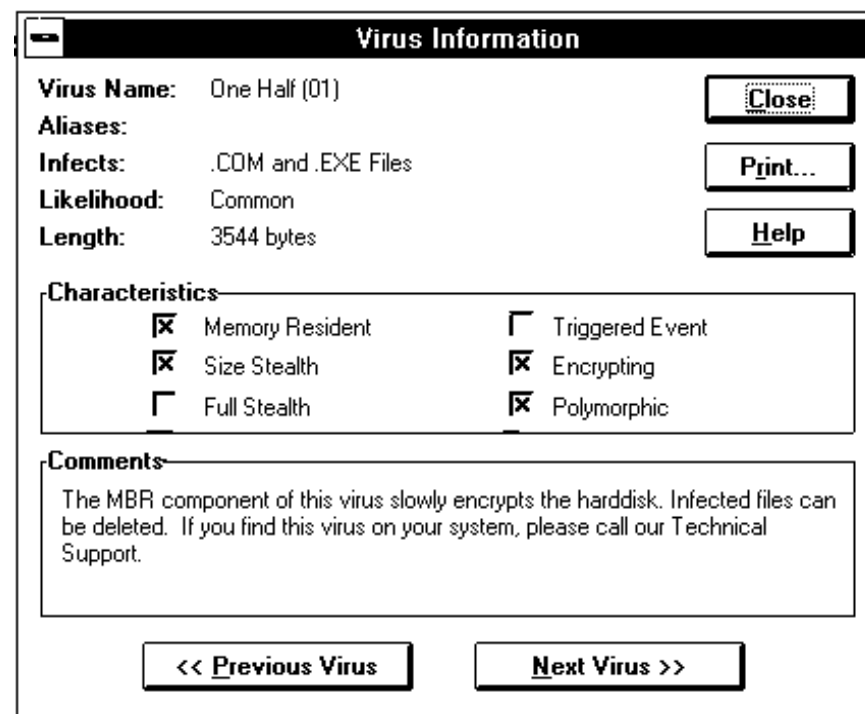


Рис. 4.20. Диалоговая панель Virus Information, содержащая описание вируса и рекомендуемые при его обнаружении действия

С помощью группы переключателей Characteristics вы можете узнать, является ли данный вирус резидентным вирусом, стелс-вирусом, использует ли он технологию шифрования и полиморфизм, способен ли он выполнять вредоносные действия при наступлении какого-либо события.

В поле Comments находятся более подробная информация и дополнительные рекомендации. Заметим, что антивирусная программа Norton AntiVirus for NetWare не может вылечить опасный полиморфный вирус One Half (в отличие от программы Doctor Web, входящей в комплект антивирусных средств АО “ДиалогНаука”). Если вы обнаружили такой вирус, вам рекомендуется обратиться в группу технического сопровождения.

Если вы сомневаетесь в успехе лечения, обращайтесь в “Компьютерную скорую помощь”® АО “ДиалогНаука”. В результате неправильного лечения могут быть потеряны важные данные и программы.

Антивирусная программа (рис. 4.21) также имеет в своем составе NLM-модуль, запускаемый в среде сетевой операционной системы Novell NetWare.

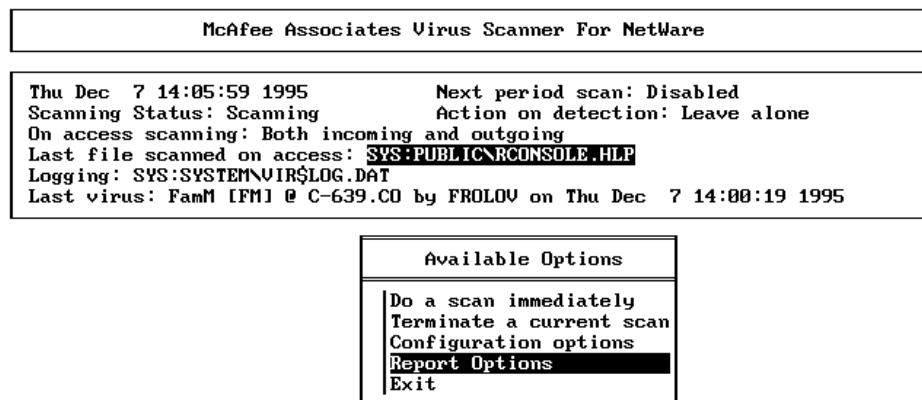


Рис. 4.21. Главное окно антивирусной программы McAfee Virus Scanner for NetWare

По своим возможностям эта программа аналогична предыдущей. Ее интерфейс, выполненный в стиле утилит Novell NetWare, привычен и удобен для системных администраторов. С помощью системы вложенных меню можно управлять работой антивирусной программы как непосредственно с консоли файл-сервера, так и с рабочей станции (через программу RCONSOLE.EXE).

На рис. 4.22 показано меню Configuration, с помощью которого вы можете выполнить настройку режимов работы программы McAfee Virus Scanner for NetWare.

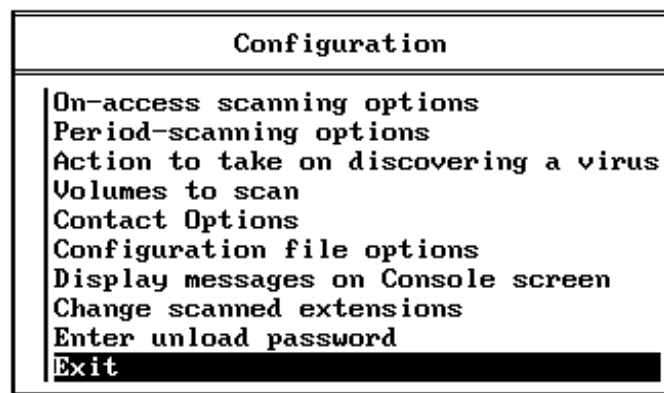


Рис. 4.22. Меню настройки режимов работы антивирусной программы McAfee Virus Scanner for NetWare

С помощью строк On-access scanning options и Period-scanning options помимо всего прочего вы можете заставить антивирусную программу проверять файлы, которые пользователи записывают на диски сервера или переписывают из сетевых каталогов на диски своих рабочих станций (рис. 4.23).

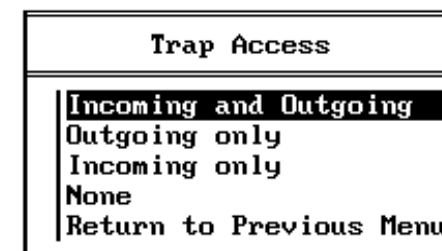


Рис. 4.23. Можно использовать автоматическое сканирование файлов, попадающих на диски файл-сервера или чужих пользователей из сетевых каталогов

Выбрав строку Action when virus found, вы сможете определить действия, которые должна выполнить антивирусная программа при обнаружении вируса (рис. 4.24).

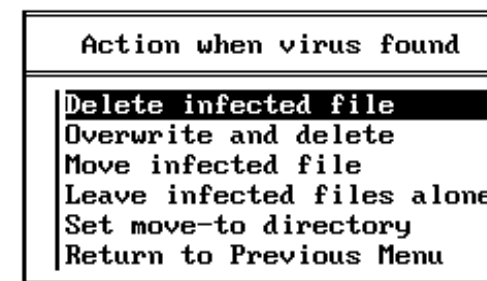


Рис. 4.24. Выбор действий при обнаружении вируса

Зараженный файл может быть удален, перемещен в другой сетевой каталог (недоступный пользователям), или оставлен на месте нетронутым.

С помощью меню Whom to contact (рис. 4.25), которое появляется на экране при выборе строки Contact Options, можно указать список пользователей, которым посылается сообщение о том, что на сервере был обнаружен вирус.

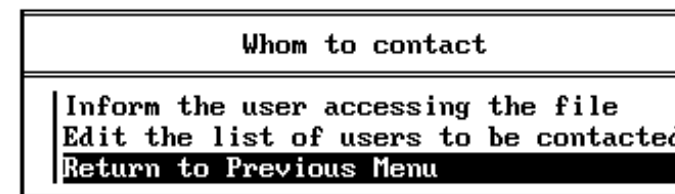


Рис. 4.25. Меню Whom to contact

С помощью строки можно задать список расширений файлов, подвергаемых сканированию (рис. 4.26).

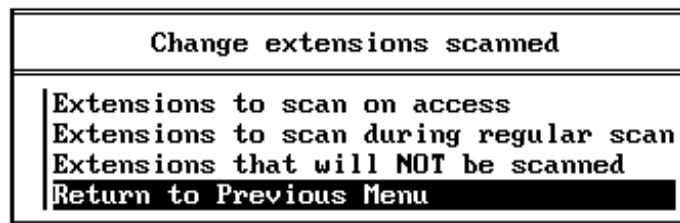


Рис. 4.26. Меню Change extensions scanned, которое появляется при выборе одной из строк из главного меню программы

Меню Report Option позволяет управлять процессом протоколирования результата сканирования (рис. 4.27).

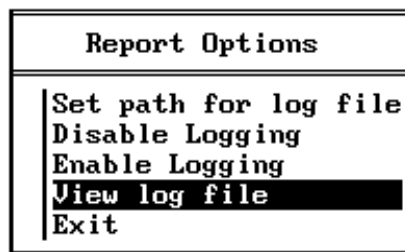
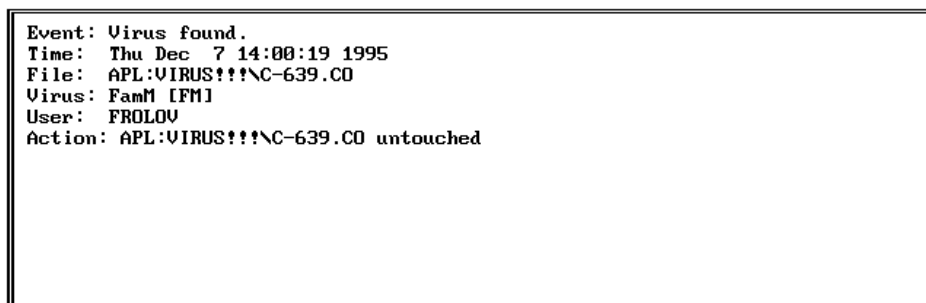


Рис. 4.27. Меню Report Option

Выбрав из этого меню строку View log file вы сможете просмотреть файл протокола сканирования на экране (рис. 4.28).



PgUp moves up PgDn moves down End last entry HOME first entry ESC exits

Рис. 4.28. Просмотр протокола сканирования сетевых каталогов

Защита сети на базе сервера IBM LAN Server для OS/2

Методика защиты сети, созданной на базе серверов IBM LAN Server во многом аналогична методике защиты сети Novell NetWare. Если вы - системный администратор такой сети, вам прежде всего необходимо правильно распределить права доступа. Кроме

того, вы можете использовать для защиты сервера специально разработанные программные и аппаратные антивирусные средства.

В отличие от сети Novell NetWare, все сетевое программное обеспечение, необходимое для доступа к файлу-серверу IBM LAN Server, хранится на рабочих станциях. Рабочие станции DOS и Windows нужно защищать от вирусов точно также, как и отдельные компьютеры, не подключенные к сети. Более подробно об установке, настройке и использовании сервера IBM LAN Server 4.0 Advanced вы можете прочитать в 20 томе нашей серии книг "Библиотека системного программиста", которая называется "Операционная система IBM OS/2 Warp".

ComeOut-3624

Резидентный вирус.

Заражает только программы с расширением имени EXE.

"Нападает" прежде всего на файлы, расположенные в текущем каталоге. Резидентный модуль остается в памяти видеоконтроллера EGA или VGA (но не CGA). Не активизируется, если в корневом каталоге диска C: имеется файл с именем COME.OUT.

Содержит заготовки для дальнейшего развития и глобальные идеи по взлому локальной сети. Сочетание глубины идей и не очень высокого класса программирования приводит к быстрому "повисанию" системы.

Системный администратор перед подключением к сети должен тщательно проверить свою рабочую станцию, убедившись в отсутствии вирусов.

Административные меры защиты

Системный администратор сети на базе сервера IBM LAN Server может создавать группы пользователей, так же как и администратор сети Novell NetWare. Однако способ присваивания прав доступа отличается от использованного в Novell NetWare. В сети Novell NetWare права доступа назначаются пользователям и группам пользователей с помощью программы SYSCON.EXE. Что же касается сервера IBM LAN Server, то права доступа определяются с помощью блокнота свойств сетевого ресурса, который отображается на экране в ответ на щелчок правой клавишей мыши по соответствующей пиктограмме.

Для определения списка пользователей и групп пользователей, имеющих права доступа к ресурсу, а также для определения самих этих прав необходимо выбрать страницу "Permissions" (рис. 4.29).

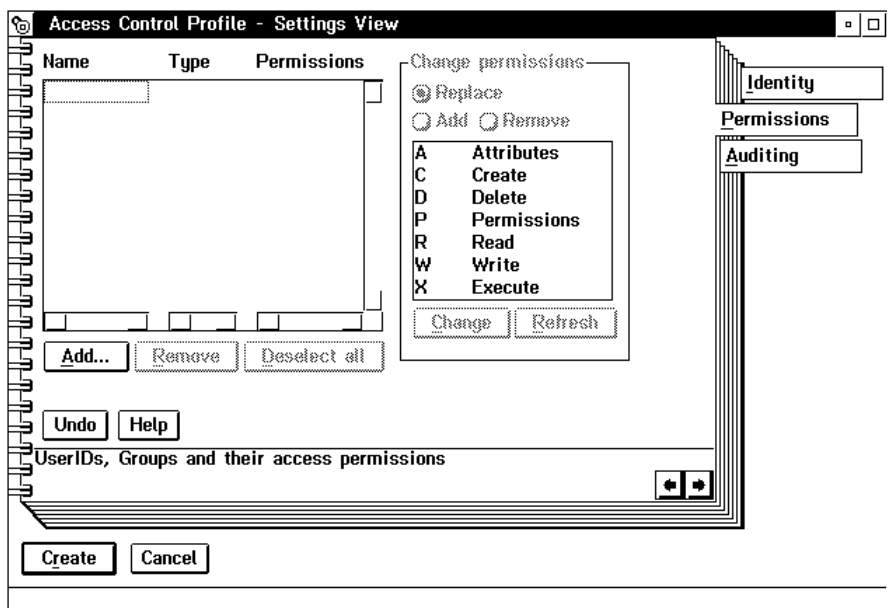


Рис. 4.29. Страница “Permissions”, позволяющая определить права доступ к ресурсу для групп пользователей и отдельных пользователей

Вы можете указать следующие права доступа:

Права доступа	Описание
Attributes	Изменение атрибутов файлов
Create	Создание файлов и каталогов
Delete	Удаление файлов и каталогов
Permissions	Изменение прав доступа
Read	Чтение
Write	Запись
Execute	Запуск программ на выполнение

Для предотвращения заражения программных файлов вирусами вы можете указать права доступа Read и Execute для обычных пользователей. По возможности никогда не предоставляйте пользователям права доступа Write, Delete, Attributes, Permissions и Create к каталогам, содержащим программные файлы.

Не используйте для программных файлов комбинацию прав доступа Execute, Write и Delete. Если вам нужно защитить файл от вирусов, укажите для него только одно право доступа - Execute

Если вы указываете для программного файла права доступа Execute, надеясь защитить его таким образом от вирусной атаки, проследите за тем, чтобы для этого файла не были указаны права доступа Write и Delete. В противном случае вирус может удалить такой файл, создав на его месте новый, для которого разрешено выполнение операции записи. Мы уже рассказывали об этой возможности при описании атрибута Execute Only, который используется в операционной системе Novell NetWare.

Антивирусные программы для защиты сети на базе IBM LAN Server

Программная защита серверов сети на базе IBM LAN Server для OS/2 может выполняться с использованием тех же средств, что и защита рабочих станций OS/2. Прежде всего это такая антивирусная программа, как IBM AntiVirus for OS/2, обладающая способностью выполнять сканирование сетевых дисков и каталогов в фоновом режиме.

Существуют и другие антивирусные программы, способные работать в среде OS/2. Это Armour/FireBreak, Dr. Solomon's AntiVirus Toolkit, LanDesk Virus Protect и т. д.

Заметим, что пока не наблюдается широкого потока вирусов, специально ориентированных на операционную систему OS/2, однако такие вирусы могут быть созданы. К тому же, в среде виртуальной машины DOS, работающей под управлением OS/2, могут распространяться и обычные вирусы, ориентированные на операционную систему DOS.

5 РАБОТА С BBS АО “ДИАЛОГНАУКА”

На протяжении всей книги мы настойчиво повторяем, что для увеличения эффективности борьбы с вирусами необходимо постоянно обновлять версии антивирусных программ. Для облегчения этой задачи многие фирмы, занимающиеся разработкой антивирусных средств, предоставляют своим подписчикам возможность получения новых версий программ через электронные доски объявлений BBS, FTP-серверы, предназначенные в основном для файлового обмена, или страницы глобальной гипертекстовой системы WWW. В этом случае вам не нужно каждый раз приезжать в представительство фирмы или пользоваться услугами курьера, так как вы сможете загружать новые версии антивирусных программ через модем.

Модем представляет собой устройство, которое может быть конструктивно выполнено в виде платы расширения, вставляемой в корпус компьютера, либо в виде отдельного устройства, которое подключается кабелем к последовательному порту компьютера. В первом случае модем является внутренним, во втором - внешним.

Как внутренний, так и внешний модем подключается к телефонной линии, для чего на его корпусе имеется стандартный телефонный разъем. Исчерпывающие сведения о выборе и подключении модема вы найдете в 16 томе нашей серии книг “Библиотека системного программиста”, которая называется “Модемы и факс-модемы”.

Одной из основных характеристик модема является скорость передачи данных. Так как размеры файлов антивирусных программ может достигать сотен Кбайт, при использовании низкоскоростных модемов время загрузки новой версии программы может оказаться значительным.

Если вы можете позволить себе потратить на приобретение модема 200-300 долларов США, мы можем порекомендовать модемы фирмы USRobotics (модели Sportster или Courier со скоростью передачи данных не менее 14400 bps), или модемы ZyXEL, которые также обладают неплохими характеристиками.

Для работы с модемом используется специальное программное обеспечение, которое, как правило, продается вместе с модемом. Однако в составе таких операционных систем, как Microsoft Windows версии 3.1, Microsoft Windows 95, IBM OS/2 Warp версии 3.0 имеются достаточно удобные встроенные средства.

Для работы с электронными досками объявлений BBS (в том числе для работы с электронной доской объявлений АО “ДиалогНаука”) вам потребуется простейшая терминальная программа. Вы можете использовать терминальные программы, разработанные для операционной системы DOS, такие как MTE, Telix, Comit или Bitcom, терминальное приложение Terminal, предназначенное для работы в среде Microsoft Windows версии 3.1, приложение HyperTerminal фирмы Hilgraeve Inc., которое поставляется вместе с операционной системой Microsoft Windows 95 и IBM OS/2 и т. д. Выбор достаточно велик.

Электронная доска объявлений BBS АО “ДиалогНаука” открывает вам доступ к самым последним версиям наиболее популярных антивирусных программ

На чем же остановиться?

Если у вас старый модем со скоростью передачи данных 2400 bps, который не способен выполнять аппаратную коррекцию ошибок по протоколу MNP (о чем вы можете узнать из документации к модему), лучшим выбором будет терминальная программа MTE, созданная фирмой Magic Soft.

Если же вы владеете современным высокоскоростным модемом, лучше всего работать с приложением HyperTerminal или использовать средства, которые поставляются вместе с модемом, например, QuickLink II FAX (поставляется вместе с модемом USRobotics Sportster 33600).

Выбирая терминальную программу, убедитесь, что она способна передавать данные с использованием протокола ZMODEM. На сегодняшний день это наиболее удобный и устойчивый протокол, способный динамически адаптироваться к качеству телефонной

линии, изменяя размер блока передаваемых данных. Все современные терминальные программы работают с протоколом ZMODEM.

Сеанс связи с BBS АО “ДиалогНаука”

Запустите терминальную программу и позвоните с ее помощью по телефону (095)938-28-56 (это телефон линии общего доступа BBS “ДиалогНаука”). Если вам повезло и линия оказалась свободной, через некоторое время вы увидите на экране следующее приглашение:

Address 2:5020/69@fidonet Using BinkleyTerm-OS/2 2.50 EE Beta
E3-32 ISDN

DialogueScience BBS, Line 2

Press <ESC> once for Maximus

Линия общего доступа используется достаточно интенсивно, поэтому с первого раза вы скорее всего обнаружите, что она занята. Для подписчиков на антивирусный комплект АО “ДиалогНаука” имеются еще несколько линий (соответствующие этим линиям номера телефонов есть в документации, которая поставляется вместе с антивирусным комплектом, а также в заставке BBS, приведенной ниже).

Подписчики АО “ДиалогНаука” могут пользоваться привилегированными линиями доступа

Нажмите один раз клавишу <Esc>. На экране появится строка:

Thank you. Please wait...

Через некоторое время вы увидите заставку BBS (рис. 5.1).

Next system event will happen in 1440 minutes
Host modem connect string was CONNECT 26400/V34/V42Bis

MAXIMUS/2 v3.00
DialogueScience BBS, 40 Uavilova str., Moscow, Russia, FIDO 2:5020/69

USR Courier U34/DS Line 0 : +7-095-938-2969 : 24 hrs <limited access>
USR Sportster U34/DS Line 1 : +7-095-938-2856 : 24 hrs
USR Courier U34/DS Line 2 : +7-095-939-3705 : 24 hrs <limited access>
ZyXEL U-1496E Plus Line 3 : +7-095-939-5239 : 24 hrs <limited access>
USR Courier U34/DS Line 4 : +7-095-938-2867 : 24 hrs <limited access>
USR Courier U34/DS Line 5 : - Mail only - : 24 hrs

Voice phone: +7-095-137-0150 : 19:00 - 23:00 <MSK>

SysOp: Boris Chernivetsky e-mail: bob@dials.msk.su

Please use REAL names! First name, last name. Uncorrect names will be deleted from user's records without any comments.

Пожалуйста используйте реальные имена (Ваше личное имя и фамилию, а не название фирмы), латинскими буквами. Если Вы не выполните эти требования, Ваше имя будет удалено из списка пользователей без комментариев.

What is your name: _

Рис. 5.1. Заставка электронной доски объявлений BBS АО “ДиалогНаука”

В ответ на запрос What is your name вы должны ввести свое имя. После этого вам будет предложено ввести фамилию (What is your LAST name). Если вы работаете с этой BBS в первый раз, можно выбрать любое имя. В следующий раз при подключении вы будете указывать выбранные вами при первом подключении имя и фамилию. Имеет смысл использовать только настоящие имена, о чем предупреждается в заставке BBS.

Если вы не зарегистрированы, то на экран будет выведено следующее сообщение:

Your name was not found in my user records. If you are indeed a new user, then answer `Y' to the following prompt, and proceed to log on.

Otherwise, type `N' and enter your name correctly.

NOTE! Please make sure that your name, as shown below, is capitalized correctly! Maximus will try to properly capitalize names, if possible, but you must manually enter the correct version of names such as "McDonald". This is only necessary on your first logon; subsequent logons will use the capitalization which you specify here.

Please, DON'T USE digits and russian letters in your name;

DON'T USE name of company you works for registration;

DON'T USE name as `Mike Mike' or `V. Ivanov';

DON'T USE aliases.

Alexandr Frolov [Y,n]?

В этом сообщении говорится, что ваше имя не найдено в списке пользователей BBS. Возможно, вы ошиблись при вводе имени. Поэтому вам предоставляется возможность еще раз проверить введенное имя.

В имени нельзя использовать цифры и русские буквы. Не следует также указывать название фирмы, сокращения и псевдонимы.

Далее новый пользователь должен выбрать язык, на котором он будет общаться с BBS (английский или русский):

Select a language:

1) ENGLISH

2) RUSSIAN

Select:

В наших примерах мы будем пользоваться английским языком. Если вы собираетесь поступить так же, в ответ на приглашение Select введите число 1. Вы увидите сообщение о том, что выбран английский язык:

English language (proper) selected.

Press ENTER to continue

Для продолжения работы нажмите клавишу <Enter>. Вам будет предложено зарегистрироваться:

Welcome to DialogueScience BBS!

Since you are a new user, you will be asked to enter your city and province, your password, and to select several configuration options. Keep in mind that these choices are not permanent; you can modify all of these settings from the C)hange menu after you've registered as a new user.

Your SysOp,

Boris Chernivetsky

Please enter your city and state/province: Moscow, Ruusia

Please enter your phone number [(xxx) yyy-zzzz]: (095) XXX-XXXX

Вы должны ввести название города и свой телефонный номер.

Затем система попросит вас выбрать пароль:

Now, you must choose your password.

A password is one word (with no spaces). Passwords can be anywhere from 4 to 15 characters long, and can include letters or numbers.

Uppercase and lowercase letters are treated identically.

Tips:

1) Write down your password somewhere (or store it in your terminal program's dialing directory), so you'll remember it for next time.

2) Don't use the same password on more than one system. Since the SysOp of each system you call has access to your password, there's nothing from stopping them from logging in as you or someone else's system.

3) For better security, use a long password (at least 6 characters).

Please enter the password you wish to use:

Вы можете выбрать любой пароль длиной от 4 до 15 символов, однако не следует выбирать слишком короткий пароль, а также использовать вместо пароля свое имя, фамилию или год рождения. Лучше всего, если пароль будет содержать смесь букв и цифр. Пароль лучше запомнить и нигде не записывать.

После ввода пароля система попросит вас ввести пароль еще раз для проверки:

Please re-enter your password for verification:

Затем вы должны ответить, способна ли ваша терминальная программа работать с ANSI-символами. Эти символы используются для раскрашивания изображения на экране терминала в различные цвета.

Посмотрите внимательно на следующее сообщение, которое появится на экране:

Maximus can optionally send "ANSI codes" to your terminal program. If your terminal does support ANSI, then you'll be able to use colour in the menu prompts, cursor movement, and other niceties. However, your terminal program must have support for these codes, or else you'll only see a lot of garbage.

If your terminal program has a terminal emulation mode of either "ANSI" or "VT-100", then you should switch to it now.

Here's what ANSI codes look like:

AAAAA BBBB CCCCC

If you can see a bunch of numbers and square brackets, then your terminal program does NOT support ANSI graphics, and you should answer "N" at the prompt

If there were three blocks of letters, with no intervening numbers, then your terminal program DOES support ANSI, and you should answer "Y" at the prompt.

To turn *on* ANSI codes, enter..... Y

To turn *off* ANSI codes, enter..... N

Does your system support ANSI screen colors [y,n]?

Если строка AAAAA BBBB CCCCC изображена разными цветами, можете считать, что ваша терминальная программа работает с управляющими символами ANSI. В этом случае вы можете ответить на приведенный выше запрос утвердительно, нажав клавишу <Y>. В противном случае (если вы видите последовательность символов “[->34...”) нажимайте клавишу <N>.

После этого вы увидите следующее приглашение:

Welcome to DialogueScience BBS, Alexandr Froloff!

DialogueScience BBS

We design, distribute, and support the anti-virus programs Aidstest by Dmitry Lozinsky, Doctor Web by Igor Daniloff, ADinf (Advanced Diskinfoscope) by Dmitry Mostovoy, and ADinf Cure Module by Vitaly Ladygin and Denis Zujev (see Area I.2 for terms and conditions of distribution).

To access the lines 938-2969, 939-3705, 939-5239, 938-2867 please inform your registration number and other subscriber details to our system operator.

Press ENTER to continue

Затем проверяется почта. Если вы впервые работаете с BBS АО “ДиалогНаука”, почты для вас скорее всего нет, о чем вы можете узнать из следующего сообщения:

Sorry, but you have no mail waiting.

Press ENTER to continue

Если вы впервые работаете с этой BBS и вас пока нет в списке пользователей, но пытаетесь позвонить по линиям, выделенным специально для подписчиков, вы получите следующее сообщение:

Please, excuse us. You cannot access this line as it is

exclusively reserved for our subscribers and partners.

In the course of next five minutes you can leave your message with

SysOp (system operator), if you have any complaints about the line.

If you are our BBS subscriber, please inform:

- 1) Your organization or your name (for individual users),
- 2) Subscriber number or date, and subscription sum paid.

After checking up these data, SysOp will either open the line

to you, or return a refusal message.

To access the public BBS, please call: 938-2856, Fido 2:5020/69.1

Press ENTER to continue

В этом сообщении говорится, что если вы являетесь подписчиком, то вам нужно оставить сообщение системному оператору BBS, в котором следует указать название вашей фирмы или фамилию (для индивидуальных пользователей), номер или дату, когда была сделана подписка, сумму, указанную в платежном поручении. Только после этого вам будет предоставлен доступ к привилегированным линиям доступа для получения последних версий антивирусных программ АО “ДиалогНаука”.

Если вы желаете оставить сообщение системному оператору, ответьте утвердительно на следующий вопрос:

Would you like to leave a message for us [y,N]?

Вслед за этим вам будет предоставлена возможность ввести и отредактировать сообщение. Сообщение нужно обязательно сохранить. Для этого в ответ на только что приведенный вопрос необходимо нажать клавишу <Y>.

Если же вы откажетесь от отправки сообщения, на экране появится девиз дня (эта фраза изменяется каждый день):

Quote for the day:

Whenever I feel like exercise, I lie down until the feeling passes.

Bye, Alexandr. Please call again!

Вслед за этим модем BBS повесит трубку и сеанс связи будет окончен.
В следующий раз, когда вы вновь позвоните на BBS АО “ДиалогНаука, система “узнает” вас и встретит следующим сообщением:

Thank you for calling DialogueScience BBS, Alexandr.

You are the 6261st caller, and this is your 6th call.

You have uploaded 0K. You have downloaded 2395K. (UL:DL=0:2395.)

Press ENTER to continue

Среди всего прочего в этом сообщении подводится баланс объемов данных, полученных вами из BBS и записанных в BBS. На некоторых BBS это соотношение определяет уровень и права пользователя, однако в случае BBS АО “ДиалогНаука” оно не играет никакой роли. Вам всегда выделяется 35 минут на один сеанс, но не более 60 минут в сутки.

После ввода имени и пароля у вас запрашивается подтверждение (имя и фамилия, разумеется, будут другие):

Alexandr Frolov [Y,n]?

Если вы все ввели правильно, нажмите клавишу <Y>, а если ошиблись - клавишу <N>. В последнем случае вам будет предоставлена возможность ввести имя и фамилию повторно.

После ввода имени и фамилии у вас запрашивается пароль:

Password:

В процессе ввода символы пароля заменяются точками.
Далее выполняется поиск почты:

Searching: L1

Searching: L2

Searching: L3

Sorry, but you have no mail waiting.

Press ENTER to continue

Затем вам предлагается выбрать область файлов, из которой вы будете загружать данные:

File area [Area, "["=Prior, "]"=Next, "?"=List]:

Для того чтобы просмотреть список доступных вам областей, введите символ “?”. На экране появится следующее меню (количество и состав строк может быть другим):

File Areas

I	... Information
A	... Antiviruses
Comm	... Communications
UL	... Unchecked Users Upload
NV	... New Viruses

File area [Area, "["=Prior, "]"=Next, "?"=List]:

Для того чтобы выбрать область, введите ее обозначение, расположенное слева, и нажмите клавишу <Enter>.

В следующем разделе мы расскажем о содержимом перечисленных в этом меню файловых областей.

Файловые области BBS АО “ДиалогНаука”

Содержимое файловых областей постоянно меняется, однако их назначение остается тем же самым. Посещая BBS, вы можете посмотреть список расположенных там файлов. Для того чтобы вам было легче ориентироваться и не тратить зря время (которое при работе с BBS всегда ограничено), мы расскажем о том, что вы можете найти в самых важных файловых областях.

Область I

Область I содержит различные информационные файлы, которые могут помочь вам в работе с BBS. Эта область делится на три области. При выборе области I на экране появится следующее меню:

File Areas

I.1	... Information: General
I.2	... Information: DialogueScience
I.3	... Information: Demo Versions

For more areas, type ".." to go up one level or "/" for top level areas.

File area [Area, "["=Prior, "]"=Next, "?"=List]:

Для выбора области достаточно ввести только младшее имя (в данном случае 1, 2 или 3).

В области I.1 находятся наиболее важные файлы:

JVDS.ZIP 131295 03-12-95* 000 JV DS BBS File list

-

CHAINIK.ZIP 34117 26-03-92 000 Для начинающих:

FIDO, BBS, модемы...

CHAINIKW.ZIP 39291 22-12-93 000 CHAINIK.TXT in WinWord format

FIDOFAQ.ZIP 29342 16-02-95 000 FidoNet FAQ

Файл JVDS.ZIP содержит полный список файлов, расположенных на BBS АО “ДиалогНаука”. Во время первого сеанса связи имеет смысл загрузить этот файл, так как в нем перечислены файлы, расположенные во всех файловых областях. Для каждого файла в списке приводится его длина в байтах и краткое однострочное описание.

Просмотрев полный список файлов, вы можете выбрать интересные для вас. Так как сеанс связи с BBS ограничен по времени, лучше сначала получить файл JVDS.ZIP и отключиться от BBS. Затем следует найти нужные вам файлы, просмотрев содержимое файла JVDS.TXT (который находится в архиве JVDS.ZIP), и позвонить на BBS еще раз. Поиск файлов в режиме On-Line отнимает слишком много времени.

Не следует просматривать содержимое файловых областей во время сеанса с BBS, так как время сеанса ограничено. Лучше предварительно загрузить список файлов, которые есть на BBS, и выбрать из него нужные вам файлы. Этот список, который находится в файле JVDS.ZIP, содержит полный список файлов, расположенных на BBS, но вы, возможно, не будете иметь доступ во все перечисленные в нем области

Начинающие найдут для себя много интересного в файле CHAINIK.ZIP или CHAINIKW.ZIP. Эти файлы содержат базовые сведения о работе с модемами и BBS. Файл CHAINIK.ZIP содержит текстовый файл, который вы можете просмотреть в среде MS-DOS, файл CHAINIKW.ZIP содержит файл, предназначенный для просмотра в среде Microsoft Windows.

В файловой области I.2 находится рекламная информация о деятельности АО “ДиалогНаука”, образцы договоров, сведения о “Компьютерной скорой помощи”, руководство по антивирусному комплекту АО “ДиалогНаука”, а также фотографии известных авторов антивирусных программ, составляющих этот комплект.

В области I.3 вы найдете программу, демонстрирующую работу операционной системы Microsoft Windows 95.

Область А

Если вы подписчик, то область А для вас самая важная, потому что в ней вы найдете самые последние коммерческие версии антивирусных программ, входящие в комплект АО “ДиалогНаука”. Для остальных будут интересны некоммерческие версии антивирусных средств, распространяемых в соответствии с принципом SHAREWARE.

Область А имеет внутреннее иерархическое деление:

File Areas

A.G ... Antiviruses: General
A.MC ... Antiviruses: McAfee

A.X ... Antiviruses: Dr.Web virus base add-on
A.AI ... Aidstest (V-Hunter), commercial
A.AW ... Dr.Web, commercial
A.AD ... ADinf, commercial
A.AE ... ADinfExt, commercial

For more areas, type ".." to go up one level or "/" for top level areas.

File area [Area, "["=Prior, "]"=Next, "?"=List]:

Область A.G содержит некоммерческие версии антивирусных программ ADinf, Doctor Web и Aidstest, доступные всем. Кроме того, в этой области находятся другие антивирусные программы, распространяемые на принципе SHAREWARE, различная документация, имеющая отношение к борьбе с вирусами, программы демонстрации работы вирусов. Есть здесь и коллекционные вещи - две самые первые версии известной антивирусной программы Aidstest.

Некоммерческие версии антивирусных программ доступны по линии общего доступа для всех

В области A.MC находятся антивирусные средства, разработанные фирмой McAfee Associates распространяемые на принципе SHAREWARE. Здесь вы найдете версии программ VirusScan для операционных систем DOS, Microsoft Windows и IBM OS/2, программу NetShield для Novell NetWare версий 3.x и 4.x и другие интересные вещи. Смотрите сами!

Область A.X содержит обновления вирусной базы данных для программы Doctor Web. Вы должны периодически заглядывать сюда и загружать самые последние дополнения. Эта область не является коммерческой и доступна всем желающим.

В области A.AI, которая делится на области A.AI.R, A.AI.E и A.AI.G, находятся, соответственно, русская, английская и немецкая версии антивирусной программы Aidstest с описанием вирусов и документацией. Причем, заметьте, это самые свежие версии.

Аналогично, в областях A.AW, A.AD и A.AE вы найдете самые свежие версии программ Doctor Web, ADinf и ADinfExt (русская, английская и немецкая версии). Файлы из этих областей доступны только подписчикам.

Область Comm

В файловой области Comm вы найдете самое разное телекоммуникационное программное обеспечение, от простейших терминальных программ, до средств работы с электронной почтой и создания электронных досок объявлений BBS. При необходимости вы сможете загрузить из этой области всю документацию, необходимую для работы с телекоммуникационными программами.

Область UL

Область UL предназначена для загрузки новых файлов. Если у вас есть доступ к этой области, вы сможете загружать сюда те файлы, которые по вашему мнению могут представлять интерес для других. После проверки загруженных файлов системный оператор BBS запишет их в другие области, доступные для чтения. Однако не следует загружать сюда файлы, зараженные вирусами, которые вы хотите передать в АО “ДиалогНаука” на исследование. Для этого предназначена область NV.

Область NV

Как мы только что сказали, область NV предназначена для передачи новых вирусов на исследование в АО “ДиалогНаука”. Вы можете записать в эту область файл, но не можете из нее ничего прочитать. Это понятно - ведь в противном случае кто-нибудь другой смог бы прочитать ваш зараженный файл и получить вместе с ним новый (или старый) вирус.

Как получить новые версии антивирусных программ

В этом разделе мы расскажем, как вы можете получить из BBS АО “ДиалогНаука” новые версии антивирусных программ, как коммерческие, так и некоммерческие, распространяемые на принципе SHAREWARE.

Коммерческая версия программы Aidstest

В этом разделе мы научим вас принимать новые версии антивирусных программ на примере программы Aidstest.

Итак, подключитесь к BBS “ДиалогНаука”, как это было описано раньше. Вы окажетесь в меню выбора области файлов, показанном ниже:

File Areas

I	... Information
A	... Antiviruses
Comm	... Communications
UL	... Unchecked Users Upload
NV	... New Viruses

File area [Area, "["=Prior, "]"=Next, "?"=List]:A

В ответ на приглашение введите символ A. Так как области файлов имеют иерархическую структуру, вы увидите содержимое области файлов A как список областей, представленный ниже:

File Areas

A.G	... Antiviruses: General
-----	--------------------------

A.MC	... Antiviruses: McAfee
A.X	... Antiviruses: Dr.Web virus base add-on
A.AI	... Aidstest (V-Hunter), commercial
A.AW	... Dr.Web, commercial
A.AD	... ADinf, commercial
A.AE	... ADinfExt, commercial

For more areas, type ".." to go up one level or "/" for top level areas.

File area [Area, "["=Prior, "]"=Next, "?"=List]:AI

Если вам будет нужно вернуться в главное (корневое) меню области файлов, введите в ответ на приглашение символ "/" или "..".

Для получения самой последней коммерческой версии программы Aidstest войдите в область A.AI. Вы увидите содержимое этой области:

File Areas

A.AI.R	... Antiviruses: Aidstest, russian
A.AI.E	... Antiviruses: Aidstest (V-Hunter), english
A.AI.G	... Antiviruses: Aidstest (V-Hunter), german

For more areas, type ".." to go up one level or "/" for top level areas.

File area [Area, "["=Prior, "]"=Next, "?"=List]:r

Теперь вы можете вернуться на один уровень иерархии выше, если введете в ответ на приглашение символ "..". Для того чтобы попасть в корневое меню области файлов, следует ввести символ "/".

В области A.AI вы можете выбрать три области, которые называются A.AI.R, A.AI.E и A.AI.G. В них расположены, соответственно, русская, английская и немецкая версии программы Aidstest.

Для получения русской версии войдите в область A.AI.R. Вы окажетесь в главном меню BBS АО “ДиалогНаука”:

MAIN (34 mins):

Message areas File areas Change setup Bulletins

Yell for SysOp Statistics Goodbye (log off) ?help

Select:f

Обратите внимание на первую строку этого меню. В скобках указано время в минутах, которое осталось до завершения сеанса связи с BBS. Это время постоянно уменьшается, так что не теряйте его даром!

В ответ на приглашение введите символ “Г”. Вы окажетесь в меню FILE, предназначенном для работы с файлами из выбранной вами ранее области:

File area A.AIR ... Antiviruses: Aidstest, russian

FILE (32 mins):

Area change Locate a file File titles View text file

Download (receive) Upload (send) Statistics Contents (archive)

Tag (queue) files New files scan Main menu Jump to msg. areas

Goodbye (log off) ?help

Select:f

Найдите в этом меню строку Download (receive). Если ее нет, вы не имеете прав для получения файлов из этой области. В этом случае если вы являетесь подписчиком на антивирусный комплект АО “ДиалогНаука”, оставьте сообщение системному оператору BBS.

Перед тем как загружать новую версию программы, просмотрите список файлов, которые есть в выбранной вами области. Для этого из приведенного выше меню выберите строку File titles. Чтобы это сделать, достаточно ввести в приглашении символ “Г”.

Далее у вас появится возможность выбора - просмотреть все файлы или только новые, либо указать шаблон для поиска файлов:

Files: ["*"=new, <enter>=all, or type a partial filename]:

Для того чтобы просмотреть весь список файлов, нажмите клавишу <Enter>. Вы увидите примерно следующее:

DOC_VIR.LZH 134631 11-03-96 000 Краткое описание вирусов

DOC_LIST.LZH 24769 11-03-96 000 Информация о текущей версии

AIDS.LZH 161669 11-03-96 000 Aidstest.exe v 1447

File area A.AIR ... Antiviruses: Aidstest, russian

FILE (31 mins):

Area change Locate a file File titles View text file

Download (receive) Upload (send) Statistics Contents (archive)

Tag (queue) files New files scan Main menu Jump to msg. areas

Goodbye (log off) ?help

Select:d

Файл AIDS.LZH содержит самую последнюю версию антивирусной программы Aidstest. Именно его нам и нужно получить в первую очередь.

Для получения этого или любого другого файла, расположенного в выбранной области файлов, в ответ на приглашение из меню FILE введите символ “d”, выбрав строку

Download. На экране появится список протоколов передачи данных, доступных на BBS АО “ДиалогНаука”:

Available protocols:

+-----+

| X)modem |

| 1)K-Xmodem |

| Z)modem |

| S)EAlink |

| Y)modem |

| G)Ymodem-G |

| Q)uit |

+-----+

Select: z

В этом списке вы должны выбрать протокол передачи данных, с которым способна работать ваша терминальная программа. Лучше всего выбрать протокол Zmodem, так как он обеспечивает высокую скорость передачи данных и динамически изменяет размер передаваемого блока в зависимости от качества линии связи. Кроме того, при обрыве связи он позволяет возобновить передачу файла с прерванного места (если включен соответствующий режим в вашей терминальной программе).

Если ваша терминальная программа не работает с протоколом Zmodem, попробуйте протоколы Ymodem или Xmodem. Более подробную информацию об использовании протоколов передачи данных вы найдете в 16 томе нашей серии книг “Библиотека системного программиста”.

Если вы выбрали протокол Zmodem, вам будет предложено ввести список файлов для загрузки:

Type "/q" on a blank line to abort download. Type "/e" to edit the

download list. Type "/g" to start the download and log off

afterwards.

For a normal download, simply press <enter>.

File(s) to download (#1): aids.lzh

(1) AIDS.LZH (00:58, 161669 bytes)

File(s) to download (#2):

Вы должны вводить имена нужных вам файлов по одному, нажимая после ввода каждого имени клавишу <Enter>. Чтобы завершить процедуру ввода имен файлов, в ответ на очередное приглашение просто нажмите клавишу <Enter>. Если из одной области вам нужно получить несколько файлов, имеет смысл сделать это сразу.

После ввода имен всех файлов начнется процесс передачи данных. Вы увидите на экране следующее сообщение:

File: AIDS.LZH
Size: 161669 bytes (1264 Xmodem blocks)
Time: 0 minutes and 58 seconds (estimated)
Mode: Zmodem

Begin your download now, or hit <Ctrl-X> several times to cancel.

<00000000000>

В этом сообщении указано имя файла, его длина в байтах и блоках, приблизительное время передачи и протокол передачи данных. Время передачи зависит от скорости передачи данных, которая в конечном счете определяется модемом и качеством телефонной линии.

Когда передача будет закончена, на экране появится соответствующее сообщение и вы вернетесь в меню FILE:

Transfer completed. (CPS=2426, 91%)

File area A.AIR ... Antiviruses: Aidstest, russian

FILE (29 mins):
Area change Locate a file File titles View text file
Download (receive) Upload (send) Statistics Contents (archive)
Tag (queue) files New files scan Main menu Jump to msg. areas
Goodbye (log off) ?help
Select:m

Если вам больше ничего не нужно на BBS, выберите строку Goodbye (log off), для чего в приглашении введите символ “g”.

Для того чтобы перейти в другую файловую область (например, для того чтобы получить последнюю версию программы Doctor Web, выберите из этого меню строку Area change. Это можно сделать, если в ответ на приглашение ввести символ “a”.

Можно также вернуться в главное меню, выбрав строку Main menu. Для этого в приглашении нужно ввести символ m. Вы увидите следующее:

MAIN (1 mins):
Message areas File areas Change setup Bulletins
Yell for SysOp Statistics Goodbye (log off) ?help
Select:

Коммерческая версия программы Doctor Web

Получение последней коммерческой версии программы Doctor Web доступно для подписчиков и выполняется аналогично тому, как это было описано в предыдущем разделе.

Войдите в область файлов A.AW. Напомним, что для перемещения в иерархической системе вложенных областей файлов вы можете использовать команды “..” и “/”. Первая из них перемещает вас в корневую область, вторая - поднимает вверх на одну иерархическую ступень.

Ниже мы привели содержимое области файлов A.AW:

File Areas

A.AW.R ... Antiviruses: Dr.Web, russian
A.AW.E ... Antiviruses: Dr.Web, english
A.AW.G ... Antiviruses: Dr.Web, german

For more areas, type “..” to go up one level or “/” for top level areas.

File area [Area, "["=Prior, "]"=Next, "?"=List]:R

В областях A.AW.R, A.AW.E и A.AW.G находятся, соответственно, русская, английская и немецкая версии антивирусной программы Doctor Web.

Вот что вы увидите, если просмотрите список файлов в области A.AW.R:

-
- Please check area AX for new virus base add-ons
-
WEB.LZH 176266 09-02-96 000 Dr.Web 3.09b, russian
WEB_DOC.LZH 239228 09-02-96 000 Dr.Web 3.09b, russian doc
DRWEBWW.LZH 19321 20-09-95 000 Dr.Web for Winword v 1.00

Файл WEB.LZH содержит последнюю версию программы Doctor Web. Документацию к ней вы найдете в файле WEB_DOC.LZH. В файле DRWEBWW.LZH находится антивирусное средство Doctor Web for Winword, предназначенное для текстового процессора Microsoft Word for Windows, способное обнаруживать и уничтожать макрокомандные вирусы в файлах документов.

Загрузив новую версию программы Doctor Web, просмотрите содержимое области файлов A.X, в которой лежат добавления к вирусной базе данных.

Ниже мы показали, как выглядит список файлов с добавлениями:

-
- ymdd.ver, please read documentation !!!
-
WEB51008.305 1825 08-10-95 000

WEB51016.305	2009 16-10-95 000
WEB51026.305	2758 26-10-95 000
WEB51109.306	2087 09-11-95 000
WEB51226.307	4720 26-12-95 000
WEB60109.308	4662 09-01-96 000
WEB60118.308	4289 18-01-96 000
WEB60206.308	8103 06-02-96 000
WEB60213.309	2511 13-02-96 000
WEB60225.309	2442 25-02-96 000

В имени файла закодирована дата добавления. Например, файл WEB51109.306 был создан 9 сентября 1995 года. О том, как пользоваться добавлениями, вы можете прочитать в документации на программу Doctor Web.

Заметим, что переписывать дополнения к более ранним версиям программы Doctor Web нет смысла, так как они включены в состав последующих версий и не будут подключаться.

Коммерческие версии программ ADinf и ADinfExt

Последнюю версию программы ADinf подписчики смогут найти в области файлов A.AD, содержимое которой приведено ниже:

A.AD.R	... Antiviruses: ADinf, russian
A.AD.E	... Antiviruses: ADinf, english
A.AD.G	... Antiviruses: ADinf, german

Для получения русской версии программы ADinf вы должны переписать файлы ADINF_1.LZH и ADINF_2.LZH из области A.AD.R:

-	
- Attention ! You need both files to install ADinf	
- Внимание! Для установки ADinf'a необходимы оба файла	
-	
ADINF_1.LZH	116276 03-03-96 000 ADinf 10.06, part 1 of 2
ADINF_2.LZH	206934 03-03-96 000 ADinf 10.06, part 2 of 2

Самая последняя версия лечащего модуля ADinfExt находится в области файлов A.AE:

A.AE.R	... Antiviruses: ADinfExt, russian
A.AE.E	... Antiviruses: ADinfExt, english
A.AE.G	... Antiviruses: ADinfExt, germany

Содержимое области A.AE.R (русская версия программы ADinfExt) представлено ниже:

-	
- Attention ! You need both files to install ADinfExt	

- Внимание! Для установки ADinfExt'a необходимы оба файла	
-	
ADINF_1.LZH	120081 03-03-96 000 ADinfExt 3.04, part 1 of 2
ADINF_2.LZH	58642 03-03-96 000 ADinfExt 3.04, part 2 of 2
Вам нужно загрузить из этой области файлы ADINF_1.LZH и ADINF_2.LZH.	

Некоммерческие версии антивирусных программ

Если вы не являетесь подписчиком на антивирусный комплект АО “ДиалогНаука”, это не значит, что вам нечего делать на BBS. Позвоните по линии общего доступа и войдите в область файлов A.G. Здесь вы найдете немало интересного.

Для примера приведем сокращенный список файлов, которые вы можете загрузить из этой области:

ADINFNCR.ZIP	310556 25-02-96 000 ADinf 10.06, noncommercial version, russian
ADINFNCE.ZIP	278476 28-02-96 000 ADinf 10.06, noncommercial version, english
ADINFNCG.ZIP	283533 28-02-96 000 ADinf 10.06, noncommercial version, german
AIDSR.ZIP	279977 30-10-95 000 Aidtest (V-Hunter) 1369, russian, noncommercial version
AIDSG.ZIP	156150 04-03-96 000 Aidtest (V-Hunter) 1369, german, noncommercial version
AIDSE.ZIP	159102 04-03-96 000 Aidtest (V-Hunter) 1369, english, noncommercial version
-	
- Please check area AX for Dr.Web virus base add-on	
-	
WEB.LZH	368699 05-12-95 000 Dr.Web 3.07b, noncommercial version, russian
WEBE.LZH	191186 05-12-95 000 Dr.Web 3.07b, noncommercial version, english
WEBG.LZH	198813 05-12-95 000 Dr.Web 3.07b, noncommercial version, german
DRWEBWW.LZH	19321 20-09-95 000 Dr.Web for WinWord v 1.00
-	
BOOTCHK.ZIP	36221 15-09-95 000 Анализатор дискет BootChecker 3.11

-

- AVL100.ZIP 173719 20-03-93 000 Antiviral Researcher's Toolkit
- FP-218A.ZIP 564540 08-06-95 000 F-prot 2.18a antivirus package
- SDSCAN.ZIP 360331 05-04-94 000 SDscan antivirus
- SOS947.ZIP 43884 31-01-94 000 SOS by Sen v.9.47
- TBAV632.ZIP 278846 23-02-95 000 Thunderbyte antivirus v 6.32
- TBAVW632.ZIP 206740 23-02-95 000 Thunderbyte antivirus
for Win v 6.32
- TBAVX632.ZIP 90264 23-02-95 000 Thunderbyte antivirus
v6.32, optimized *.exe
- TRAP4VIR.ZIP 4867 05-03-90 000 Traps for viruses
- VACCINE.ZIP 14764 14-10-95 000 Вакцина для *.exe файлов
-
- Boot Sector Antiviruses
-
- VITAMINB.ZIP 16734 30-06-92 000 Boot sector virus protector 2.0
by A.Sessa.
- VFORMAT.ZIP 20786 04-11-91 000 Format & boot sector virus
protect 1.9 by A.Sessa
-
- Documentation
-
- ADINFQ&A.ZIP 20168 02-09-95 000 ADInf. Часто задаваемые вопросы
- ADINFQAE.ZIP 6242 02-09-95 000 ADInf. QUESTIONS AND ANSWERS
- ADINFEXT.ZIP 9889 02-09-95 000 ADInf Cure Module (ADInfExt)
-
- MVDEMO.ZIP 12498 16-09-91 000 MARTINs Virus Demonstrator.
- VIRUS.ZIP 21534 12-02-90 000 Virus simulators (not virulent)
- VBOOK.ZIP 160176 20-09-89 000 Virus Presentation (McAfee)
- AIDS001.ZIP 9151 17-11-88 000 Для коллекционеров: самая
первая версия AIDSTEST'a
(подтверждено автором)
- AIDS002.ZIP 9821 16-12-88 000 Для коллекционеров:
вторая версия Aidstest'a

Обратите внимание на файлы ADINFNCR.ZIP, AIDSR.ZIP, WEB.LZH и DRWEBWW.LZH. В них находятся некоммерческие версии всех основных антивирусных программ, входящих в антивирусный комплект АО “ДиалогНаука”. Эти версии вы

можете использовать бесплатно, однако по времени выпуска они всегда отстают от коммерческих примерно на два месяца. Не забывайте об этом, так как каждый день появляются новые вирусы. Кроме того, в этой области находится только некоммерческая версия программы ADInf.

Обратите также внимание на анализатор дискет BOOTCHK.ZIP а также на раздел документации, в котором есть информация по программе ADInf и лечебному модулю ADInfExt.

Просмотр сообщений

Пользуясь электронной доской BBS АО “ДиалогНаука”, вы можете кроме всего прочего послать сообщение авторам антивирусных программ Дмитрию Лозинскому (автор программы Aidstest) и Игорю Данилову (автор программы Doctor Web).

Прежде всего войдите в главное меню BBS:

MAIN (35 mins):
Message areas File areas Change setup Bulletins
Yell for SysOp Statistics Goodbye (log off) ?help
Select:m

В приглашении введите символ “m”. После этого вы окажетесь в разделе сообщений:

The MESSAGE Section
There are 117 messages in this area. The highest is #117
You haven't read any of these.

[0 / 117] Msg.area L1 ... Comments to the SysOp
Press <enter> for the NEXT message.

MESSAGE (35 mins):
Area change Next message Previous message
Enter message Reply to a message
Change current msg =ReadNonStop -ReadOriginal
+ReadReply *ReadCurrent List (brief)
Tag areas Main menu Jump to file areas
Goodbye (log off) Kill (delete) msg Upload a message
Forward (copy) \$Reply Elsewhere
^Download Attaches ?help
Select:a

Из меню MESSAGE выберите строку Area change. Для этого введите в приглашении символ “a”.

На экране появится список доступных вам областей сообщений:

Message Areas

- *L1 ... Comments to the SysOp
- *L2 ... Local Messages
- L3 ... Messages to Dmitry Lozinsky & Igor Daniloff

Message area [Area, "["=Prior, "]"=Next, "?"=List]:

Область L1 предназначена для передачи сообщений системному оператору BBS АО “ДиалогНаука”. В области L2 происходит свободный обмен сообщениями между пользователями, зарегистрированными на BBS. Что же касается области L3, то она предназначена для передачи сообщений авторам антивирусных программ.

Вы можете просмотреть список пользователей BBS АО “ДиалогНаука”, если выберете из меню Main menu строку Statistics и затем строку UserList. При этом на экране появится следующее сообщение:

Press <enter> to list all, or

type a partial name to match:

Если ввести в ответ на него начальные буквы имени пользователя, она покажет всех пользователей, в имени или фамилии которых встречаются введенные вами буквы. Можно нажать клавишу <Enter> и просмотреть полный список пользователей, однако эта процедура может отнять много времени - список довольно длинный.

Для перехода к нужной вам области достаточно ввести обозначение этой области в приглашении Message area.

Для просмотра списка сообщений, находящихся в области, выберите строку List (brief). Для более детального просмотра сообщений используйте строку Browse messages.

Вы можете записать свое сообщение, выбрав строку Enter message, или ответить на сообщение другого пользователя, выбрав строку Reply to a message.

С помощью строки Main menu можно вернуться в главное меню BBS. Выбрав строку Jump to file areas, можно перейти в область файлов.

6 ВОССТАНОВЛЕНИЕ ФАЙЛОВОЙ СИСТЕМЫ

Как правило, опасные вирусы полностью или частично разрушают файловую систему, после чего пользователи теряют доступ ко всем или только некоторым файлам, причем не только программным, но и к файлам данных. Именно такое воздействие вирусов наносит максимальный ущерб, так как файлы документов могут содержать чрезвычайно ценную информацию, ущерб от потери которой может превышать стоимость компьютера во много раз.

Поэтому когда вы приступаете к лечению компьютера, зараженного вирусами, или имеющего поврежденную файловую систему, в первую очередь необходимо выгрузить с его дисков все нужные вам файлы данных. Если в процессе лечения вы потеряете программные файлы, то скорее всего сможете их восстановить без особых проблем, воспользовавшись дистрибутивами или обратившись в фирму, где вы приобретали программы. Потеря же ваших данных невосполнима, и если вы регулярно не выполняете резервное копирование, последствия вирусной атаки могут быть очень неприятными.

Как правило, антивирусные программы, такие как Doctor Web или Aidstest, вылечивают компьютер и автоматически восстанавливают поврежденную файловую систему. Однако бывают случаи, когда и эти программы оказываются бессильными. Например, вирус может уничтожить таблицу размещения файлов или элемент каталога, соответствующий файлу, при этом данные могут оставаться на диске и вы еще сможете их восстановить.

Скажем сразу, что “ручное” восстановление файловой системы доступно только опытным пользователям. Если вы не знакомы в деталях со структурой файловой системы, для восстановления потерянных в результате вирусной атаки данных лучше всего обратиться к специалистам из компьютерной скорой помощи АО “ДиалогНаука”. В крайнем случае можно попробовать восстановить файловую систему такими средствами, как программа SCANDISK.EXE, входящей в комплект поставки современных версий MS-DOS, или программой Norton Disk Doctor. Однако результаты такого восстановления могут быть неудовлетворительными.

В этой главе мы поможем опытным пользователям выполнить самые важные действия по проверке и восстановлению файловой системы MS-DOS с использованием различных программных средств, в первую очередь с использованием программы Norton Disk Editor. Эта программа позволяет просматривать и редактировать содержимое отдельных секторов диска и очень удобна для проведения восстановительных работ.

Восстановление файловой системы необходимо начинать с проверки ее состояния. Именно об этом мы и будем говорить в этой главе.

Проверка файловой системы

Пред тем как начинать восстановление файловой системы, необходимо определить масштаб повреждений. Для этого вы должны тщательно проверить содержимое всех структур данных файловой системы.

С чего лучше начинать проверку файловой системы?

Прежде всего следует проверить установку параметров BIOS, среди которых есть такие ключевые параметры, как типы установленных в компьютере жестких дисков, количество дорожек и секторов на одной дорожке. Если эти параметры установлены неправильно, загрузка операционной системы скорее всего будет невозможна.

Далее необходимо проверить содержимое так называемой главной загрузочной записи MBR (Master Boot Record). В этой записи есть программа начальной загрузки и таблица разделов диска Partition Table. Программа начальной загрузки является объектом атаки загрузочных и файлово-загрузочных вирусов, которые записывают сюда свое тело. При повреждении таблицы разделов диска некоторые или все логические диски будут недоступны для DOS.

На следующем этапе вы должны проверить загрузочную запись Boot Record, которая располагается в самом начале логического диска (не путайте ее с главной загрузочной записью MBR). В загрузочной записи располагается программа начальной загрузки операционной системы, расположенной на логическом диске, а также блок параметров BIOS, который называется BPB (BIOS Parameter Block). Блок BPB содержит важную информацию о логическом диске, такую, например, как размер кластера. Вирус может записать свое тело на место загрузочной записи и повредить блок BPB.

Знор

Очень опасный загрузочный вирус. Заражает главную загрузочную запись MBR на жестком диске и загрузочную запись дискета. Если первый байт на загрузочном секторе имеет значение 0E9h, то вирус записывает на место загрузочной программы свой код, способный заразить главную загрузочную запись MBR жесткого диска и загрузочные секторы дискет.

После выполнения проверки загрузочной записи следует заняться таблицей размещения файлов FAT. В этой таблице находится критически важная информация о расположении отдельных кластеров для всех записанных на данном логическом диске файлов. На диске находится две копии таблицы FAT. Вы можете использовать вторую копию FAT для восстановления.

На следующем этапе нужно проверить корневые каталоги логических дисков, а также все нужные вам вложенные каталоги. При необходимости вы должны восстановить испорченные элементы каталогов, описывающие нужные вам файлы.

Ниже мы подробно рассмотрим все эти действия. Попутно мы приведем всю необходимую информацию о важнейших структурах данных файловой системы.

Проверка параметров BIOS

Когда вы первый раз подходите к компьютеру, возможно зараженному вирусом, необходимо вначале проверить параметры BIOS, которые хранятся в CMOS. Для просмотра и изменения параметров BIOS предназначена специальная программа, которая называется BIOS Setup.

Способ запуска программы BIOS Setup зависит от ее изготовителя и версии, однако обычно запуск выполняется, если во время начального теста оперативной памяти нажать

клавиши <Delete>, <F2> или комбинацию клавиш <Alt+Ctrl+Esc>. Более точную информацию вы можете получить из документации, которая прилагается к системной плате компьютера.

Выключите питание компьютера, если оно было включено, и через 20-30 секунд включите его опять. Такая процедура гарантированно “убивает” резидентные вирусы, “выживающие” после теплой перезагрузки с помощью комбинации клавиш <Ctrl+Alt+Del>. Когда начнется тест памяти, нажмите одну из перечисленных выше клавиш для запуска программы BIOS Setup.

Через некоторое время на экране появится окно программы BIOS Setup, внешний вид которого зависит от изготовителя и версии программы. На рис. 6.1 мы показали внешний вид такого окна для программы BIOS Setup, созданной фирмой AMI.

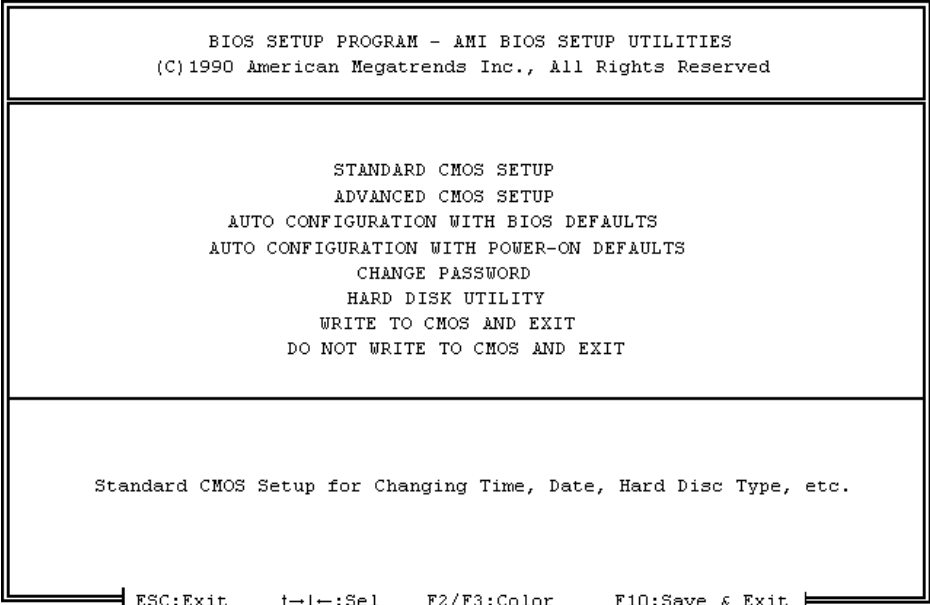


Рис. 6.1. Окно программы BIOS Setup, созданной фирмой AMI

Прежде всего вам нужно выбрать в меню программы строку STANDARD CMOS SETUP и проверить установку стандартных параметров BIOS. Обратите особое внимание на типы и параметры установленных жестких дисков (Hard disk), типы накопителей на гибких магнитных дисках (Floppy Drive) и дату. Примерный вид таблицы, в которой отображаются стандартные параметры, показан на рис. 6.2.

BIOS SETUP PROGRAM - AMI BIOS SETUP UTILITIES							
(C)1990 American Megatrends Inc., All Rights Reserved							
Date (mn/date/year): Fri, Jan 25 1991				Base memory : 640 KB			
Time (hour/min/sec): 02 : 32: 55				Ext. memory : 2816 KB			
	Cyln	Head	WPcom	LZone	Sect	Size	
Hard disk C: type : 40	820	6	820	820	17	41 MB	
Hard disk D: type : Not Installed							
Floppy drive A: : 1.2 MB							
Floppy drive B: : 1.4 MB							
Primary display : VGA/PGA/EGA							
Keyboard : Installed							

Рис. 6.2. Просмотра стин дартны х параме про в BIOS

Перепишите параметры жестких дисков, такие как тип, количество цилиндров, головок и секторов на одной дорожке. Сравните эти значения с паспортными данными, взятыми из документации на жесткий диск. Вирусы могут уменьшать количество дорожек, записывая свое тело в конец диска. Поэтому если значения не совпадают с паспортными, это выглядит очень подозрительно.

Напомним, что тип диска представляет собой число, которое обычно лежит в диапазоне значений от 1 до 47. При этом типам от 1 до 46 соответствуют стандартные наборы параметров.

Как правило, для современных устройств IDE указывается тип 47, который позволяет выполнять ручную установку количества цилиндров, головок и секторов на одной дорожке, а также других. Если в параметрах BIOS установлен 47 тип диска, обязательно проверьте параметры по документации, которая поставляется вместе с диском.

В некоторых случаях может быть указан тип диска с номером 1, хотя в компьютере установлен жесткий диск очень большого размера (типу 1 соответствует размер диска 10 Мбайт). Это означает, что диск полклучен через контроллер, имеющий собственные программы обслуживания в постоянном запоминающем устройстве (ПЗУ).

Иногда оба диска отмечены в параметрах BIOS как Not Installed, однако компьютер нормально работает и операционная система загружается с диска C: (примером может служить портативный компьютер В-300 фирмы Bondwell). В этом случае контроллер диска также имеет собственные программы обслуживания.

<i>Vlad</i>
<i>Неопасный загрузочный вирус. Записывает свой код в перепрограммируемое ПЗУ Flash BIOS, если оно имеет я в компьютере.</i>

Если операционная система не загружается с жесткого диска, прежде всего следует проверить параметры BIOS. Эти параметры могут быть установлены неправильно в

результате разряда аккумуляторной батареи, расположенной на основной плате компьютера или в результате вирусной атаки.

Обратите также внимание на тип накопителя на гибких магнитных дисках (НГМД). Если НГМД с обозначением A: отмечен как Not Installed, вы не сможете загрузить операционную систему с чистой дискеты, свободной от вирусов.

Некоторые вирусы специально отключают устройство A: для того чтобы затруднить процедуру лечения. Когда какая-нибудь программа обращается к устройству A:, вирус перехватывает такое обращение и временно подключает устройство, а затем, после выполнения операции, подключает его снова. Смысл такой процедуры заключается в том, что при отключенном устройстве A: операционная система загружается с диска C: (к счастью, это верно не для всех компьютеров). При этом вирус получает управление первым и контролирует загрузку операционной системы с чистой дискеты.

SMEG.Pathogen.3732

Очень опасный полиморфный вирус, использующий довольно сложный алгоритм шифровки.

В понедельник может записать в байт CMOS с номером 10h значение 0 (тип используемых НГМД). Это означает, что устройства НГМД не установлены. После этого вирус корректирует контрольную сумму CMOS (ячейки 2Eh-2Fh), чтобы при инициализации системы BIOS "не заподозрил" неладное. После данных манипуляций компьютер "не видит" устройства НГМД.

Также при определенных условиях в понедельник в 11 часов вирус может вывести на экран следующий текст

Your hard-disk is being corrupted, courtesy of PATHOGEN!

Programmed in the U.K. (Yes, NOT Bulgaria!) [C] The Black Baron 1993-4. Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!

'Smoke me a kipper, I'll be back for breakfast.....'

Unfortunately some of your data won't!!!!

После этого вирус перехватывает обработчик прерывания от клавиатуры INT 09h и уничтожает информацию в случайных секторах первого же сектора диска. Если в этот момент не перегрузить компьютер кнопкой "RESET" или не выключить питание, то содержимое диска может быть полностью уничтожено (комбинация клавиш <Ctrl+Alt+Del> не поможет)

В завершении процедуры проверки параметров BIOS выберите из главного меню программы BIOS Setup строку ADVANCED CMOS SETUP. На экране появится меню настройки расширенных параметров BIOS (рис. 6.3).

BIOS SETUP PROGRAM - AMI BIOS SETUP UTILITIES (C)1990 American Megatrends Inc., All Rights Reserved			
Typeomatic Rate Programming	: Disabled	Fast Gate A20 Option	: Enabled
Typeomatic Rate Delay (msec)	: 250	Password Checking Option	: Enabled
Typeomatic Rate (Chars/Sec)	: 30.0	Video ROM Shadow C000, 32K	: Enabled
Extended Memory Test	: Disabled	Adapter ROM Shadow C800,32K	: Enabled
Memory Test Tick Sound	: Disabled		
Memory Parity Error Check	: Enabled		
Hit Message Display	: Disabled		
Hard Disk Type 47 R&M Area	: 0:300		
Wait For <F1> If Any Error	: Disabled		
System Boot Up Num Lock	: Off		
Numeric Processor	: Present		
Floppy Drive Seek at Boot	: Disabled		
System Boot Up Sequence	: C:, A:		

Рис. 6.3. Меню настр ойки расширенных параметр ов BIOS

В этом меню обратите внимание на строку System Boot Up Sequence, в которой определяется порядок загрузки операционной системы. Если в этой строке указан порядок загрузки C:, A:, вы не сможете загрузить операционную систему с дискеты. Так как для поиска вирусов вы *обязательно* должны загрузить DOS с чистой дискеты, измените порядок загрузки на A:, C:.

После завершения всех работ с компьютером верните установку C:, A: или C: Only (если такое значение есть в данной версии BIOS). В этом случае компьютер будет надежно защищен от заражения загрузочным вирусом через накопитель на гибких магнитных дисках.

Перед тем как перейти к следующему этапу анализа состояния файловой системы компьютера, убедитесь в том, что в стандартных параметрах BIOS установлен правильный тип диска, что НГМД с обозначением A: подключен и его тип также указан правильно. Кроме этого, в расширенных параметрах BIOS установите порядок загрузки A:, C:.

В некоторых случаях содержимое памяти CMOS разрушается. Это может произойти, например, при выходе из строя аккумуляторной батареи, которая питает память CMOS, или в результате воздействия вируса.

Если это произошло, вы должны восстановить параметры BIOS, воспользовавшись для этого программой BIOS Setup. Как правило, эта программа предоставляет вам возможность установить параметры BIOS, принятые по умолчанию.

Программа BIOS Setup, созданная фирмой AMI, позволяет вам загрузить два набора параметров BIOS.

Первый из них загружается при выборе в главном меню программы (рис. 6.1) строки AUTO CONFIGURATION WITH BIOS DEFAULTS. Этот набор параметров предназначен для нормальной работы системной платы и может быть оптимизирован вручную (при помощи строки ADVANCED CMOS SETUP).

Второй набор параметров соответствует строке AUTO CONFIGURATION WITH POWER-ON DEFAULTS и используется главным образом в тех случаях, когда с первым набором компьютер не запускается. Во втором наборе устанавливаются более консервативные параметры (например, отключается кэширование основной оперативной памяти), что иногда позволяет запустить даже частично неисправный компьютер.

Анализ главной загрузочной записи MBR и таблицы разделов

Когда программа FDISK.EXE впервые создает разделы на жестком диске, она записывает в начало самого первого сектора жесткого диска (сектор 1, дорожка 0, головка 0) главную загрузочную запись MBR.

Главная загрузочная запись является программой, которая во время начальной загрузки операционной системы с жесткого диска помещается по адресу 7C00h:0000h, после чего ей передается управление. Загрузочная запись продолжает процесс загрузки операционной системы.

Заметим, что указанный механизм работает и в том случае, если на диске компьютера вместо DOS установлена какая-нибудь другая операционная система, например, Microsoft Windows 95, Microsoft Windows NT, IBM OS/2 Warp или UNIX.

Если вирус заражает главную загрузочную запись, он получает управление до загрузки операционной системы и может противодействовать даже самым современным антивирусным средствам, применяя стелс-технологии.

Визуально отличить нормальный главный загрузочный сектор от зараженного бывает не всегда просто. Иногда вирус изменяет только несколько байт, в которых записан адрес загрузочного сектора операционной системы, оставляя программу загрузки нетронутой. Такие изменения можно обнаружить только дизассемблированием и последующим анализом восстановленного исходного текста программы загрузки. В некоторых случаях изменения настолько заметны, что их можно обнаружить “невооруженным глазом”, просто взглянув на дамп самого первого сектора диска.

BootCom.Peanut.445

Опасный резидентный вирус с элементами стелс-технологии.
Заражает главную загрузочную запись MBR жесткого диска,
загрузочные секторы дискет а также COM-файлы в момент их запуска.
Если запустить инфицированный COM-файл или загрузить операционную

систем у с зараженной дискеты, вирус поражает главную загрузочную запись диска.

При загрузке с инфицированного жесткого диска вирус размещает свою резидентную копию в верхних адресах памяти и перехватывает прерывание INT 13h. После запуска первой EXE-программы вирус перехватывает прерывание INT 21h.

Вирус не сохраняет оригинальный загрузочный сектор дискеты.

Когда программа или операционная система попытается прочитать содержимое главного загрузочного сектора MBR с помощью прерывания INT 21h, вирус подставляет на место зараженного оригинальный сектор MBR

Другая важная часть первого сектора диска - таблица разделов диска Partition Table.

В ней имеются четыре элемента, которые описывают до четырех разделов диска. В последних двух байтах сектора находится значение 55AAh. Это признак таблицы разделов (сигнатура таблицы разделов).

В разделах диска располагаются логические диски. Обычно создается один первичный раздел для диска C: и один вторичный раздел, в котором создаются логические диски D:, E: и т. д.

Описание формата таблицы разделов

Формат самого первого сектора жесткого диска можно представить следующим образом:

Смещение, байт	Размер, байт	Описание
0	1BEh	Главная загрузочная запись
1BEh	10h	Элемент таблицы разделов диска
1CEh	10h	Элемент таблицы разделов диска
1DEh	10h	Элемент таблицы разделов диска
1EEh	10h	Элемент таблицы разделов диска
1FEh	2	Признак таблицы разделов - значение 0AA55h

Как видно из этой таблицы, байты со смещением от 0 до 1BEh (шестнадцатиричное значение) занимает главная загрузочная запись, то есть программа. Далее идут четыре элемента таблицы разделов, причем каждый элемент занимает 10h байт. После таблицы располагаются два байта признака таблицы разделов.

В элементе таблицы раздела записана информация о расположении и размере раздела в секторах, а также о назначении раздела. Формат элемента таблицы раздела представлен ниже:

Смещение, байт	Размер, байт	Описание
0	1	Признак активного раздела: 0 раздел неактивный; 80h раздел активный
1	1	Номер головки для начального сектора раздела
2	2	Номер сектора и дорожки для начального сектора раздела
4	1	Код операционной системы, которой принадлежит данный раздел: 0 неизвестная система или свободный элемент таблицы разделов; 1, 4 MS-DOS; 5 расширенный раздел MS-DOS
5	1	Номер головки для последнего сектора раздела
6	2	Номер сектора и дорожки для последнего сектора раздела
8	4	Относительный номер сектора начала раздела
0Ch	4	Размер раздела в секторах

Первый байт элемента таблицы раздела содержит признак активного раздела. Если раздел активный, из него будет выполняться загрузка операционной системы. Диск может содержать одновременно несколько активных разделов, которые могут принадлежать разным операционным системам.

Следующие три байта определяют физический адрес на диске начального сектора раздела (который описывает данный элемент раздела).

В байте со смещением 1 записан номер головки начального сектора раздела. В двухбайтовом поле со смещением 2 закодированы номера сектора и дорожки самого первого сектора раздела. При этом биты 0...5 этого поля задают номер сектора, а биты 6...15 - номер дорожки (рис. 6.4).

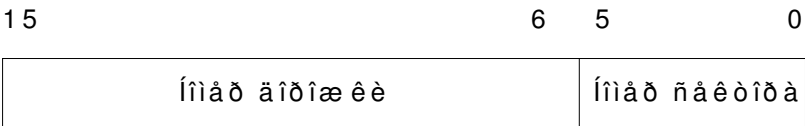


Рис. 6.4. Формат слова, содержащего номер сектора и номер дорожки

Байт со смещением 4 содержит код операционной системы, создавшей раздел. Операционная система MS-DOS отмечает первичный раздел кодом 1 или 4, расширенный

- кодом 5. Для разделов, созданных другими операционными системами, в этом поле будут находиться другие значения.

В байте со смещением 5 и двухбайтовом слове со смещением 6 записаны номер головки, сектора и дорожки последнего раздела. Номер сектора и дорожки хранится в формате, показанном на рис. 6.4.

Последние два поля элемента таблицы разделов имеют длину 4 байта и содержат, соответственно, относительный номер самого первого сектора в разделе (т. е. относительный номер сектора начала раздела) и количество секторов, имеющих в разделе.

Остановимся подробнее на относительном номере самого первого сектора в разделе. Значение относительного номера, равное 0, соответствует дорожке 0, головке 0, сектору 1. При увеличении относительного номера сектора вначале увеличивается номер сектора на дорожке, затем номер головки, и, наконец, номер дорожки. Зная номер дорожки, номер сектора на дорожке и номер головки, можно вычислить относительный номер сектора по следующей формуле:

$$RelSect = (Cyl * Sect * Head) + (Head * Sect) + (Sect - 1)$$

Здесь Cyl обозначает номер дорожки, Sect - номер сектора на дорожке, Head - номер головки.

Обычно разделы диска начинаются с четных номеров дорожек, за исключением самого первого раздела. Этот раздел может начинаться с сектора 2 нулевой дорожки (головка 0), так как самый первый сектор диска занят главной загрузочной записью.

Для наглядности мы воспроизвели из 19 тома нашей серии книг “Библиотека системного программиста” пример схемы разделения жесткого диска на разделы (рис. 6.5).

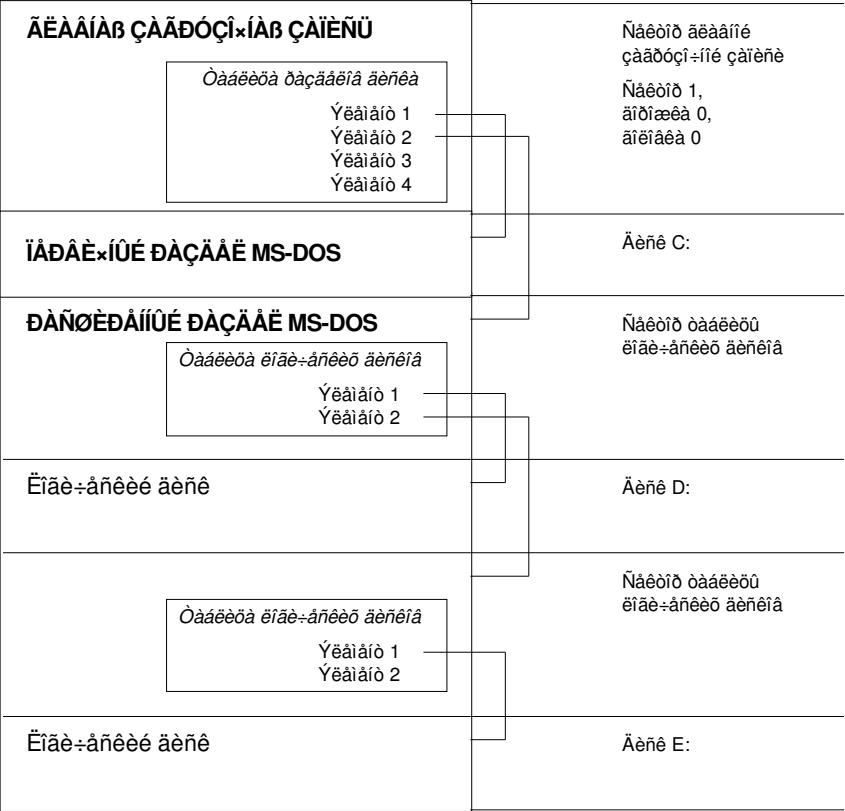


Рис. 6.5. Пример разделения диска на разделы

Как вы знаете, для создания первичного и расширенного разделов диска используется программа FDISK.EXE, входящая в состав дистрибутива MS-DOS.

Первичный раздел должен быть единственным и активным, он используется как диск C: и из него выполняется загрузка операционной системы. В расширенном разделе программа FDISK.EXE создает логические диски D:, E: и т. д. Расширенный раздел не может быть активным, следовательно, из логических дисков, расположенных в этом разделе, невозможно выполнить загрузку операционной системы.

Если байт кода операционной системы имеет значение 5, то в начале соответствующего раздела располагается сектор, содержащий таблицу логических дисков. Эта таблица является расширением таблицы разделов диска, расположенной в самом первом секторе физического диска.

Таблица логических дисков имеет формат, аналогичный таблице разделов диска, но содержит только два элемента. Один из них указывает на первый сектор логического диска MS-DOS, он имеет код системы 1 или 4. Второй элемент может иметь код системы

5 или 0. Если этот код равен 5, то элемент указывает на следующую таблицу логических дисков. Если код системы равен 0, то соответствующий элемент не используется.

Таким образом, таблицы логических дисков связаны в список. Элемент таблицы разделов диска с кодом системы, равным 5, указывает на начало этого списка.

Для таблицы логических дисков имеется отличие в использовании полей границ логических дисков.

Если код системы равен 1 или 4, эти границы вычисляются относительно начала расширенного раздела. Для элемента с кодом системы 5 используется абсолютная адресация (относительно физического начала диска).

Проверка таблицы разделов при помощи программы DISKEDIT.EXE

Наиболее удобное, на наш взгляд, средство анализа логических структур файловой системы - редактор диска DISKEDIT.EXE, который входит в пакет Norton Utilities. Лучше всего записать эту программу на системную дискету, так как только при загрузке с такой дискеты вы сможете исследовать файловую систему, зараженную вирусами или разрушенную файловую систему, когда DOS не загружается с жесткого диска.

Меню Object предоставляет вам широкие возможности выбора структуры для просмотра (рис. 6.6).

Object	Edit	Link	View	Info
Drive...			Alt+D	
Directory...			Alt+R	
File...			Alt+F	
Cluster...			Alt+C	
Sector...			Alt+S	
Physical Sector...			Alt+P	
Partition Table			Alt+A	
Boot Record			Alt+B	
1st FAT			Alt+F1	
2nd FAT			Alt+F2	
Memory Dump...			Alt+M	
Exit			Alt+X	

Рис. 6.6. Меню Object программы DISKEDIT.EXE из пакета Norton Utilities

Для начала выберите из этого меню строку Drive. Если на физическом жестком диске имеются исправные разделы с определенными в них логическими дисками, вы увидите список логических дисков, показанный на рис. 6.7.

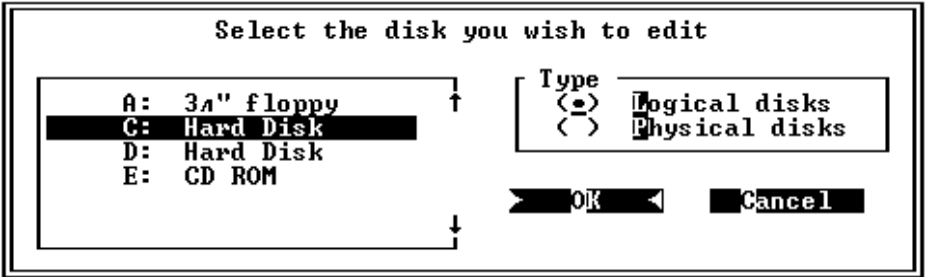


Рис. 6.7. Просмотр списка логических дисков

В данном случае для просмотра доступны логические диски C: и D:, расположенные, соответственно, в основном и расширенном разделах.

Если файловая система компьютера разрушена до такой степени, что невозможно выполнить загрузку операционной системы с диска C:, а при ее загрузке с устройства A: не видно ни одного логического диска, при выборе строки Drive вам будет показан список физических дисков (рис. 6.8).

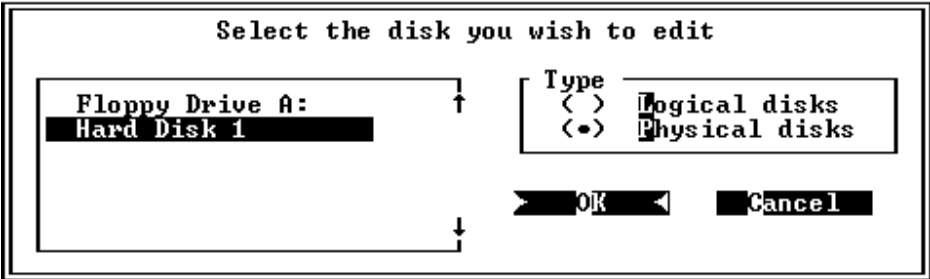


Рис. 6.8. Просмотр списка физических дисков, установленных в компьютере

Для просмотра самого первого сектора физического диска, содержащего главную загрузочную запись и таблицу разделов, выберите физический диск Hard Disk 1 и нажмите кнопку ОК. После этого на экране появится содержимое искомого сектора в виде дампа (рис. 6.9).

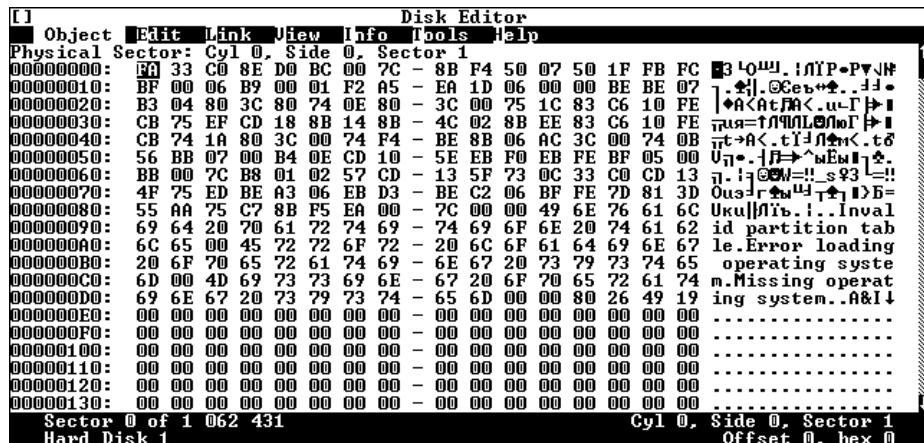


Рис. 6.9. Просмотр содержимого первого сектора первого физического диска

Сектор имеет размер 512 байт, поэтому на одном экране его содержимое не помещается. Вы можете нажать клавишу <PgDn> и посмотреть вторую часть сектора (рис. 6.10).

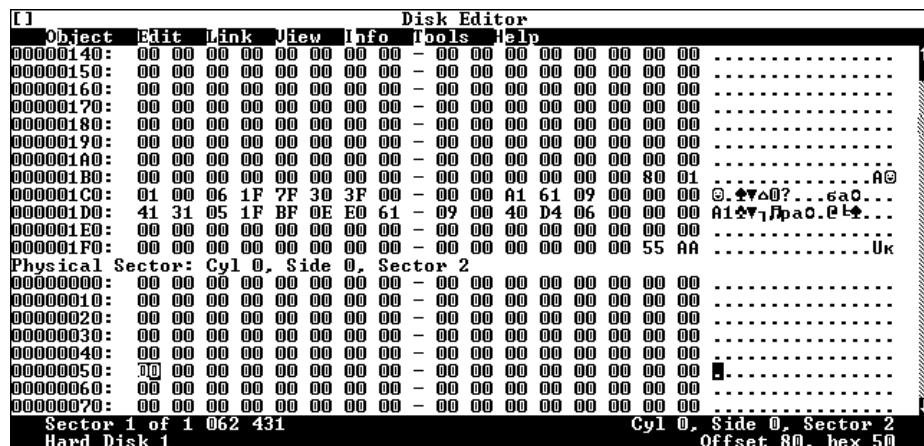


Рис. 6.10. Просмотр второй части первого сектора

На что здесь нужно обратить внимание? В начале сектора (рис. 6.9) находится главная загрузочная запись, которая, как мы уже говорили, является программой. При наличии достаточного опыта вы можете ее дизассемблировать и исследовать. В любом случае следует проверить ее длину (программа загрузки не очень большая). После программы загрузки до начала таблицы разделов должны располагаться нулевые байты. Кроме того, внутри программы загрузки

должны быть сообщения Invalid Partition table, Error loading operating system и Missing operating system.

Несмотря на то что существуют загрузочные вирусы, лишь слегка изменяющие главную загрузочную запись, во многих случаях вы сможете заметить следы нападения, просто взглянув на дампы первого сектора жесткого диска и сравнив его визуально с изображенным на рис. 6.9. Особенно подозрительно, если помимо перечисленных выше текстовых сообщений в теле программы загрузки присутствуют какие-либо еще сообщения.

Что же касается второй части самого первого сектора жесткого диска, в ней должна находиться таблица разделов диска.

Последние два байта должны содержать признак таблицы разделов (сигнатуру) - значение 0AA55h. Обратите внимание, что байты сигнатуры приведены в обратном порядке - байт с младшим значением находится по младшему адресу. Это особенность архитектуры процессоров фирмы Intel.

Вы можете выполнить анализ таблицы разделов диска, пользуясь приведенной выше информацией о ее формате. Напомним, что таблица располагается в первом секторе диска со смещением 1BEh. Однако намного удобнее воспользоваться для анализа этой таблицы форматным просмотром редактора DISKEDIT.EXE.

Установите курсор (мышью или клавишами перемещения курсора) на байт со смещением 1BEh, который соответствует началу таблицы разделов. Затем из меню View выберите строку as Partition Table (рис. 6.11).

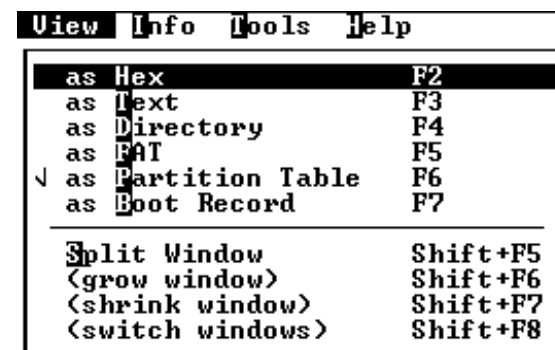


Рис. 6.11. Меню View программы DISKEDIT.EXE из пакета Norton Utilities

На экране появится таблица разделов диска в отформатированном виде (рис. 6.12).

Disk Editor								
Object Edit Link View Info Tools Help								
System	Boot	Starting Location			Ending Location			Number of
		Side	Cylinder	Sector	Side	Cylinder	Sector	Sectors
BIGDOS	Yes	1	0	1	31	304	63	614817
EXTEND	No	0	305	1	31	526	63	447552
unused	No	0	0	0	0	0	0	0
unused	No	0	0	0	0	0	0	0

Partition Table
Hard Disk 1

Cyl 0, Side 0, Sector 1
Offset 446, hex 1BE

Рис. 6.12. Просмотр таблицы разделов диска в отформатированном виде

В столбце System отображается информация об операционной системе, которая строится на основе анализа поля кода операционной системы элемента раздела. Если раздел активен, в столбце Boot для него указана строка Yes, если нет - строка No.

Столбцы Starting Location и Ending Location в полях Side, Cylinder и Sector, содержат в расшифрованном виде информацию, соответственно, о расположении самого первого и самого последнего секторов раздела.

Номер относительного сектора, с которого начинается раздел, вы можете узнать из столбца Relative Sectors, а общее количество секторов - в столбце Number of Sectors.

Полученную информацию о границах разделов имеет смысл сравнить с параметрами жесткого диска, полученными с помощью программы BIOS Setup, так как вирусы могут прятать свое тело в секторах диска, которые находятся в конце диска и не распределены ни одному разделу. Однако при этом следует учитывать, что современные дисковые контроллеры способны выполнять так называемую трансляцию дорожек и головок, которая может исказить полученную картину.

Поясним сказанное на примере.

В одном из наших компьютеров установлен диск, имеющий 1057 дорожек и 16 головок. На каждой дорожке расположено 63 сектора размером 512 байт. При этом общий объем диска составляет 520 Мбайт. Именно эти параметры нам сообщила программа BIOS Setup.

Программа FDISK.EXE определила, что на диске имеется два раздела, размером 300 и 219 Мбайт, а диск используется на 100 процентов (рис. 6.13).

Display Partition Information						
Current fixed disk drive: 1						
Partition	Status	Type	Volume Label	Mbytes	System	Usage
C: 1	A	PRI DOS	MS-DOS_6	300	FAT16	58%
2		EXT DOS		219		42%

Total disk space is 519 Mbytes <1 Mbyte = 1048576 bytes>

The Extended DOS Partition contains Logical DOS Drives.
Do you want to display the logical drive information (Y/N).....?[Y]

Press Esc to return to FDISK Options

Рис. 6.13. Просмотр параметров разделов диска программой FDISK.EXE

В то же время, как видно из рис. 6.12, программа DISKEDIT.EXE для этого диска показывает, что последний сектор последнего раздела расположен на дорожке с номером 526.

На первый взгляд, тут что-то не так: программа BIOS Setup сообщает нам, что на диске имеется 1057 дорожек и 16 головок, а в таблице разделов для последнего сектора последнего раздела мы видим совсем другие значения: этот сектор расположен на 526 дорожке, а номер головки равен 31!

Причина такого несоответствия заключается в том, что наш контроллер типа Enhanced IDE (другое название - Fast ATA), расположенный непосредственно на основной плате компьютера, выполняет трансляцию дорожек и головок, предоставляя программам диск, в котором по сравнению с действительным состоянием меньше дорожек, но больше головок.

Зачем это нужно?

Из-за внутренних ограничений операционная система DOS не может работать с дорожками, номер которых превышает значение 1023. Однако современные дисковые накопители обладают значительной емкостью (порядка 1 - 4 Гбайт и даже больше), поэтому в них приходится делать очень много дорожек. Другие операционные системы, такие как IBM OS/2, Microsoft Windows NT, UNIX или Novell NetWare, не имеют ограничений на количество адресуемых дорожек диска. Что же касается DOS, то без дополнительных мер максимальный размер раздела диска не будет превышать примерно 500 Мбайт.

Логическая трансляция, выполняемая контроллером диска, позволяет операционной системе DOS работать с разделами очень большого размера, поэтому вы можете с ней столкнуться при исследовании большинства современных компьютеров.

Сохранение параметров диска и таблицы разделов диска

Прежде чем продолжить исследование файловой системы, мы настоятельно рекомендуем вам записать параметры диска, определенные с помощью программы BIOS Setup, и

содержимое таблицы разделов диска. Просто перепишите полученные значения на лист бумаги. Если в ходе ремонта вы случайно разрушите область данных BIOS или главный загрузочный сектор, вы сможете легко восстановить критичные данные.

Исследование расширенного раздела диска

Если на диске создан только первичный раздел, можно переходить к анализу логического диска C: (соответствующая процедура будет описана ниже). Если же есть расширенный раздел, необходимо проверить сектор таблицы логических дисков. Это самый первый сектор в расширенном разделе (рис. 6.5).

Давайте посмотрим на этот сектор.
Запустите программу DISKEDIT.EXE, определите с ее помощью расположение расширенного раздела (дорожка, головка и номер сектора). Затем из меню Object выберите строку Physical Sector. На экране появится диалоговая панель Select physical sector range, с помощью которой можно выбрать для просмотра один или несколько секторов (рис. 6.14).

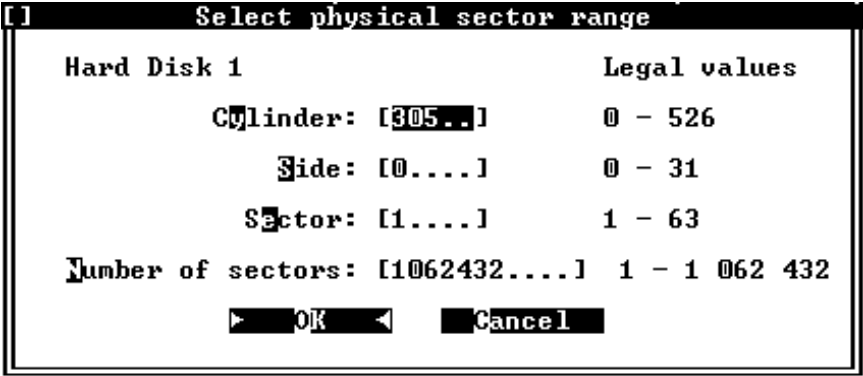


Рис. 6.14. Просмотр сектора по его физическому расположению на диске

В нашем случае согласно рис. 6.12 первый сектор расширенного раздела рсполгается на 305 дорожке, головка 0, сектор 1. Укажите нужные значения и нажмите кнопку ОК.

Сектор таблицы логических дисков, в отличие от сектора главной загрузочной записи, практически пуст (рис. 6.15).

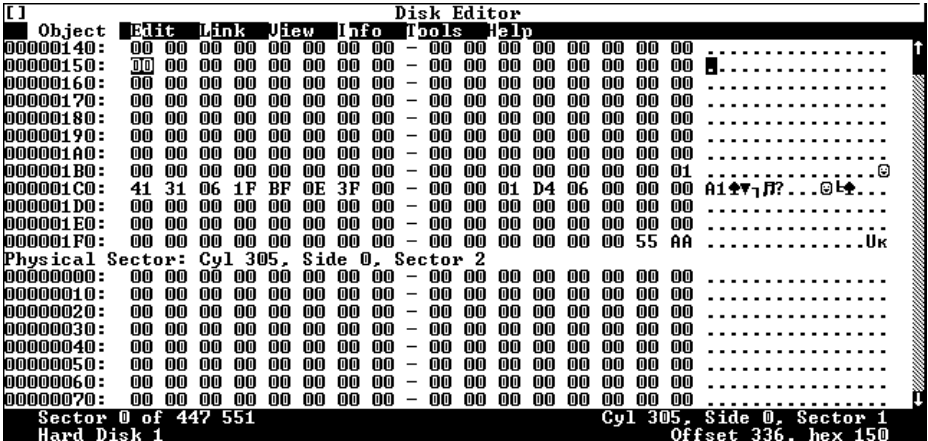


Рис. 6.15. Просмотр сектора таблицы логических дисков

Все байты в нем от начала и до смещения 1BDh включительно должны содержать нулевой значение. Далее со смещения 1BEh располагается таблица логических дисков, состоящая из двух элементов. В конце сектора располагается уже знакомая вам сигнатура - значение 0AA55h.

Формат элементов полностью аналогичен формату элементов таблицы разделов, поэтому вы можете использовать форматный просмотр (рис. 6.16). Для этого установите курсор на байт со смещением 1BEh и затем из меню View выберите строку as Partition Table.

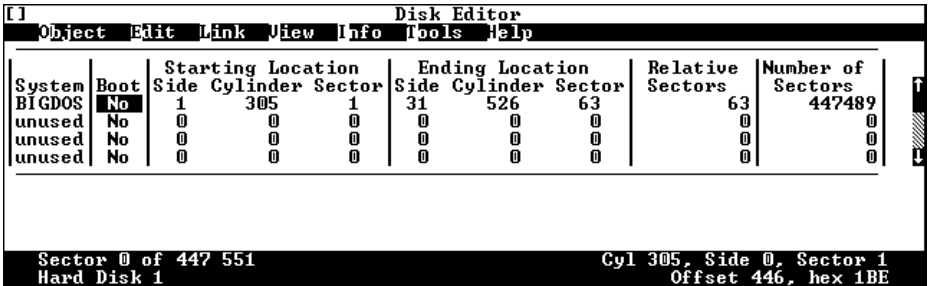


Рис. 6.16. Форматный просмотр таблицы логических дисков

Первая строка таблицы логических дисков описывает логический диск D:, вторая содержит нулевые значения. Если бы в расширенном разделе были созданы несколько логических дисков, второй элемент таблицы таблицы логических дисков указывал на следующий сектор таблицы логических дисков, расположенный непосредственно перед логическим диском E:.

Последняя в списке таблица логических дисков всегда состоит из одной строки, которая описывает последний логический диск.

Сохранение содержимого таблиц логических дисков

На том же листе бумаги, где вы записывали параметры диска и сведения из таблицы разделов диска, запишите информацию о всех логических дисках, полученную из таблиц логических дисков. Если содержимое таблиц логических дисков будет случайно разрушено, вы потеряете доступ к логическим дискам.

Исследование логических дисков

Формат логических дисков, расположенных в разделах жесткого диска, полностью идентичен формату дискет, поэтому многое из того, о чем вы узнаете в этом разделе, будет справедливо и для дискет.

Схематически структура логического диска (или дискеты) изображена на рис. 6.17.

Çàãðóçî÷íúé ñâêðîð çàðâçàðâêðîââíúâ ñâêðîðû
İâðâây êîëÿ FAT
Âòîðây êîëÿ FAT
Êîðíââíé âàðâêîâ
İâêâñòû ââíúô

Рис. 6.17. Структура логического диска

В самом начале логического диска располагается сектор загрузочной записи Boot Record (не путайте его с сектором главной загрузочной записи, который является самым первым на физическом диске), а также, возможно, зарезервированные секторы.

Вслед за этим сектором находятся две копии таблицы размещения файлов (о которой мы еще будем говорить) и корневой каталог. Область данных, занимающая оставшуюся часть логического диска, содержит файлы и остальные каталоги.

Проверка загрузочного сектора

Адрес загрузочного сектора логического диска нетрудно найти в таблице логических дисков (рис. 6.16). В загрузочном секторе логического диска находится программа начальной загрузки операционной системы. Эта программа загружается в оперативную память загрузчиком, расположенным в главной загрузочной записи MBR.

Назначение программы, расположенной в загрузочном секторе логического диска - загрузка операционной системы, находящейся на этом логическом диске.

Таким образом, при включении питания после выполнения процедуры тестирования BIOS загружает в оперативную память содержимое главной загрузочной записи и передает ей управление. Главная загрузочная запись просматривает таблицу разделов

диска и находит активный раздел. Затем она считывает загрузочный сектор логического диска, расположенного в активном разделе, и передает управление находящейся в этом секторе программе загрузки операционной системы. Эта программа, в свою очередь, выполняет всю работу по загрузке операционной системы в память компьютера.

Программа начальной загрузки операционной системы, расположенная в загрузочной записи, является излюбленным объектом нападения загрузочных и файлово-загрузочных вирусов, записывающих в нее свое тело (точно также, как и программа загрузки, расположенная в главной загрузочной записи MBR).

Формат загрузочного сектора зависит от операционной системы и даже от версии операционной системы. Мы рассмотрим формат этого сектора для версий MS-DOS, более ранних, чем 4.0, и для современных версий, таких как 6.22.

Tchechen.1909, 1912, 1914, 3604

Очень опасные резидентные шифрованные вирусы (вирус Tchechen.3604 - полиморфный).

При стирте вирусы данной группы (кроме вируса Tchechen.3604) считывают второй сектор жесткого диска и записывают в него слово "МИР:" и число 4, которое будет являться счетчиком запусков инфицированных программ.

Потом вирусы пытаются найти в ПЗУ BIOS текст вые строки Megatrends, AWARD. Если это им удастся, то вирусы выключают в CMOS-памяти параметр Virus Warning on Boot (контроль записи в загрузочный сектор). Но следует отметить, что при поиске этих двух слов вирусы никогда не смогут найти слово AWARD.

При достижении счетчиком во втором секторе нулевого значения вирусы заменяют слово "МИР:" и помещают в главную загрузочную запись MBR жесткого диска "проанский" код.

Этот код при загрузке операционной системы самостоятельно передает управление активному загрузочному сектору жесткого диска, но примерно через месяц (10 дней для вируса Tchechen.3604) после записи данного кода в MBR уничтожается содержимое всего первого жесткого диска. После чего автором вируса планировался вывод на экран текста, который мы здесь не приводим.

Вирус Tchechen.3604 не заражает программы, имя которых начинается с символов WE, AD, AI, CO, DR, AV, TB, CH. Вирусы Tchechen.1914, 3604 неспособны на процессоре Pentium

Для любой версии MS-DOS помимо программы начальной загрузки операционной системы загрузочная запись содержит параметры, описывающие характеристики данного логического диска. Все эти параметры располагаются в самом начале сектора, в его так

называемой форматированной области. Последние два байта загрузочного сектора содержат уже знакомую вам сигнатуру 0AA55h.

Перед исследованием загрузочной записи вы должны при помощи команды VER определить версию операционной системы MS-DOS, установленной в компьютере. Для версий MS-DOS, более ранних чем 4.0, формат загрузочной записи приведен ниже:

Смещение, байт	Размер, байт	Описание
0	3	Команда JMP xxxx (переход на программу начальной загрузки)
3	8	Название фирмы-изготовителя операционной системы и версия, например: IBM 4.0
0Bh	13	Блок параметров BIOS (BPB)
18h	2	Количество секторов на дорожке
1Ah	2	Количество головок
1Ch	2	Количество скрытых секторов (эти секторы могут использоваться для схемы разделения физического диска на разделы и логические диски)

В самом начале загрузочного сектора располагается команда внутрисегментного перехода JMP. Она нужна для обхода форматированной зоны сектора и передачи управления загрузочной программе, располагающейся со смещением 1Eh.

Название фирмы-изготовителя не используется операционной системой и представляет из себя текстовую строку длиной 8 байт.

Со смещением 0Bh располагается блок параметров BIOS, который обычно обозначается как BPB. Этот блок содержит некоторые характеристики логического диска, такие как количество секторов в одном кластере, общее количество секторов и т. д. Формат блока BPB будет описан позже.

Поля загрузочного сектора со смещениями 18h и 1Ah содержат, соответственно, количество секторов на дорожке и количество головок. Поле со смещением 1Ch содержит количество "скрытых" секторов, которые не принадлежат ни одному логическому диску. Эти секторы могут содержать таблицу разделов диска или таблицы логических дисков.

Для современных версий MS-DOS загрузочный сектор имеет другой формат:

Смещение, байт	Размер, байт	Описание
----------------	--------------	----------

0	3	Команда JMP xxxx (переход на программу начальной загрузки)
3	8	Название фирмы-изготовителя операционной системы и версия
0Bh	25	Extended BPB - расширенный блок параметров BIOS
24h	1	Физический номер устройства (0 - накопитель на гибком магнитном диске НГМД, 80h - жесткий диск)
25h	1	Зарезервировано
26h	1	Символ ')' - признак расширенной загрузочной записи Extended BPB
27h	4	Серийный номер диска (Volume Serial Number), создается во время форматирования диска
2Bh	11	Метка диска (Volume Label)
36h	8	Текстовая строка 'FAT12 ' или 'FAT16 ', которая указывает на формат таблицы размещения файлов FAT

Первые два поля имеют то же назначение, что и в загрузочной записи старых версий MS-DOS.

Поле со смещением 26h содержит символ ')'. Этот символ означает, что используется формат расширенной загрузочной записи и, соответственно, расширенный блок параметров BIOS Extended BPB.

Серийный номер диска формируется во время форматирования диска на основе даты и времени форматирования. Поэтому можно считать, что все диски и дискеты имеют разные серийные номера.

Метка диска формируется при форматировании и может быть изменена командой LABEL операционной системы MS-DOS. Одновременно метка диска помещается в корневой каталог в виде специального дескриптора. О формате каталогов и дескрипторов, а также о формате таблицы размещения файлов FAT мы расскажем позже.

Теперь о блоке параметров BIOS BPB и расширенном блоке параметров BIOS Extended BPB.

Для версий MS-DOS, более ранних чем 4.0, блок BPB имеет следующий формат:

Смещение, байт	Размер, байт	Описание
0	2	Количество байт в одном секторе диска
2	1	Количество секторов в одном кластере
3	2	Количество зарезервированных секторов

5	1	Количество таблиц FAT
6	2	Максимальное количество дескрипторов файлов в корневом каталоге диска
8	2	Общее количество секторов на носителе данных (в разделе MS-DOS)
0Ah	1	Байт-описатель среды носителя данных
0Bh	2	Количество секторов, занимаемых одной копией FAT

Расширенный блок параметров BIOS состоит из обычного блока BPB и дополнительного расширения:

Смещение, байт	Размер, байт	Описание
0	2	Количество байт в одном секторе диска
2	1	Количество секторов в одном кластере
3	2	Количество зарезервированных секторов
5	1	Количество таблиц FAT
6	2	Максимальное количество дескрипторов файлов в корневом каталоге диска
8	2	Общее количество секторов на носителе данных (в разделе MS-DOS)
0Ah	1	Байт-описатель среды носителя данных
0Bh	2	Количество секторов, занимаемых одной копией FAT
0Dh	2	Количество секторов на дорожке
0Fh	2	Количество магнитных головок
11h	2	Количество скрытых секторов для раздела, который по размеру меньше 32 Мбайт
13h	2	Количество скрытых секторов для раздела, превышающего по размеру 32 Мбайт
15h	4	Общее количество секторов на логическом диске для раздела, превышающего по размеру 32 Мбайт

Байт-описатель среды может содержать следующие значения, характеризующие носитель данных:

Значение	Количество сторон	Количество секторов	Диаметр, дюймы	Емкость, Кбайт
0F0h	2	18	3,5	1440
- “ -	2	36	3,5	2880
- “ -	2	15	5,25	1200
0F8h	-	-		Жесткий диск любой емкости
0F9h	2	9	3,5	720
- “ -	2	15	5,25	1200
0FAh	1	8	5,25	320
0FBh	2	8	3,5	640
0FCh	1	9	5,25	180
0FDh	2	9	5,25	360
0FEh	1	8	5,25, 8	160
0FFh	2	8	5,25, 8	320

В этой таблице мы привели данные для дискет и жесткого диска.

Для форматного просмотра блока параметров BPB (или расширенного блока параметров Extended BPB, в зависимости от версии MS-DOS) удобно использовать программу DISKEDIT.EXE. При этом вы можете найти загрузочную запись двумя способами.

Во-первых, можно выбрать из меню Object строку Boot Record (выбрав предварительно нужный логический диск при помощи строки Drive того же меню). При этом вы сразу же окажетесь в режиме форматного просмотра блока параметров BIOS выбранного вами диска (рис. 6.18).

Для распечатки выберите из меню Tools строку Print Object as и в появившейся на экране диалоговой панели выберите строку Boot Record (рис. 6.21). Затем нажмите кнопку OK.

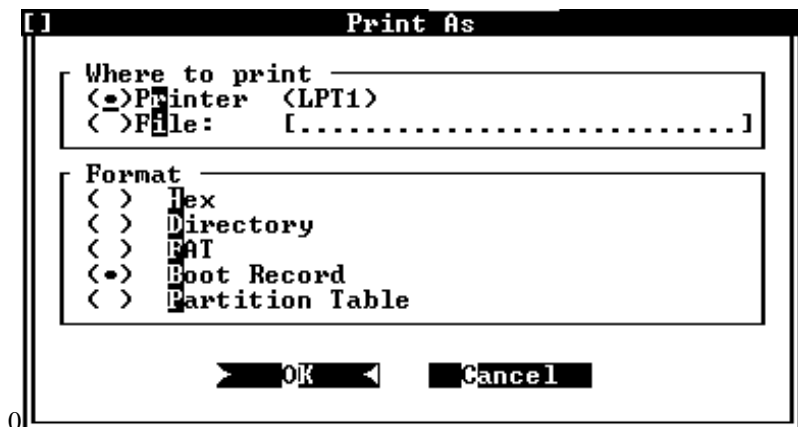


Рис. 6.21. Форматная печать содержимого загрузочного сектора

Аналогичным образом вы можете распечатать содержимое других логических структур файловой системы, например, содержимое таблицы разделов диска.

Анализ зарезервированных секторов

Между загрузочным сектором и таблицей размещения файлов FAT могут находиться зарезервированные секторы, которые являются служебными для файловой системы или не используются.

Количество секторов, зарезервированных на логическом диске, можно узнать из блока параметров BIOS (BPB или Extended BPB, в зависимости от версии операционной системы MS-DOS). Искомое значение находится в поле этого блока со смещением 3. При форматном просмотре количество зарезервированных секторов указано в строке Reserved sectors at beginning (рис. 6.18).

Если зарезервирован только один сектор, то первая копия таблицы размещения файлов FAT располагается сразу вслед за загрузочным сектором. Именно загрузочный сектор в данном случае является зарезервированным.

Когда зарезервировано несколько секторов, между загрузочным сектором и первой копией таблицы FAT может находиться еще несколько секторов, содержащих нулевые значения. В этих секторах может быть спрятано тело вируса или копия оригинальной загрузочной записи, замещенной вирусом.

Таблицы размещения файлов FAT

Операционная система MS-DOS объединяет отдельные секторы диска в так называемые кластеры. При создании новых каталогов и непустых файлов для них выделяется один

или несколько кластеров. Если размер файла увеличивается, для него выделяются дополнительные кластеры.

Размер кластера в секторах (т. е. количество секторов в одном кластере) вы можете узнать из поля блока параметров BIOS BPB со смещением 2. При форматном просмотре содержимого загрузочного сектора размер кластера отображается в строке Sectors per cluster (рис. 6.18).

Для экономии дискового пространства файлам и каталогам распределяются кластеры, которые не обязательно расположены рядом. Таким образом, отдельные кластеры, принадлежащие одному и тому же файлу, могут находиться в разных местах логического диска. За такую экономию приходится платить производительностью, так как считывание фрагментированного файла связано с многочисленными перемещениями магнитных головок, а это самая медленная дисковая операция.

Другая проблема, связанная с фрагментацией файлов, заключается в необходимости хранения списка кластеров, выделенных каждому файлу. Очевидно, для того чтобы прочитать файл, операционная система MS-DOS должна последовательно прочитать все кластеры, распределенные этому файлу.

Где же хранятся списки кластеров?

Эти списки хранятся в таблице размещения файлов FAT, к анализу которой мы скоро приступим.

Таблицу размещения файлов можно представить себе как массив, содержащий информацию о кластерах. Размер этого массива определяется общим количеством кластеров на логическом диске. В элементах этого массива находятся списки кластеров, распределенных файлам. Элементы массива, соответствующие свободным кластерам, содержат нулевые значения.

Если файл занимает несколько кластеров, то эти кластеры связаны в список. При этом элементы таблицы FAT содержат номера следующих используемых данным файлом кластеров. Конец списка отмечен в таблице специальным значением. Номер первого кластера, распределенного файлу, хранится в элементе каталога, описывающего данный файл.

Таким образом, зная имя файла и каталог, в котором этот файл расположен, операционная система MS-DOS может определить номер первого кластера, распределенного файлу, а затем, проследив список кластеров по таблице FAT, определить и номер остальных кластеров, занятых этим файлом.

Программа FORMAT.COM, предназначенная для форматирования диска и некоторые специальные программы аналогичного назначения проверяют логический диск на предмет наличия дефектных областей. Кластеры, которые находятся в этих дефектных областях, отмечаются в FAT как плохие и не используются операционной системой.

Для примера на рис. 6.22 показаны упрощенные дескрипторы корневого каталога диска C:, в которых описаны файлы MYFILE1.DOC и MYLETTER.DOC, а также элементы таблицы размещения файлов FAT, выделенные для этих файлов.

Рис. 6.22. Пример распределения кластеров для файлов в autoexec.bat и config.sys

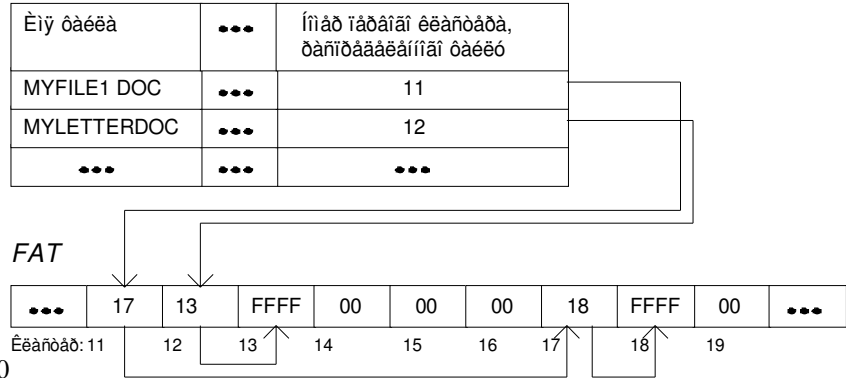


Рис. 6.22. Пример распределения кластеров для файлов в autoexec.bat и config.sys

Файл MYFILE1.DOC занимает три кластера с номерами 11, 17 и 18, а файл MYLETTER.DOC - два кластера с номерами 12 и 13. В каталоге указаны номера первых кластеров, распределенных этим файлам (соответственно 11 и 12). Последние ячейки, которые соответствуют последним кластерам, распределенным файлам, содержат специальное значение - 0FFFh (признак конца цепочки кластеров).

Формат таблицы FAT

Остановимся подробнее на формате таблицы FAT.

Таблица FAT может иметь 12- или 16-разрядный формат. При этом в таблице для хранения информации об одном кластере диска используется, соответственно, 12 или 16 бит.

Первый из этих двух форматов (12-разрядный) применяется для дисков с небольшим количеством секторов. При этом вся таблица размещения файлов помещается в одном секторе.

Если размер диска слишком большой, для представления всех кластеров двенадцати разрядов будет недостаточно. В этом случае используется 16-разрядный формат FAT. При этом операционная система MS-DOS может работать с диском, который имеет размер более 32 Мбайт. Поэтому для жестких дисков используется именно 16-разрядный формат таблицы FAT.

Как узнать формат FAT?

Проще всего прочитать его в текстовой строке, расположенной в загрузочном секторе со смещением 36h. При форматном отображении содержимого загрузочного сектора тип таблицы FAT отображается в строке File System ID (рис. 6.18).

Кроме того, если разделы жесткого диска создавались программой FDISK.EXE, формат FAT можно определить, анализируя содержимое поля кода системы соответствующего элемента таблицы разделов, расположенной в главной загрузочной записи MBR. Если это поле содержит значение 1, используется 12-разрядный формат, если 4, то 16-разрядный.

Первый элемент таблицы FAT имеет особый формат.

Самый первый байт таблицы FAT называется "Описатель среды" (Media Descriptor). Он имеет такое же значение, как и байт-описатель среды, загрузочного сектора логического диска.

Следующие 5 байт для 12-разрядного формата или 7 байт для 16-разрядного формата всегда содержат значение 0FFh.

Вся остальная часть таблицы FAT состоит из 12- или 16-разрядных ячеек. Каждая ячейка соответствует одному кластеру диска. Эти ячейки для разных форматов таблицы FAT могут содержать следующие значения:

0FAT12	0FAT16	0Описание
1000h	10000h	1Свободный кластер
20FF0h - 0FF6h	20FFF0h - 0FFF6h	2Зарезервированный кластер
30FF7h	30FFF7h	3Плохой кластер
40FF8h - 0FFFh	40FFF8h - 0FFFh	4Последний кластер в списке
5002h - 0FEFh	50002h - 0FFEfFh	5Номер следующего кластера в списке

Просмотр таблицы FAT

Для просмотра таблицы размещения файлов FAT мы воспользуемся программой DISKEDIT.EXE. Из меню Object выберите строку Drive и укажите интересующий вас диск. Если файловая система находится в более или менее исправном состоянии, вы сможете выбрать нужный вам логический диск.

Затем из меню Object выберите одну из двух строк - 1st FAT или 2nd FAT. На экране появится, соответственно, содержимое первой или второй копии таблицы FAT в отформатированном виде (рис. 6.23).

0

Disk Editor							
Object	Edit	Link	View	Info	Tools	Help	
Sector 1							
9	10	11	4	5	6	<EOF>	8
<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>
<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>
61	<EOF>	35	36	37	46	<EOF>	<EOF>
<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>	<EOF>
<EOF>	<EOF>	51	52	53	54	58	56
57	<EOF>	59	60	63	888	<EOF>	64
65	69	67	68	<EOF>	70	71	<EOF>
73	74	75	76	77	<EOF>	79	80
81	82	83	84	85	86	87	88
89	90	91	92	93	94	100	96
<EOF>	98	99	<EOF>	101	102	103	104
105	106	107	108	109	110	111	112
113	<EOF>	<EOF>	116	117	118	119	120
121	122	123	124	125	126	127	128
129	130	131	132	133	134	135	136
<EOF>	<EOF>	139	140	141	142	143	144
<EOF>	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160
FAT (1st Copy)				Sector 1			
C:\IO.DOS				Cluster 2, hex 2			

Рис. 6.23. Просмотр первой копии таблицы размещения FAT в отформатированном виде

Вы также можете найти первую или вторую копию таблицы FAT, зная физический адрес загрузочной записи логического диска. Напомним, что загрузочная запись располагается в самом первом секторе дискеты. Расположение загрузочной записи для логических дисков, созданных в разделах жесткого диска, можно определить из таблицы разделов (для логического диска C:) или таблицы логических дисков (для логических дисков, созданных в расширенном разделе).

0BadSectors.3422, 3428

Опасные резидентные вирусы.

О перехваты вают прерывания INT 8h, INT 16h, INT 21h, INT 25h, INT 26h.

ОИногда отмечают кластеры диска как плохие посредством манипуляций с таблицами размещения файлов в FAT. Не заражают антивирусную программу SCAN.

ОСодержат текстовые строки:

ОСOMEXE

ОSCAN

0BadSectors.3422: BadSectors 1.1

0BadSectors.3428: BadSectors 1.2

ОДалее, в рамках логического диска существует своя последовательная нумерация секторов. При этом порядок нумерации выбран таким, что при последовательном увеличении номера сектора вначале увеличивается номер головки, затем номер дорожки.

ОПоясним это на примере.

ОПусть, например, у нас есть дискета с девятью секторами на дорожке. Сектор с логическим номером, равным 1, расположен на нулевой дорожке и для обращения к нему используется нулевая головка. Это самый первый сектор на дорожке, он имеет номер 1. Следующий сектор на нулевой дорожке имеет логический номер 2, последний сектор на нулевой дорожке имеет логический номер 9. Сектор с логическим номером 10 расположен также на нулевой дорожке. Это тоже самый первый сектор на дорожке, но теперь для доступа к нему используется головка с номером 1. И так далее, по мере увеличения логического номера сектора изменяются номера головок и дорожек.

ОСогласно такой нумерации, сектор с последовательным номером 0 - это загрузочный сектор. Для того чтобы просмотреть содержимое загрузочного сектора при помощи программы DISKEDIT.EXE, вы можете выбрать из меню Object строку Sector и в появившейся диалоговой панели указать номер сектора, равный нулю (рис. 6.24).

0

Select sector range

Drive C:
Valid sector numbers are
0 through 615 118.

Starting Sector: [0.....]

Ending Sector: [615118]

Sector	Usage
0	Boot area (used by DOS)
1 - 151	1st FAT area (used by DOS)
152 - 302	2nd FAT area (used by DOS)
303 - 334	Root dir area (used by DOS)
335 - 615 118	Data area (where files are stored)

OK
Cancel

Рис. 6.24. Просмотр сектора логического диска по его последовательному номеру

ОЗаметьте, что в этой диалоговой панели в рамке, озаглавленной Sector Usage, показано распределение секторов. Пользуясь этим распределением, вы легко сможете определить последовательный номер сектора загрузочной записи, начало и границы обеих копий FAT, а также начало и границы корневого каталога и области данных, содержащих файлы и другие каталоги.

ОС помощью меню View вы можете просмотреть содержимое таблицы FAT в виде дампа (рис. 6.25).

0Любой каталог (и корневой в том числе) содержит 32-байтовые элементы - дескрипторы, описывающие файлы и другие каталоги. Приведем формат дескриптора:

0

0Смещение, байт	0Размер, байт	0Описание
10	18	1Имя файла или каталога, выравненное на левую границу и дополненное пробелами
28	23	2Расширение имени файла, выравненное на левую границу и дополненное пробелами
30Bh	31	3Байт атрибутов файла
40Ch	410	4Зарезервировано
516h	52	5Время создания файла или время его последней модификации
618h	62	6Дата создания файла или дата его последней модификации
71Ah	72	7Номер первого кластера, распределенного файлу
81Ch	84	8Размер файла в байтах

0

0Обратите внимание на поле со смещением 1Ah. Это номер первого кластера, распределенного файлу или каталогу (если дескриптор описывает каталог более низкого уровня). Пользуясь этим значением, вы сможете проследить по таблице размещения файлов FAT всю цепочку кластеров, распределенных данному файлу или каталогу. Таким образом, у нас имеется способ отыскать начало цепочки кластеров для любого файла - нужно лишь найти соответствующий дескриптор.

0В любом каталоге, кроме корневого, два первых дескриптора имеют специальное назначение. Первый дескриптор содержит в поле имени строку:

0". "

0Этот дескриптор указывает на содержащий его каталог. То есть каталог имеет ссылку сам на себя. Второй специальный дескриптор содержит в поле имени строку:

0".. "

0Этот дескриптор указывает на каталог более высокого уровня.

0Если в поле номера первого занимаемого кластера для дескриптора с именем ".. " находится нулевое значение, это означает, что данный каталог содержится в корневом каталоге.

0В древовидной структуре каталогов имеются ссылки как в прямом, так и в обратном направлении. Эти ссылки можно использовать для проверки сохранности структуры каталогов файловой системы.

0Байт атрибутов является принадлежностью каждого файла. Биты байта атрибутов имеют следующие значения:

0

0Бит	0Описание
10	1Файл предназначен только для чтения. 2В этот файл нельзя писать и его нельзя стирать
21	3Скрытый файл. 4Этот файл не будет появляться в списке файлов, который отображается командой DIR
32	5Системный файл. 6Этот бит обычно установлен для файлов, которые являются составной частью операционной системы
43	7Данный дескриптор описывает метку диска. 8Для этого дескриптора поле имени файла и поле расширения имени файла должны рассматриваться как одно поле длиной 11 байт. Это поле содержит метку диска
54	9Дескриптор описывает файл, являющийся подкаталогом данного каталога
65	10Флаг архивации. 11Если этот бит установлен в 1, то данный файл не был выгружен утилитой архивации
76-7	12Зарезервированы

0

0Обычно файлы имеют следующие атрибуты:

0

0Атрибут	0Описание
10	1Обычные файлы (тексты программ, загрузочные модули, пакетные файлы)
27	2Только читаемые, скрытые, системные файлы. Такая комбинация битов байта атрибутов используется для файлов операционной системы IO.SYS, MSDOS.SYS
38	3Метка тома. Дескриптор метки тома может находиться только в корневом каталоге логического диска
410h	4Дескриптор, описывающий каталог
520h	5Обычный файл, который не был выгружен программами BACKUP.EXE или XCOPY.EXE

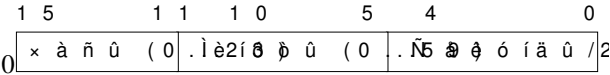
0

0При удалении файла первый байт его имени заменяется на байт E5h (символ “х”). Все кластеры, распределенные удаленному файлу, отмечаются в таблице FAT как свободные.

0Если вы только что удалили файл, его еще можно восстановить, так как в дескрипторе сохранились все поля, кроме первого байта имени файла. Но если на диск записать новые файлы, то содержимое кластеров удаленного файла будет изменено и восстановление станет невозможным.

0Теперь о полях времени и даты.

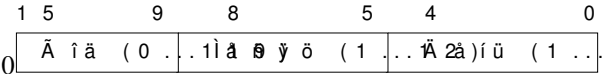
0Формат поля времени показан на рис. 6.27.



0Рис. 6.27. Формат поля времени

0Старшие пять бит содержат значение часа модификации файла, шесть бит с номерами 5 - 10 хранят значение минут модификации файла, и, наконец, в младших 5 битах находится значение секунд, деленное на 2. Для того, чтобы время обновления файла уместилось в шестнадцати битах, пришлось пойти на снижение точности времени до двух секунд. В подавляющем большинстве случаев такое снижение точности не играет никакой роли.

0Формат даты обновления файла напоминает формат времени и показан на рис. 6.28.



0Рис. 6.28. Формат поля даты

0Для того чтобы получить значение года обновления файла, необходимо прибавить к величине, хранимой в старших семи битах, значение 1980.

0Некоторые вирусы используют поля времени и даты для отметки зараженных файлов. Такая отметка нужна для того чтобы избежать повторного заражения. Однако такой примитивный способ используется только простейшими вирусами.

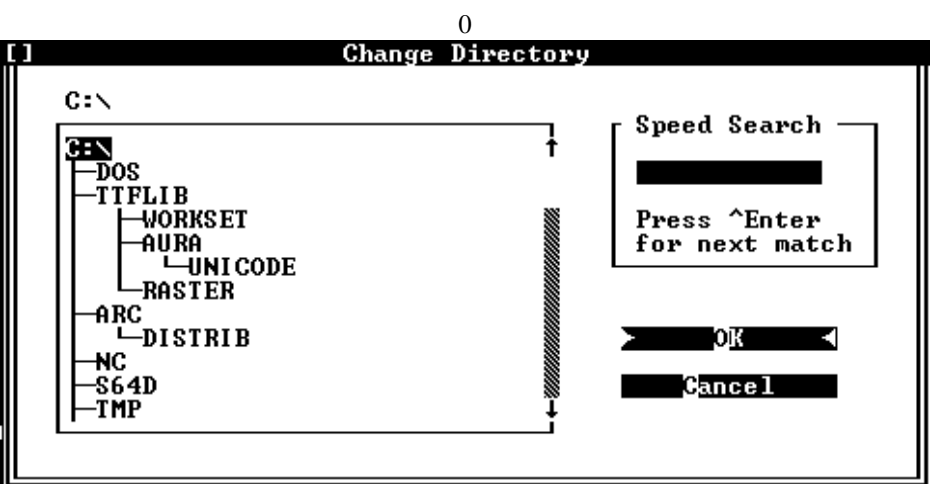
0Поле длины в дескрипторе содержит точную длину файла в байтах. Для каталогов в поле длины записано нулевое значение.

0Когда вирус заражает файл, его длина, как правило, увеличивается. Тем не менее стелс-вирусы эффективно маскируют такое увеличение, поэтому его можно заметить только при загрузке операционной системы с чистой дискеты.

0Просмотр каталогов

0Для просмотра каталогов с целью проверки их структуры мы воспользуемся программой DISKEDIT.EXE.

0Запустите эту программу и из меню Object выберите строку Directory. На экране появится диалоговая панель Change Directory, показанная на рис. 6.29.



0Рис. 6.29. Диалоговая панель Change Directory, предназначенная для выбора каталога

0В левой части диалоговой панели отображается дерево каталогов текущего диска. Выберите в нем корневой каталог C:\ и нажмите кнопку ОК. После этого на экране появится содержимое корневого каталога в форматированном виде (рис. 6.30).

Disk Editor										
Object	Edit	Link	View	Info	Tools	Help				
Name	Ext	Size	Date	Time	Cluster	Arc	R/O	Sys	Hid	Dir
Sector 303										
BOOTLOG	TXT	45741	25.11.95	20:40	187	Arc			Hid	
MSDOS	SYS	1651	8.12.95	19:57	37427	Arc	R/O	Sys	Hid	
IO	SYS	223148	24.08.95	9:50	17215		R/O	Sys	Hid	
MS-DOS_6		0	10.01.95	17:50	0	Arc				Vol
DOS		0	10.01.95	17:50	2					Dir
TTFLIB		0	10.01.95	19:55	797					Dir
ARC		0	10.01.95	20:03	13					Dir
NC		0	13.05.95	21:22	15					Dir
S64D		0	10.01.95	18:33	23					Dir
TEMP		0	23.05.95	13:17	24					Dir
UT		0	10.01.95	19:46	14					Dir
NC4		0	10.01.95	21:19	69					Dir
SYMANTEC		0	10.01.95	21:27	70					Dir
TEMP		0	10.01.95	22:12	72					Dir
BACKUP		0	11.01.95	13:13	73					Dir
GAMES		0	5.03.95	20:38	171					Dir
Sector 304										
IMPORT		0	15.05.95	21:23	176					Dir
TEXTS		0	15.05.95	21:24	195					Dir
Root Directory										
C:\										
										Sector 303
										Offset 0, hex 0

0Рис. 6.30. Просмотр содержимого корневого каталога диска C: в форматированном виде

Анализируя полученную информацию, вы можете обнаружить подозрительные изменения в полях размера файла, даты и времени. Кроме того, для каждого файла в столбце Cluster отображается номер распределенного ему первого кластера.

ОС помощью меню View можно переключиться в режим неформатированного просмотра, когда содержимое каталога отображается в виде дампа (рис. 6.31).

0

Disk Editor	
Object	Edit Link View Info Tools Help
Sector 303	
00000000:	4F 4F 54 4C 4F 47 20 - 54 58 54 22 00 00 00 00 BOOTLOG TXT"....
00000010:	00 00 79 1F 00 00 1B A5 - 79 1F BB 00 AD B2 00 00 ..y...ey...H
00000020:	4D 53 44 4F 53 20 20 20 - 53 59 53 27 00 AA 21 9F MSDOS SYS'.k!Я
00000030:	88 1F 88 1F 00 00 21 9F - 88 1F 33 92 73 06 00 00 MWM...!ЯW3Ts
00000040:	49 4F 20 20 20 20 20 20 - 53 59 53 07 00 00 00 00 IO SYS.
00000050:	00 00 7A 1F 00 00 40 4E - 18 1F 3F 43 AC 67 03 00 ..z...@M?Cmg
00000060:	4D 53 2D 44 4F 53 5F 36 - 20 20 20 28 00 00 00 00 MS-DOS_6 <....
00000070:	00 00 00 00 00 00 5D 8E - 2A 1E 00 00 00 00 00 0010*Δ
00000080:	44 4F 53 20 20 20 20 20 - 20 20 20 10 00 00 00 00 DOS >.....
00000090:	00 00 00 00 00 00 5D 8E - 2A 1E 02 00 00 00 00 0010*Δ
000000A0:	54 54 46 4C 49 42 20 20 - 20 20 20 10 00 00 00 00 TIFLIB >.....
000000B0:	00 00 00 00 00 00 F5 9E - 2A 1E 1D 03 00 00 00 0010*Δ
000000C0:	41 52 43 20 20 20 20 20 - 20 20 20 10 00 00 00 00 ARC >.....
000000D0:	00 00 00 00 00 00 6C A0 - 2A 1E 0D 00 00 00 00 001a*Δ
000000E0:	4E 43 20 20 20 20 20 20 - 20 20 20 10 00 00 00 00 NC >.....
000000F0:	00 00 00 00 60 01 DB AA - AD 1E 0F 00 00 00 00 00 00C...k...*
00000100:	53 36 34 44 20 20 20 20 - 20 20 20 10 00 00 00 00 \$64D >.....
00000110:	00 00 00 00 00 00 37 94 - 2A 1E 17 00 00 00 00 007...*Δ
00000120:	54 4D 50 20 20 20 20 20 - 20 20 20 10 00 00 00 00 TMP >.....
00000130:	00 00 00 00 00 00 25 6A - B7 1E 18 00 00 00 00 00Z...inΔ
Root Directory C:\	
Sector 303 Offset 0, hex 0	

Рис. 6.31. Просмотр содержания корневого каталога диска C: в виде дампа

Обратите внимание на меню Link. С помощью этого меню вы можете переходить к просмотру логически связанных между собой структур файловой системы (рис. 6.32).

0

Disk Editor	
Object	Edit Link View Info Tools Help
Name	.Ext
Sector	303
BOOTLOG	TXT
MSDOS	SYS
IO	SYS
MS-DOS_6	
DOS	
TIFLIB	

File	Ctrl+F
<directory>	Ctrl+D
Cluster chain <FAT>	Ctrl+I
<partition>	
<window>	

Рис. 6.32. Меню Link позволяет просматривать логически связанные структуры файловой системы

Выделите в корневом каталоге диска C: файл IO.SYS, как это показано на рис. 6.32, и затем выберите из меню Link строку Cluster chain (FAT). Вы окажетесь в режиме просмотра первой копии таблицы размещения файлов FAT, причем цепочка кластеров, выделенная файлу IO.SYS, будет выделена (рис. 6.33).

0

Disk Editor	
Object	Edit Link View Info Tools Help
17105	17106 17107 17108 17109 17110 17111 17112
17113	17114 17115 17116 17117 17118 17119 17120
17121	17122 17123 17124 17125 17126 <EOF> 17128
17129	17130 <EOF> 17132 17133 17134 17135 17136
17137	17138 17139 17140 17141 17142 <EOF> 17144
17145	17146 17147 17148 17149 17150 17151 17152
Sector 68	
17153	17154 <EOF> 17156 17157 17158 17159 17160
17161	17162 17163 17164 17165 17166 17167 17168
17169	17170 17171 17172 17173 17174 17175 17176
17177	17178 17179 17180 17181 17182 17183 17184
17185	17186 17187 17188 17189 17190 17191 17192
17193	17194 17195 17196 17197 17198 17199 17200
17201	17202 17203 <EOF> 17205 17206 17207 17208
17209	17210 17211 17212 17213 17214 <EOF> n 17216
n 17217	n 17218 n 17219 n 17220 n 17221 n 17222 n 17223 n 17224
n 17225	n 17226 n 17227 n 17228 n 17229 n 17230 n 17231 n 17232
n 17233	n 17234 n 17235 n 17236 n 17237 n 17238 n 17239 n 17240
n 17241	n 17242 n <EOF> 17244 17245 <EOF> <EOF> <EOF>
17249	17250 <EOF> <EOF> <EOF> <EOF> <EOF> <EOF>
<EOF>	<EOF> <EOF> <EOF> <EOF> 17261 17262 17263 17264
FAT (1st Copy) C:\IO.SYS	
Cluster 17 231, hex 434F	

Рис. 6.33. Просмотр цепочки кластеров, выделенный файлу IO.SYS

ОС помощью строки File меню Link вы можете перейти в режим просмотра содержимого файла IO.SYS (рис. 6.34).

0

Disk Editor	
Object	Edit Link View Info Tools Help
Cluster 17 215, Sector 275 743	
00000000:	5D 5A AC 01 B4 01 00 00 - 20 2B 3A 03 FF FF 76 0B 7Zm@ @...+:v vδ
00000010:	80 00 00 00 00 00 00 00 - 1E 00 00 00 01 00 00 00 A...BΔ...@...
00000020:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000030:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000040:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000050:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000060:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000070:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000080:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000090:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000A0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000B0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000C0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000D0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000E0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
000000F0:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000100:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000110:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000120:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
00000130:	00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
File C:\io.sys	
Cluster 17 215 Offset 0, hex 0	

Рис. 6.34. Просмотр содержимого файла IO.SYS в виде дампа

Отметим, что во многих случаях можно выполнять переходы между логически связанными структурами данных двойным щелчком левой клавиши мыши по изображению этих структур, что очень удобно. Подробности вы найдете в документации к пакету Norton Utilities.

На что следует обратить внимание при проверке структуры каталогов?

ОКроме визуальной проверки полей расположенных там дескрипторов следует просмотреть весь каталог до конца. Необходимо убедиться, что в каталоге отсутствуют посторонние данные, которые могут быть записаны туда вирусом.

ОНа рис. 6.35 вы видите удаленный файл с именем xONFIG.SYS (бывший CONFIG.SYS) и свободные элементы каталога, отмеченные строкой Unused directory entry.

0

Disk Editor										
Object	Edit	Link	View	Info	Tools	Help				
Name	Ext	Size	Date	Time	Cluster	Arc	R/O	Sys	Hid	Dir
Cluster 23, Sector 671										
.		0	10.01.95	18:33	23					Dir
..		0	10.01.95	18:33	0					Dir
\$64DMODE	EXE	86021	17.12.95	9:03	4303	Arc				
\$64DDIAG	EXE	28023	29.09.94	15:35	4314	Arc				
\$64DDPMS	COM	3456	17.10.94	16:27	4318	Arc				
README	S3	6432	27.12.94	2:17	4319	Arc				
xONFIG	SYS	836	8.12.95	19:57	37133	Arc				
Unused directory entry										
Unused directory entry										
Unused directory entry										
Unused directory entry										
Unused directory entry										
Unused directory entry										
Unused directory entry										
Unused directory entry										
Cluster 23, Sector 672										
Unused directory entry										
Unused directory entry										
Sub-Directory										
C:\\$64D										
Cluster 23										
Offset 256, hex 100										

ОРис. 6.35. Удаленный файл и свободные элементы каталога

ОЕсли перейти в режим неформатированного просмотра, то можно убедиться, что свободные элементы каталога содержат нулевые значения. Если же после свободных элементов находятся какие-либо данные, существует очень большая вероятность того, что они записаны туда вирусом или системой защиты программ от несанкционированного копирования (если исследуемый каталог содержит такие программы).

ОЕсли каталог поврежден полностью или частично, ссылки на описанные в нем файлы будут потеряны. Если вы найдете тем или иным способом секторы, содержащие нужный вам файл, для которого разрушен дескриптор, пользуясь описанной ниже методикой вы сможете восстановить дескриптор и получить доступ к файлу.

ООбласть данных

ОВслед за корневым каталогом начинается область данных, которая простирается до конца логического диска (рис. 6.17). Область данных разбита на кластеры, причем нумерация кластеров начинается с числа 2. Кластеру с номером 2 соответствуют первые секторы области данных.

ОПриведем формулу, которая связывает номер кластера с номерами секторов, занимаемых им на логическом диске:

$$0SectNumber = DataStart + ((ClustNumber - 2) * ClustSize)$$

ОВ этой формуле использованы следующие обозначения:

0

0Переменная	0Описание
1SectNumber	1Номер первого сектора, распределенного кластеру с номером ClustNumber
2DataStart	2Начальный сектор области данных
3ClustNumber	3Номер кластера, для которого необходимо определить номер первого сектора
4ClustSize	4Количество секторов, занимаемых одним кластером

0Эта формула может вам пригодиться при ручном восстановлении файловой системы.

0Поиск и восстановление файлов

ОВ этом разделе мы приведем некоторые рекомендации, направленные на восстановление файлов, доступ к которым стал невозможен из-за вредоносного действия вирусов или в результате разрушения файловой системы по любой другой причине. В любом случае перед началом восстановительных работ следует провести полное исследование файловой системы с использованием методики, изложенной в предыдущей части этой главы.

ОНеобходимо также убедиться, что вы хорошо владеете структурой файловой системы и знаете форматы всех ее компонент, таких как таблица разделов, таблица логических дисков, таблица размещения файлов FAT и т. д. В тяжелых случаях мы рекомендуем обращаться к специалистам, например, из скорой компьютерной помощи АО “ДиалогНаука”.

ОМногие повреждения файловой системы можно восстановить в автоматическом режиме при помощи программы Norton Disk Doctor. Однако эта весьма неплохая программа в некоторых случаях не сможет оказать вам существенной помощи. Поэтому вы должны владеть хотя бы основными приемами ручного восстановления файловой системы.

ОЕсли в процессе исследования файловой системы вы обнаружили, что некоторые структуры оказались полностью разрушены (например, главная загрузочная запись с таблицей разделов, таблица логических дисков, каталоги и т. д.), еще не все потеряно. Многое можно восстановить с помощью таких программ, как Norton Disk Doctor или Norton Disk Editor.

ООсновная идея поиска потерянных файлов и структур данных заключается в том, что вы знаете (хотя бы приблизительно) их содержимое.

0Например, секторы, содержащие таблицу разделов, таблицу логических дисков и загрузочную запись имеют сигнатуру 0AA55h. Из предыдущих разделов этой главы вы знаете, что программы начальной загрузки содержат в своем теле текстовые строки, которые также можно использовать для поиска. В теле расширенного блока параметров BIOS Extended PBP имеются текстовые строки FAT12 или FAT16, которые также можно использовать для поиска.

0Если вы знаете характерные слова или последовательности байт, встречающиеся в потерянных файлах данных, их тоже можно использовать для восстановления.

0Секторы, содержащие дескрипторы каталогов, можно обнаружить, зная имена описанных в нем файлов.

0Поиск с помощью программы File Find

0Наиболее распространенное повреждение файловой системы возникает при внезапном отключении питания и заключается в появлении так называемых потерянных кластеров. Это повреждение также бывает следствием аппаратного сброса компьютера кнопкой Reset при работающей операционной системе Microsoft Windows.

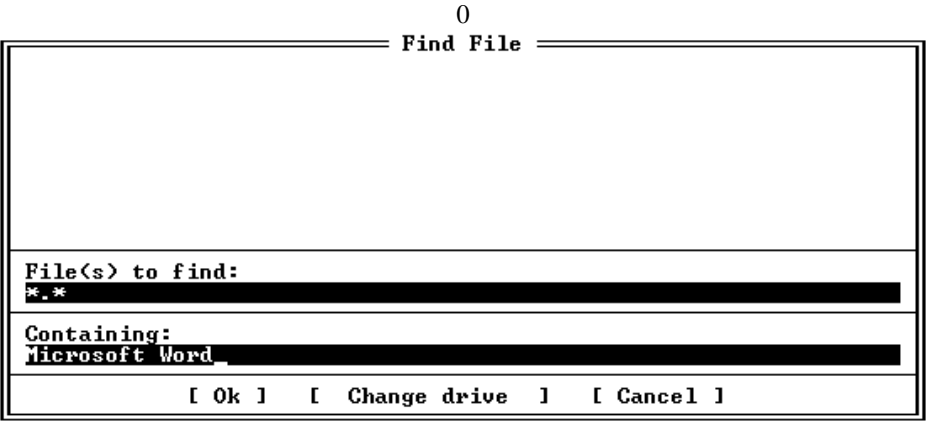
0Потерянные кластеры называются так потому, что на них нет ссылок ни в одном каталоге файловой системы. Например потому, что соответствующий каталог был просто уничтожен и, следовательно, ссылки на описанные в нем файлы исчезли.

0Чаше всего для ремонта повреждений такого рода пользователи применяют программу SCANDISK.EXE, входящую в состав операционной системы MS-DOS, или программу NDD.EXE из пакета Norton Utilities (программа Norton Disk Doctor).

0После восстановления файловой системы программой Norton Disk Doctor или SCANDISK.EXE на диске может образоваться громадное количество файлов со специфическим расширением имени (каждая программа восстановления использует свое имя), составленные из цепочек потерянных кластеров. Таких файлов в зависимости от серьезности повреждений файловой системы может быть очень много, до нескольких тысяч.

0Если после сбоя или вирусной атаки вы проверили диск одной из перечисленных выше программ, и в результате нужные вам файлы исчезли, существует большая вероятность того что они оказались среди восстановленных. Однако как их найти среди сотен и тысяч других?

0Проще всего это сделать, например, с помощью программы Find File, которую можно запустить из популярной оболочки Norton Commander при помощи комбинации клавиш <Alt+F7> (рис. 6.36).

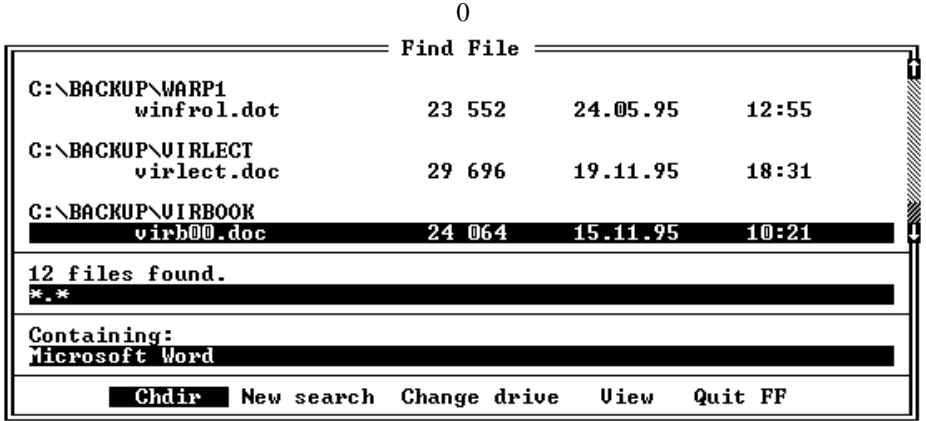


0Рис. 6.36. Поиск файлов по конте ксту при помощи программы Find File, запущенной из оболочки Norton Commander

0В поле File(s) to find вы должны задать шаблон для имени файла и расширения имени, например, *.nnd. Поиск будет выполняться только среди файлов, имя которых удовлетворяет указанному шаблону.

0Необходимо также в поле Containing указать шаблон для поиска, т. е. какую-либо текстовую строку, присутствующую в файле. Например, для того чтобы найти все файлы, созданные текстовым процессором Microsoft Word for Windows, вы можете указать шаблон Microsoft Word, а для того чтобы найти все файлы, подготовленные в среде процессора электронных таблиц Microsoft Excel, укажите шаблон Microsoft Excel.

0Список путей к найденным файлам отобразится в верхней части окна программы Find File (рис. 6.37).

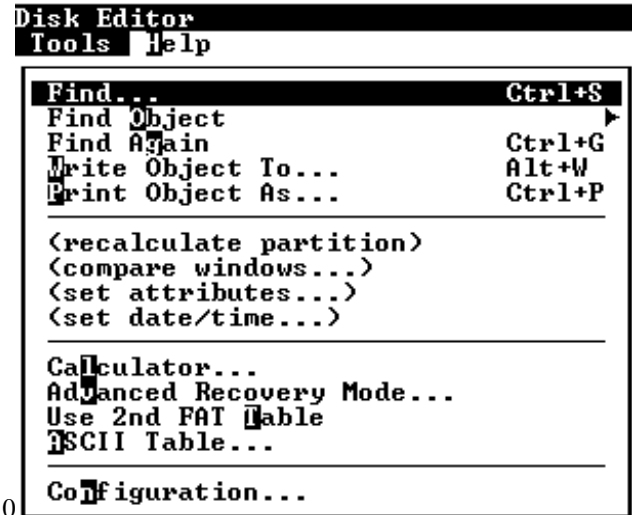


0Рис. 6.37. Программ а Find File нашла несколько файлов, содержащих указанный контекст

0В дальнейшем, если найденных файлов будет все еще очень много, вы можете переписать их в отдельный каталог и переименовать, а затем продолжить поиск, используя другие строки в качестве контекста.
0Описанную процедуру контекстного поиска вы можете использовать и для поиска в файлах документов изсестных вирусов, таких, например, как WinWord.Concept.

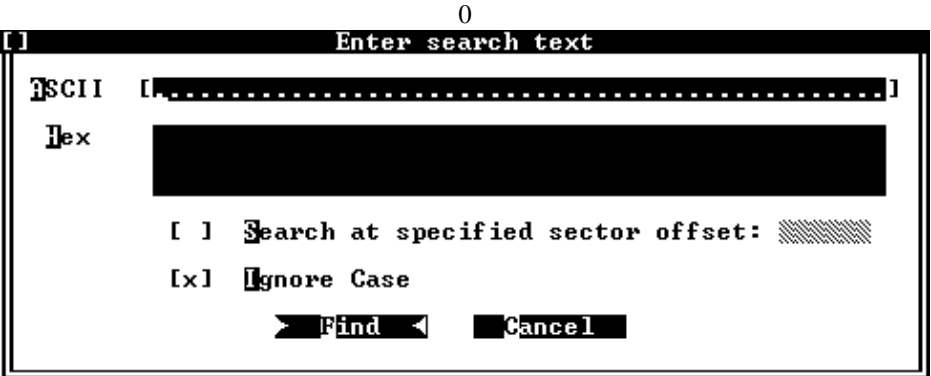
0Поиск с помощью программы DISKEDIT

0По сревнению с описанной в предыдущем разделе программой Find File программа DISKEDIT.EXE предоставляет намного больше возможностей для поиска файлов, а также различных структур файловой системы.
0Обратите внимание на меню Tools программы DISKEDIT.EXE (рис. 6.38).



0Рис. 6.38. Меню Tools программы DISKEDIT.EXE открывает доступ к набору инструмент ьных средств для работы с файло вой систе мой

0Если выбрать из этого меню строку Find, на экране появится диалоговая панель, показанная на рис. 6.39.



0Рис. 6.39. Диалоговая панель Enter search text, предоставляющая широкие возможности контекстн ого поиска

0С помощью этой диалоговой панели вы сможете выполнять контекстный поиск строк, заданных как смивольным, так и шестнадцатиричным представлением. Дополнительно можно указать смещение сектора и выбрать режим Ignore Case, при котором сравнение с образцом будет выполняться без учета строчных или прописных букв.
0Строка Find Object позволяет выполнить поиск различных структур файловой системы. Если выбрать эту строку, на экране появится меню второго уровня, показанное на рис. 6.40.



0Рис. 6.40. Меню, с помощью которого можно выполнить поиск служебных спр уктур файло вой систе мы

0Попробуйте все это в действии. Для этого откройте меню Object и выберите из него строку Physical Sector. Затем укажите самый первый сектор, расположенный на нулевой дорожке. Этот сектор должен содержать главную загрузочную запись MBR. Перейдите в режим неформатированного просмотра, выбрав из меню View строку as Hex.
0Теперь выберите из меню Tools строку Find Object и затем строку FAT. Программа DISKEDIT.EXE выполнит поиск первой копии таблицы размещения файлов FAT и отобразит ее дамп, выделив в этом дампе первые три байта, как это показано на рис. 6.41.

0

Disk Editor																			
Object	Edit	Link	View	Info	Tools	Help													
Physical Sector: Cyl 0, Side 1, Sector 2																			
00000000:	F8	FF	FF	FF	FF	FF	04	00	-	05	00	06	00	07	00	FF	FF	0	♦.♦.♦.♦.
00000010:	09	00	0A	00	0B	00	0C	00	-	FF	FF	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000020:	5F	00	1C	00	FF	FF	FF	FF	-	FF	FF	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000030:	FF	FF	FF	FF	FF	FF	FF	FF	-	B9	07	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000040:	FF	FF	FF	FF	FF	FF	FF	FF	-	FF	FF	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000050:	FF	FF	FF	FF	FF	FF	FF	FF	-	FF	FF	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000060:	FF	FF	FF	FF	FF	FF	FF	FF	-	FF	FF	FF	FF	FF	FF	FF	FF	0	0.0.0.0.
00000070:	39	00	3A	00	3B	00	3C	00	-	3D	00	3E	00	3F	00	40	00	0	9.:.:.<.=.>.?.@.
00000080:	41	00	42	00	43	00	44	00	-	FF	FF	FF	FF	FF	FF	FF	FF	0	A.B.C.D.
00000090:	FF	FF	FF	FF	FF	FF	4C	00	-	4D	00	4E	00	4F	00	50	00	0	L.M.N.O.P.
000000A0:	51	00	52	00	53	00	54	00	-	55	00	56	00	57	00	58	00	0	Q.R.S.T.U.V.W.X.
000000B0:	59	00	5A	00	5B	00	5C	00	-	5D	00	FF	FF	FF	FF	61	00	0	Y.Z.[.\]. a.
000000C0:	FF	FF	63	00	FF	FF	66	00	-	FF	FF	FF	FF	67	00	69	00	0	c. f. g.i.
000000D0:	FF	FF	CC	00	FF	FF	6C	00	-	6D	00	6E	00	6F	00	70	00	0	h. l.m.n.o.p.
000000E0:	71	00	72	00	73	00	74	00	-	FF	FF	76	00	77	00	78	00	0	q.r.s.t. u.v.w.x.
000000F0:	79	00	7A	00	7B	00	7C	00	-	7D	00	7E	00	7F	00	80	00	0	y.z.<[.]>~.a.A.
00000100:	81	00	82	00	83	00	84	00	-	85	00	86	00	87	00	88	00	0	Б.В.Г.Д.Е.Ж.З.И.
00000110:	89	00	8A	00	8B	00	8C	00	-	8D	00	8E	00	8F	00	90	00	0	Й.К.Л.М.Н.О.П.Р.
00000120:	91	00	92	00	93	00	94	00	-	95	00	96	00	97	00	98	00	0	С.Т.У.Ф.Х.Ц.Ч.Ш.
00000130:	99	00	9A	00	9B	00	FF	FF	-	9D	00	9E	00	9F	00	A0	00	0	Щ.Ъ.Ы. Э.Ю.Я.а.
Sector 64 of 1 062 431																Cyl 0, Side 1, Sector 2			
Hard Disk 1																Offset 0, hex 0			

Рис. 6.41. Программа DISKEDIT.EXE нашла первую копию таблицы размещения файла в FAT

Если теперь сместить текстовый курсор вниз или нажать клавишу <PgDn>, а затем выбрать из меню Tools/Find Object строку FAT еще раз, будет найдена вторая копия таблицы размещения файлов FAT.

Учтите, что поиск таблиц FAT в данном случае сводится к поиску последовательности байт F8 FF FF, поэтому выполнив поиск в третий раз, вы сможете найти еще одну, ненастоящую “таблицу FAT”. Дело в том, что наверняка на диске найдется какой-нибудь файл, содержащий указанную выше последовательность байт, поэтому будьте внимательны.

Если взглянув на главную загрузочную запись вы увидели, что таблица разделов разрушена или зашифрована, можно выполнить контекстный поиск секторов загрузочных записей, содержащих блоки параметров BIOS BPB. Проще всего это сделать, если после просмотра главной загрузочной записи по ее физическому адресу и перехода к следующему сектору диска выбрать из меню Tools/Find Object строку Partition/Boot.

Программа DISKEDIT.EXE найдет сектор, содержащий в конце последовательность байт 55 AA, которая соответствует сигнатуре загрузочного сектора 0AA55h (рис. 6.42).

0

Disk Editor																			
Object	Edit	Link	View	Info	Tools	Help													
000000D0:	3B	FB	72	E5	EB	D7	2B	C9	-	B8	D8	7D	87	46	3E	3C	D8	0	0.0.0.0.
000000E0:	75	99	BE	80	7D	AC	98	03	-	F0	AC	84	C0	74	17	3C	FF	0	0.0.0.0.
000000F0:	74	09	B4	0E	BB	07	00	CD	-	10	EB	EE	BE	83	7D	EB	E5	0	0.0.0.0.
00000100:	BE	81	7D	EB	E0	33	C0	CD	-	16	5E	1F	8F	04	8F	44	02	0	0.0.0.0.
00000110:	CD	19	BE	82	7D	8B	7D	0F	-	83	FF	02	72	C8	8B	C7	48	0	0.0.0.0.
00000120:	48	8A	4E	0D	F7	E1	03	46	-	FC	13	56	FE	BB	00	07	53	0	0.0.0.0.
00000130:	B1	04	E8	16	00	5B	72	C8	-	81	3F	4D	5A	75	A7	81	BF	0	0.0.0.0.
00000140:	00	02	42	4A	75	9F	EA	00	-	02	70	00	50	52	51	91	92	0	0.0.0.0.
00000150:	33	D2	F7	76	18	91	F7	76	-	18	42	87	CA	F7	76	1A	8A	0	0.0.0.0.
00000160:	F2	8A	56	24	8A	E8	D0	CC	-	D0	CC	0A	CC	B8	01	02	CD	0	0.0.0.0.
00000170:	13	59	5A	58	72	09	40	75	-	01	42	03	5E	0B	E2	CC	C3	0	0.0.0.0.
00000180:	03	18	01	27	0D	0A	49	6E	-	76	61	6C	69	64	20	73	79	0	0.0.0.0.
00000190:	73	74	65	6D	20	64	69	73	-	6B	FF	0D	0A	44	69	73	6B	0	0.0.0.0.
000001A0:	20	49	2F	4F	20	65	72	72	-	6F	72	FF	0D	0A	52	65	70	0	0.0.0.0.
000001B0:	6C	61	63	65	20	74	68	65	-	20	64	69	73	6B	2C	20	61	0	0.0.0.0.
000001C0:	6E	64	20	74	68	65	6E	20	-	70	72	65	73	73	20	61	6E	0	0.0.0.0.
000001D0:	79	20	6B	65	79	0D	0A	00	-	49	4F	20	20	20	20	20	20	0	0.0.0.0.
000001E0:	53	59	53	4D	53	44	4F	53	-	20	20	20	53	59	53	80	01	0	0.0.0.0.
000001F0:	00	57	49	4E	42	4F	4F	54	-	20	53	59	53	00	00	55	AA	0	0.0.0.0.
Physical Sector: Cyl 0, Side 1, Sector 2																			
00000000:	F8	FF	FF	FF	FF	FF	04	00	-	05	00	06	00	07	00	FF	FF	0	♦.♦.♦.♦.
Sector 63 of 1 062 431 Cyl 0, Side 1, Sector 1																			
Hard Disk 1 Offset 222, hex DE																			

Рис. 6.42. Найден загрузочный сектор

После того как вы нашли загрузочный сектор, его физический адрес можно вручную подставить в таблицу разделов, отредактировав ее программой DISKEDIT.EXE. О том как выполнить редактирование, вы можете узнать из документации, которая поставляется с набором утилит Нортон.

Так как структура разделов диска в процессе эксплуатации последнего может многократно изменяться, не исключено что вы найдете слишком много загрузочных секторов. Некоторые из них принадлежали старым разделам и не были уничтожены при изменении структуры разделов, некоторые вообще могут принадлежать другим операционным системам. В любом случае проверяйте расположение найденного загрузочного сектора относительно других найденных вами логических структур файловой системы. Например, вы можете использовать для “опознания” тот факт, что сразу после загрузочного сектора должна следовать таблица размещения файлов. Так как в процессе поиска программа DISKEDIT.EXE проверяет только последние два байта сектора, возможны ложные срабатывания. На рис. 6.43 показана как раз такая ситуация.

0

Disk Editor																									
Object	Edit	Link	View	Info	Tools	Help																			
00000120:	35	4C	A4	00	A8	81	A4	B1	-	45	D4	61	DB	0F	50	60	BC	51	Д.иБд	Е	а	хР	Д		
00000130:	1A	E2	F9	FC	25	89	2B	B0	-	14	A2	9B	4E	CF	17	3A	D0	+	Н	В	Т	Б	Н		
00000140:	94	D3	51	65	D4	05	A1	FB	-	E7	88	00	26	64	93	48	7C	Ф	Q	е	Б	с	Ч		
00000150:	77	63	5D	B6	60	D4	10	92	-	01	47	4E	3A	B7	39	B7	36	w	c	I		4	T		
00000160:	34	B2	9A	45	04	4E	99	B0	-	CD	A1	E5	44	A9	55	2B	AB	4	Б	Е	Н	И	с		
00000170:	89	35	58	CA	DE	2E	62	76	-	35	26	68	AB	AF	DB	29	E7	И	5	Х		б	Т		
00000180:	31	1B	6D	30	55	1F	4F	94	-	06	20	A1	B0	99	64	A0	C5	1	+	м	О	У	Ф		
00000190:	C8	DE	94	61	43	87	AE	18	-	05	CC	22	90	35	69	6B	FE		0	a	C	3	т		
000001A0:	20	42	C4	E9	78	D9	E5	16	-	32	28	56	3D	8C	A8	8A	DD	B	-	ш	х	2	У		
000001B0:	3F	45	1D	52	8B	82	C4	45	-	AF	E8	25	2A	81	46	BE	FE	?	E	+R	Л	В	Д		
000001C0:	35	97	32	3F	88	84	22	6F	-	C4	57	1B	9E	AF	AB	CB	76	5	4	?	И	Д	Т		
000001D0:	B2	CE	D6	6B	32	5C	5C	9E	-	E7	BF	B8	07	83	61	A6	E1		h	k	2	\\	Т		
000001E0:	B5	D1	65	19	9F	4E	89	85	-	B9	1A	C4	D5	C9	32	5A	75		т	e	Л	В	Д		
000001F0:	32	7D	80	03	53	1E	E3	07	-	22	BE	5A	EF	78	E0	55	AA	2	+	A	*S		Д		
Physical Sector: Cyl 178, Side 25, Sector 33																									
00000000:	28	98	A0	BF	04	7F	61	3D	-	8A	89	9E	E4	8F	07	4C	02	<		a	γ		Л		
00000010:	4D	17	F4	F4	A5	AE	73	58	-	90	0A	45	DF	95	AF	0E	1A	M		I	e		Л		
00000020:	90	EA	D4	A5	4B	BA	18	A6	-	87	05	1A	54	62	56	FE	41	P		b	e		Л		
00000030:	78	C5	AA	DA	01	86	E2	18	-	D2	73	C4	5D	F4	17	A1	A8	х		т	8		Л		
00000040:	83	3D	D1	38	BA	3B	AE	2C	-	B7	DD	23	12	E0	2E	5E	15		т	8		Л			
00000050:	6A	19	E3	5A	2C	EA	7F	5D	-	CF	3A	0A	AC	5C	79	54	04		γ	Z		Л			
Sector 360 455 of 1 062 431													Cyl 178, Side 25, Sector 33												
Hard Disk 1													Offset 94, hex 5E												

Орис. 6.43. При поиске загрузочного сектора найден сектор, содержащий нужную сигнатуру, который однако, не является загрузочным

Нетрудно заметить, что вслед за найденным располагается сектор, содержащее которого мало похоже на таблицу размещения файлов.

Теперь займемся поиском каталогов, на которые нет ссылок из других каталогов (т.е. потерянных каталогов).

Для поиска вы можете воспользоваться строкой Subdirectory меню Tools/Find Object. Программа DISKEDIT.EXE просматривает секторы диска в поисках такого, в начале которого находится последовательность байт 2E 20 20 20 20 20 20 20 20 20 20 (рис. 6.44). Эта последовательность соответствует дескриптору, который содержит ссылку каталога на себя самого.

0

Disk Editor																							
Object	Edit	Mink	View	Info	Tools	Help																	
Physical Sector: Cyl 179, Side 6, Sector 53																							
00000000:	2E	20	20	20	20	20	20	20	-	20	20	20	10	00	00	00	00	00	00	00	00	00	00
00000010:	00	00	79	1F	00	00	64	9D	-	79	1F	1E	58	00	00	00	00	00	00	00	00	00	00
00000020:	2E	2E	20	20	20	20	20	20	-	20	20	20	10	00	00	00	00	00	00	00	00	00	00
00000030:	00	00	79	1F	00	00	64	9D	-	79	1F	CB	12	00	00	00	00	00	00	00	00	00	00
00000040:	4C	49	43	45	4E	53	45	20	-	54	58	54	20	00	00	00	00	00	00	00	00	00	00
00000050:	00	00	79	1F	00	00	40	4E	-	18	1F	DE	3B	7A	32	00	00	00	00	00	00	00	00
00000060:	48	59	50	45	52	54	52	4D	-	43	4E	54	20	00	00	00	00	00	00	00	00	00	00
00000070:	00	00	79	1F	00	00	40	4E	-	18	1F	73	5B	8E	03	00	00	00	00	00	00	00	00
00000080:	4D	53	50	41	49	4E	54	20	-	43	4E	54	20	00	00	00	00	00	00	00	00	00	00
00000090:	00	00	79	1F	00	00	40	4E	-	18	1F	74	5B	BA	07	00	00	00	00	00	00	00	00
000000A0:	50	41	43	4B	41	47	45	52	-	43	4E	54	20	00	00	00	00	00	00	00	00	00	00
000000B0:	00	00	79	1F	00	00	40	4E	-	18	1F	75	5B	AC	03	00	00	00	00	00	00	00	00
000000C0:	48	59	50	45	52	54	52	4D	-	48	4C	50	20	00	00	00	00	00	00	00	00	00	00
000000D0:	00	00	79	1F	00	00	40	4E	-	18	1F	1D	1A	E1	53	00	00	00	00	00	00	00	00
000000E0:	4D	53	50	41	49	4E	54	20	-	48	4C	50	20	00	00	00	00	00	00	00	00	00	00
000000F0:	00	00	79	1F	00	00	40	4E	-	18	1F	21	1A	64	AA	00	00	00	00	00	00	00	00
00000100:	50	41	43	4B	41	47	45	52	-	48	4C	50	20	00	00	00	00	00	00	00	00	00	00
00000110:	00	00	79	1F	00	00	40	4E	-	18	1F	27	1A	E9	5B	00	00	00	00	00	00	00	00
00000120:	44	49	41	4C	45	52	20	20	-	43	4E	54	20	00	00	00	00	00	00	00	00	00	00
00000130:	00	00	79	1F	00	00	40	4E	-	18	1F	3A	1A	28	02	00	00	00	00	00	00	00	00
Sector 361 294 of 1 062 431												Cyl 179, Side 6, Sector 53											
Hard Disk 1												Offset 0, hex 0											

Орис. 6.44. Найден сектор, принадлежащий каталогу

Нажимая комбинацию клавиш <Control+G>, вы можете продолжить поиск нужного вам каталога, пока не найдете тот, что содержит интересующие вас файлы. Можно выполнять поиск и по имени файла, если вы его знаете.

Как только нужный каталог найден, вы должны записать физический адрес соответствующего сектора диска и найти либо вычислить номер кластера, соответствующего каталогу.

Для поиска номера кластера, соответствующего найденному каталогу, перейдите в режим форматированного просмотра каталога, выбрав из меню View строку as Directory. Затем из меню Link выберите стоку Cluster chain (fat). На экране появится содержимое таблицы FAT в режиме форматированного просмотра, при этом искомый номер кластера будет выделен.

Зная номер кластера потерянного каталога, вы можете создать новый дескриптор каталога, например, в корневом каталоге диска, и сделать в этом дескрипторе ссылку на найденный каталог. После этого потерянный каталог вновь станет доступным.

Аналогично можно вручную восстановить ссылки на потерянные файлы и даже собрать файлы из отдельных кластеров.

Можно предложить следующий алгоритм восстановления файла:

выполнить контекстный поиск секторов файла с помощью строки Files из меню Tools, а также последовательным просмотром секторов диска;

определить номер кластеров, соответствующего найденным секторам, пользуясь приведенной выше формулой или средствами программы DISKEDIT.EXE;

восстановить цепочку номеров кластеров для файла в таблице размещения файлов FAT, отметив в ней последний кластер значением OFFFFh;

создать в любом каталоге (например, в корневом) дескриптор, который описывает файл, указав в нем ссылку на первый кластер восстановленного файла, а также размер этого файла.

Если вы восстановили файл документа, созданный текстовым процессором Microsoft Word for Windows или процессором таблиц Microsoft Excel, загрузите его в соответствующее приложение и затем сохраните его под другим именем. При этом будет восстановлена правильная длина файла.

Простой текстовый файл можно загрузить в текстовый редактор и “отрезать” лишние данные в конце файла. Затем сохраните файл под другим именем.

Особенности файловой системы Microsoft Windows 95

Восстанавливая файловую систему компьютера, на котором установлена операционная система Microsoft Windows 95, следует соблюдать осторожность, так как структура каталогов в ней отличается от структуры каталогов в MS-DOS.

Как вы, возможно, знаете, пользователи Microsoft Windows 95 не скованы ограничениями на длину имен файлов и каталогов. И хотя такое ограничение существует (255 символов), оно не имеет существенного значения.

Создавая новую операционную систему, программисты из Microsoft нашли остроумное решение проблемы совместимости с программами MS-DOS, использующими имена в “формате 8.3” (8 символов - имя файла или каталога, 3 - расширение имени).

Это решение заключается в том, что в каталогах наряду с обычными дескрипторами располагаются дескрипторы специального вида, количество которых зависит от длины имени файла или каталога. В этих дескрипторах и хранится длинное имя. Специально для программ MS-DOS создается обычный дескриптор, содержащий альтернативное имя, отвечающее стандартам MS-DOS.

Взгляните на рис. 6.45. На этом рисунке показана структура каталога, созданного в файловой системе Microsoft Windows 95, причем просмотр выполнялся программой DISKEDIT.EXE из пакета Norton Utilities версии 8.0, предназначенной для MS-DOS.

Disk Editor											
Object		Edit	Link	View	Info	Tools	Help				
Name	Ext	Size	Date	Time	Cluster	Arc	R/O	Sys	Hid	Dir	Vol
Cluster 32 226, Sector 515 919											
..		0	19.12.95	15:40	32226					Dir	
AS.y.s.t	.e.	4294967295	31.15.07	31:63	8282					Dir	
SYSTEM		0	19.12.95	15:40	0		R/O	Sys	Hid		Vol
RESCUE	EXE	358482	5.07.95	9:00	32227					Dir	
DISKS	INF	19426	5.07.95	14:35	32437	Arc					
END-USER	TXI	5813	5.07.95	9:00	32283	Arc					
xERSION	DLL	6144	5.07.95	9:00	32287	Arc					
SIWFMOD	EXE	5088	5.07.95	9:00	32288	Arc					
Ar.e.a.d	.n.	4294967295	0.00.80	0:03	32289	Arc					
README	TXI	12502	5.07.95	9:00	0		R/O	Sys	Hid		Vol
SUNZIP32	DLL	43520	5.07.95	9:00	32292						
ai.n.s.t	.a.	4294901760	6.03.80	0:03	32298	Arc					
INSTALL	INF	39246	5.07.95	9:00	0		R/O	Sys	Hid		Vol
SIWDL32	DLL	71168	5.07.95	9:00	32304						
As.e.t.u	.p.	4294967295	31.15.07	0:00	32322	Arc					
Cluster 32 226, Sector 515 920					0		R/O	Sys	Hid		Vol
SETUP	EXE	42304	5.07.95	9:00							
INST32	EXE	354304	5.07.95	9:00	32331						
Sub-Directory					32393	Arc					
C:\PROGRA~1\NORTON~1											
										Cluster 32 226	
										Offset 0. hex 0	

Рис. 6.45. Просмотр структуры каталогов программой DISKEDIT.EXE, предназначенной для работы в среде MS-DOS

Обратите внимание на дескрипторы, расположенный над дескрипторами каталога SYSTEM, дескрипторами файлов README.TXT, INSTALL.INF и SETUP.EXE. Это и есть специальные дескрипторы, хранящие информацию о длинных именах в кодировке UNICODE (в этой кодировке каждый символ представлен двумя байтами).

Для того чтобы специальные дескрипторы не мешали работе программ MS-DOS, в них установлены атрибуты Read Only, System, Hidden и Volume Label. Элементы каталога с таким экзотическим набором игнорируются всеми обычными программами MS-DOS.

Если просматривать содержимое каталога программой DISKEDIT.EXE из пакета Norton Utilities для Microsoft Windows 95, специальные дескрипторы будут отображаться в форматированном виде, доступном для исследования (рис. 6.46).

Disk Editor													
Object	Edit	Link	View	Info	Tools	Help	More>						
Name	.Ext	ID	Size	Date	Time	Cluster	76	A	R	S	H	D	V
Cluster 32,226, Sector 515,919													
.		Dir	0	12-19-95	3:40 pm	32,226	-	-	-	-	D	-	
..		Dir	0	12-19-95	3:40 pm	8,282	-	-	-	-	D	-	
System		LFN				0	-	R	S	H	-	V	
SYSTEM		Dir	0	12-19-95	3:40 pm	32,227	-	-	-	-	D	-	
RESCUE	EXE	File	358482	7-05-95	9:00 am	32,437	A	-	-	-	-	-	
DISKS	INF	File	19426	7-05-95	2:35 pm	32,283	A	-	-	-	-	-	
END-USER	TXT	File	5813	7-05-95	9:00 am	32,287	A	-	-	-	-	-	
ERSION	DLL	Erased	6144	7-05-95	9:00 am	32,288	A	-	-	-	-	-	
SIWFMOD	EXE	File	5088	7-05-95	9:00 am	32,289	A	-	-	-	-	-	
readme.txt		LFN				0	-	R	S	H	-	V	
README	TXT	File	12502	7-05-95	9:00 am	32,292	-	-	-	-	-	-	
SUNZIP32	DLL	File	43520	7-05-95	9:00 am	32,298	A	-	-	-	-	-	
install.inf		LFN				0	-	R	S	H	-	V	
INSTALL	INF	File	39246	7-05-95	9:00 am	32,304	-	-	-	-	-	-	
SIWDDL32	DLL	File	71168	7-05-95	9:00 am	32,322	A	-	-	-	-	-	
setup.exe		LFN				0	-	R	S	H	-	V	
Cluster 32,226, Sector 515,920													
SETUP	EXE	File	42304	7-05-95	9:00 am	32,331	-	-	-	-	-	-	
INST32	EXE	File	354304	7-05-95	9:00 am	32,393	A	-	-	-	-	-	
Sub-Directory							Cluster 32,226						
C:\PROGRA~1\NORTON~1							Offset 1, hex 1						

Рис. 6.46. Просмотр структуры каталогов новой версии программы DISKEDIT.EXE, предназначенной для Microsoft Windows 95

Специальный дескриптор отмечается новой версией программы DISKEDIT.EXE как LFN (Long File Name) и ссылается на кластер с номером 0. Настоящий номер первого кластера, распределенного файлу или каталогу, находится в стандартном дескрипторе, расположенном непосредственно вслед за специальным. Например, каталог с именем System отмечен в стандартном дескрипторе как SYSTEM и расположен в кластере с номером 32227.

Если имя файла или каталога превышает 8 символов, стандартный дескриптор, расположенный после специальных, содержит алиасное имя, состоящее из начальных символов имени, символа “~” (тильда) и десятичного числа. Этот дескриптор называется алиасным.

В главном меню программы DISKEDIT.EXE появилась новая строка More, выбрав которую, вы сможете просмотреть или отредактировать остальные поля специальных дескрипторов (рис. 6.47 и 6.48).

Disk Editor											
Object	Edit	Link	View	Info	Tools	Help	<More	More>			
Name	.Ext	ID	NT	Create Date	Create Time	Accessed	EA				
Cluster 32,226, Sector 515,919											
.		Dir	0	12-19-95	3:40.118 pm	12-19-95	0				
..		Dir	0	12-19-95	3:40.118 pm	12-19-95	0				
System		LFN									
SYSTEM		Dir	0	12-19-95	3:40.118 pm	12-19-95	0				
RESCUE	EXE	File	0	7-05-95	9:00.000 am	12-20-95	0				
DISKS	INF	File	0	12-19-95	3:40.002 pm	12-19-95	0				
END-USER	TXT	File	0	12-19-95	3:40.127 pm	12-19-95	0				
ERSION	DLL	Erased	0	12-19-95	3:40.079 pm	12-19-95	0				
SIWFMOD	EXE	File	0	12-19-95	3:40.157 pm	12-20-95	0				
readme.txt		LFN									
README	TXT	File	0	12-19-95	3:40.164 pm	12-19-95	0				
SUNZIP32	DLL	File	0	12-19-95	3:40.037 pm	12-19-95	0				
install.inf		LFN									
INSTALL	INF	File	0	12-19-95	3:40.189 pm	12-19-95	0				
SIWDDL32	DLL	File	0	12-19-95	3:40.003 pm	12-19-95	0				
setup.exe		LFN									
Cluster 32,226, Sector 515,920											
SETUP	EXE	File	0	12-19-95	3:40.079 pm	12-20-95	0				
INST32	EXE	File	0	12-19-95	3:40.111 pm	12-20-95	0				
Sub-Directory						Cluster 32,226					
C:\PROGRA~1\NORTON~1						Offset 1, hex 1					

Рис. 6.47. Просмотр остальных полей специальных дескрипторов

Disk Editor											
Object	Edit	Link	View	Info	Tools	Help	<More				
Name	.Ext	ID	Ordinal	Last?	Type	Checksum	Linked				
Cluster 32,226, Sector 515,919											
.	Dir										
..	Dir										
System	LFN		1	Yes	0	9A	Yes				
SYSTEM	Dir										
RESCUE	EXE	File									
DISKS	INF	File									
END-USER	TXT	File									
ERSION	DLL	Erased									
SIWFMOD	EXE	File									
readme.txt	LFN		1	Yes	0	73	Yes				
README	TXT	File									
SUNZIP32	DLL	File									
install.inf	LFN		1	Yes	0	D4	Yes				
INSTALL	INF	File									
SIWDDL32	DLL	File									
setup.exe	LFN		1	Yes	0	3E	Yes				
Cluster 32,226, Sector 515,920											
SETUP	EXE	File									
INST32	EXE	File									
Sub-Directory							Cluster 32,226				
C:\PROGRA~1\NORTON~1							Offset 1, hex 1				

Рис. 6.48. Просмотр остальных полей специальных дескрипторов (продолжение)

Например, дата и время создания файла находятся, соответственно, в полях Create Date и Create Time. Дополнительно операционная система Microsoft Windows 95 фиксирует дату последнего обращения к файлу. Эту дату вы можете увидеть в поле Accessed.

Поле EA содержит признак расширенных атрибутов и имеет нулевое значение для стандартных атрибутов.

Если имя настолько длинное, что не помещается в одном специальном дескрипторе, создается несколько таких дескрипторов, расположенных друг за другом. Следом за ними идет алиасный дескриптор. В поле Ordinal находится порядковый номер специального дескриптора. Для последнего специального дескриптора в поле Last? находится отметка Yes.

Что же касается таблицы размещения файлов FAT, то хотя в операционной системе Microsoft Windows 95 она и называется виртуальной таблицей размещения файлов VFAT, ее формат остался прежним. Это сделано для совместимости с программами MS-DOS. Сохранились форматы и других логических блоков файловой системы, таких как таблица разделов диска, таблица логических дисков, загрузочная запись и расширенный блок параметров BIOS Extended BPB.

Для восстановления файловой системы Microsoft Windows 95 нельзя использовать старые версии пакета Norton Utilities. Вы должны выполнять автоматическое восстановление либо приложением ScanDisk, которое входит в состав этой операционной системы, либо программой NDD.EXE из пакета Norton Utilities для Microsoft Windows 95. Полуавтоматическое восстановление можно выполнять только новой версией программы DISKEDIT.EXE для Microsoft Windows 95, но не в коем случае не старой, которая ничего не знает о специальных дескрипторах.

7 АХИЛЛЕСОВА ПЯТА ОПЕРАЦИОННОЙ СИСТЕМЫ

В этой главе мы попытаемся сделать анализ устойчивости различных операционных систем к “нашествию” вирусов, чтобы помочь системным администраторам и обычным пользователям выбрать наиболее защищенную от вирусов операционную систему.

Не секрет, что надежность многих современных операционных систем оставляет желать лучшего. Это можно сказать и про устойчивость ко всякого рода внешним воздействиям, таким, например, как попытки несанкционированного доступа или вирусные атаки. Причина этого лежит в неполном использовании возможности аппаратуры, в необходимости обеспечения совместимости новых операционных систем со старым программным обеспечением, а также, вероятно и в том, что при разработке операционных систем для персональных компьютеров вопросам защищенности не уделялось достаточно внимания.

Наиболее беззащитной является операционная система MS-DOS и все совместимые с ней, такие как Novell DOS, IBM DOS и т. д. Основная причина заключается в том, что эта операционная система использует реальный режим работы процессора и предоставляет

запущенным программам полный и бесконтрольный доступ ко всем системным ресурсам компьютера (в том числе и к модулям самой операционной системы).

Операционная система Microsoft Windows версии 3.1 (а также Microsoft Windows for Workgroups версии 3.11) запускается из MS-DOS. Хотя она использует защищенный режим работы процессора, ее устойчивость к вирусным воздействиям также невысока.

С точки зрения полноты использования возможностей защищенного режима одно из первых мест принадлежит такой операционной системе, как IBM OS/2. Если системный администратор (или пользователь) запретит запуск в ее среде программ MS-DOS (а также приложений Windows), эта операционная система будет работать очень стабильно. Однако файловая система рабочей станции OS/2 может оказаться баззащитной перед нашествием вирусов. Тем не менее создание вируса для OS/2 - непростая задача. Возможно поэтому нигде в мире не наблюдается лавинообразного роста вирусов, ориентированных на OS/2, что говорит в пользу этой операционной системы.

Операционная система Microsoft Windows 95 может подвергнуться нападению со стороны вирусов, предназначенных для DOS, так как из соображений совместимости она предоставляет таким программам полный доступ к файловой системе и стартует из среды MS-DOS версии 7.0. Последний факт нигде особенно не афишируется, однако на диске C: по-прежнему существуют файлы AUTOEXEC.BAT и CONFIG.SYS, которые не изменили своего назначения. Следовательно, для вируса есть возможность остаться резидентным в памяти до загрузки Windows 95.

Такая операционная система, как Novell NetWare, заслуживает всяческих похвал и потому широко распространена. Ее файловая система хорошо защищена и сама по себе может выдержать вирусную атаку. Однако вирус не обязательно будет пытаться обойти защиту Novell NetWare (что весьма и весьма непросто). Вместо этого он может, например, подсмотреть пароль системного администратора на рабочей станции и таким образом получить неограниченные привилегии. К счастью, работоспособных вирусов подобного типа не так много.

В операционной системе Microsoft Windows NT предусмотрены специальные меры, исключающие возможность выманить у пользователя его пароль. Файловая система NTFS, которая используется в Microsoft Windows NT, содержит мощные встроенные средства защиты от несанкционированного доступа. На сегодняшний день нам не известен ни один вирус, специально разработанный для этой операционной системы.

Операционная система MS-DOS

Подавляющее большинство вирусов было создано для операционной системы MS-DOS, которая и до сегодняшнего дня является наиболее популярной. Популярность MS-DOS и ее “доверчивость” к программам способствуют появлению все новых и новых вирусов.

В этом разделе мы расскажем вам о некоторых уязвимых местах операционной системы MS-DOS, которые активно используются вирусами для своего закрепления и

распространения, а также для того чтобы скрыть свое существование (как это делают стелс-вирусы).

Вы увидите, что вирус в MS-DOS имеет полный доступ к любому байту оперативной памяти и к любому сектору любого диска. Поистине трудно найти более беззащитную операционную систему, чем MS-DOS.

Использование реального режима работы процессора

Как мы уже говорили, использование реального режима работы процессора значительно ухудшает защищенность и стабильность операционной системы MS-DOS.

Напомним, как выполняется адресация памяти в реальном режиме (рис. 7.1).

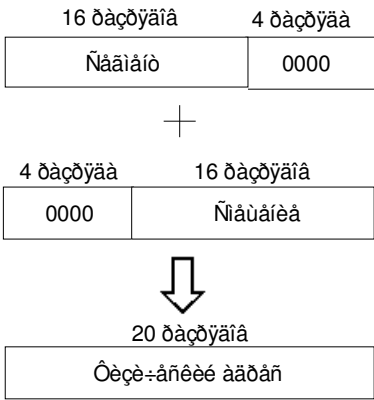


Рис. 7.1. Адресация памяти в реальном режиме работы процессора

Программы (как системные, так и программы, запускаемые пользователем) работают с адресом, состоящим из двух 16-разрядных компонент, которые называются сегментом и смещением.

Для вычисления физического адреса памяти (который попадает на системную шину компьютера) значение сегмента сдвигается влево на четыре бита и складывается со значением смещения, расширенного до 20 разрядов. Задавая различные значения для компонент адреса, любая программа может получить доступ к любой области памяти (в границах первого Мбайта адресного пространства).

В результате программы, которые запускают пользователи, а также, разумеется, вирусы, могут изменить любую область оперативной памяти, распределенную операционной системе MS-DOS или другой программе, обычной или резидентной. Поэтому вирусу не составляет никакого труда встроить себя, например, в цепочку драйверов устройств, перехватить программное или аппаратное прерывание, или сделать что-нибудь еще.

Другой недостаток реального режима работы процессора заключается в том, что программы могут бесконтрольно обращаться к портам периферийных устройств.

Изменение вирусами структуры памяти

Система управления памятью, встроенная в MS-DOS, является чисто символической, так как ее нормальная работа зависит от того, будут ли программы выполнять заранее оговоренные соглашения, или нет. Однако ничто не мешает программе стать “нарушителем”, полностью разрушив всю операционную систему или внося в нее те или иные “незаконные” изменения.

Например, программа может запросить у MS-DOS блок памяти размером 10 Кбайт. В ответ соответствующая функция MS-DOS предоставит программе сегментный адрес выделенного блока. Используя полученный адрес как указатель на массив, программа может записать в этот массив не 10, а 20 или 30 Кбайт данных, и ничто не мешает ей в этом, так как MS-DOS не будет проверять значение указателя на предмет выхода за пределы массива.

Какие же изменения могут внести вирусы в структуру памяти?

Вспомним, как распределен первый мегабайт оперативной памяти в операционной системе MS-DOS:

Диапазон адресов	Описание
0000h:0000h	Векторы прерываний
0000h:0400h	Область данных BIOS
0000h:0500h	Область данных MS-DOS
xxxx:0000h	Область программ MS-DOS. Здесь располагаются обработчики прерываний MS-DOS, буферы, внутренние структуры данных MS-DOS, встроенные и загружаемые драйверы устройств
xxxx:0000h	Резидентная часть командного процессора COMMAND.COM
xxxx:0000h	Резидентные программы (если загружены)
xxxx:0000h	Запущенные прикладные программы
xxxx:0000h	Транзитная часть командного процессора COMMAND.COM
0A000h:0000h	Память видеоадаптера EGA
0B000h:0000h	Память монохромного видеоадаптера
0B800h:0000h	Память видеоадаптера CGA
0C800h:0000h	Внешнее ПЗУ или адреса периферийных устройств, отображаемые на память
0F600h:0000h	ПЗУ интерпретатора BASIC или адреса периферийных устройств, отображаемые на память
0FE00h:0000h	ПЗУ BIOS

Первый килобайт памяти занимает таблица векторов прерываний. Она содержит 256 элементов, имеющих размер 4 байта. Таблица содержит адреса обработчиков прерываний, состоящие из компонент сегмента и смещения.

Таблица векторов прерываний - любимый объект для нападения вирусов. Вирусы могут изменять содержимое этой таблицы прерываний напрямую или с помощью соответствующего сервиса, предоставляемого операционной системой MS-DOS.

Цель изменений заключается в том, чтобы подключить обработчики прерываний, расположенные в теле вируса, вместо стандартных. При этом вирус получает доступ к важнейшим функциям MS-DOS и BIOS, полностью контролируя их. Подменяя обработчики аппаратных прерываний, вирус может держать под контролем работу периферийных устройств, например, жесткого диска или накопителя на гибких магнитных дисках.

Так как современные антивирусные программы проверяют целостность таблицы векторов прерываний, некоторые вирусы используют для внедрения в обработчики прерываний другие технологии. Например, вирус изменяет несколько первых команд стандартного обработчика прерывания, сохраняя оригинальные команды в своем теле. На место этих команд он записывает другие, передающие управление вирусу. Таким образом, хотя таблица векторов прерываний не изменяется, вирус полностью контролирует ситуацию.

Область памяти с адресами 0000h:0400h - 0000h:04FFh занимает область данных BIOS. Это внутренние переменные BIOS. Здесь хранится важная информация, например, параметры жестких дисков, накопителей на гибких магнитных дисках, текущие параметры операционной системы и т. д. В некоторых случаях вирусы намеренно изменяют некоторые параметры, расположенные в этой области, нарушая нормальную работу операционной системы, или хранят собственные параметры и флаги. Например, вирусы могут отключать накопитель на гибком магнитном диске с целью затруднения загрузки MS-DOS с чистой дискеты.

В области памяти, которая начинается с адреса 0000h:0500h, располагается область данных MS-DOS. Здесь MS-DOS хранит свои внутренние таблицы, переменные и структуры данных. Вслед за областью данных находятся модули системы ввода/вывода MS-DOS, обработчики прерываний MS-DOS, внутренние буферы и внутренние структуры данных, а также загружаемые драйверы. После драйверов располагается резидентная часть командного процессора COMMAND.COM.

И драйверы, и командный процессор могут быть подвергнуты вирусной атаке. В частности, вирусы могут встраивать себя в тело драйвера, перехватывая поступающие в него команды.

Далее в оперативной памяти располагаются резидентные программы и программа, которая выполняется в текущий момент времени.

В нижней части адресного пространства (до адреса 0A000h:0000h) находится транзитная часть командного процессора COMMAND.COM, которая может перекрываться выполняющейся программой.

Область адресов от 0A000h:0000h до 0C800h:0000h используется видеоадаптерами. Так как в этом диапазоне адресов может располагаться оперативная память (которая физически установлена в видеоадаптере), здесь тоже могут “жить” вирусы.

Вся оперативная память, принадлежащая MS-DOS, разделена на фрагменты, перед которыми расположены блоки управления памятью MCB (Memory Control Block). Внутри блока MCB хранится длина описываемого данным MCB фрагмента памяти. Следующий фрагмент памяти начинается сразу за предыдущим. При этом все блоки MCB связаны в список.

В ранних версиях MS-DOS формат блока MCB не был документирован, что, тем не менее, не останавливало разработчиков вирусов от попыток изменения структуры памяти на уровне этих блоков. Теперь же сведения о формате блока MCB можно почерпнуть из руководства программиста, полученного в Microsoft:

Смещение, байт	Размер, байт	Описание
0	1	Тип блока MCB (М или Z)
1	2	Сегментная компонента адреса владельца блока или 0, если блок описывает сам себя
3	2	Число параграфов в этом блоке (размер параграфа равен 16 байт)
5	11	Зарезервировано

Блоки MCB бывают двух типов - М и Z. М-блоки - это промежуточные блоки. Блок типа Z является последним блоком в списке и может быть только один.

Так как любой программе, запущенной под управлением MS-DOS, доступна для записи вся оперативная память, вирус может изменить количество и расположение фрагментов памяти, создав для себя новый фрагмент и, соответственно, новый блок MCB. При этом вирус остается резидентным в памяти, не обращаясь для этого к соответствующим функциям операционной системы. Таким образом вирус предпринимает простейшую попытку скрыть тот факт, что он пытается стать резидентным в оперативной памяти.

Sayha.DieHard

Опасный резидентный и зашифрованный вирус. Перехватывает прерывания INT 10h, 13h, 21h. Вирус крадет данные прерывания для выяснения

адресов оригинальных обработчиков и для попытки "внедрения" в цепочки обработчиков прерываний.

Когда происходит открывание ASM-файлов, вирус записывает в них следующий текст

```
.model small
.code
org 256
s:  push  cs
    pop   ds
    call  t
db    'Te$'
t:   pop   dx
    mov   ah,9
    int   33
    mov   ah,76
    int   33
end s
```

Аналогично, при открывании файлов с расширением имени PAS в них записывается такой текст

```
begin
write('Te');
end.
```

При устном вводе графического режима с номером 13h (разрешение 320x200, 256 цветов) вирус рисует в центре экрана буквы "SW".

Если возникают ошибки при попытке записи на диск (переход за границу 64 Кбайт при работе с DMA или если данные были скорректированы с использованием ECC), вирус пытается их исправить!

В своем теле вирус одерживает текст вые строки "SW Error", "SW DIE HARD 2"

Тщательно изучая структуру блоков MCB (например, при помощи программы MEM.EXE, которая входит в состав MS-DOS), при наличии достаточного опыта вы сможете обнаружить фрагменты памяти, созданные вирусами. Для этого вы должны знать, какие резидентные программы и драйверы загружаются через файлы AUTOEXEC.BAT и CONFIG.SYS, какие они создают блоки, а также понимать назначение блоков памяти, принадлежащих MS-DOS. Более полную информацию об этом

вы можете получить из 18 тома нашей серии книг "Библиотека системного программиста", которая называется "MS-DOS для программиста".

Внесение изменений в файловую систему

Для того чтобы "закрепиться" в компьютере, вирус, как правило, вносит те или иные изменения в файловую систему.

Файловая система MS-DOS не содержит абсолютно никаких защитных механизмов, которые могли бы воспрепятствовать проникновению в ее логические структуры вирусов. Более того, системные прерывания BIOS и MS-DOS предоставляют вирусам весь инструментарий, необходимый для такого проникновения. Эти прерывания хорошо описаны как в документации, поставляемой Microsoft, так и в различной компьютерной литературе (например, в 18 и 19 томах "Библиотеки системного программиста").

Для обеспечения совместимости с периферийными устройствами, выпускаемыми различными фирмами, операционная система MS-DOS выполняет операции ввода/вывода не самостоятельно, а с помощью базовой системы ввода вывода BIOS. При этом любая программа (в том числе вирусная), также может обращаться к прерываниям BIOS.

Прерывание INT 13h

Прерывание INT 13h, обработчик которого находится в BIOS, позволяет любой программе беспрепятственно читать и записывать любые секторы жесткого или гибкого диска. Зная логическую структуру файловой системы MS-DOS (частично описанную в предыдущей главе), разработчик вируса при помощи этого прерывания может встроить вирусный код в загрузочную запись или в любое другое подходящее с его точки зрения место.

Разумеется, о прерывании INT 13h знают не только разработчики вирусов, но и авторы антивирусных программ. И те и другие борются за получение "настоящей" точки входа в обработчик этого прерывания, который должен быть расположен в постоянном запоминающем устройстве. Целью вируса является перехват прерывания INT 13h, а целью антивирусной программы - обнаружение такого перехвата.

Тем не менее, даже надежно защитив точку входа в обработчик прерывания INT 13h, нельзя гарантировать полную защиту от вирусной атаки.

Как вы, возможно, знаете, в реальном режиме работы процессора программе разрешается выполнять операции обмена данными с любыми портами периферийных устройств. В том числе и с портами контроллера жесткого диска или накопителя на гибком магнитном диске. В 19 томе "Библиотеки системного программиста" мы привели пример программы, которая работает именно таким образом, читая сектор дискеты без обращения к прерыванию INT 13h.

Для того чтобы у вас было некоторое представление о том, что может сделать вирус при помощи прерывания INT 13h, приведем краткое описание функций этого прерывания:

Номер функции	Описание
00h	Сброс дисковой системы
01h	Определение состояния дисковой системы
02h	Чтение сектора
03h	Запись сектора
04h	Проверка сектора
05h	Форматирование дорожки
06h	Форматирование дорожки НМД
07h	Форматирование НМД
08h	Получить текущие параметры НГМД или НМД
09h	Инициализация таблиц параметров НМД
0Ah	Чтение длинное (только для НМД)
0Bh	Запись длинная (только для НМД)
0Ch	Поиск цилиндра (только для НМД)
0Dh	Альтернативный сброс НМД
0Eh	Чтение буфера (только для НМД)
0Fh	Запись буфера (только для НМД)
10h	Проверка готовности НМД
11h	Рекалибровка НМД
12h	Проверка памяти контроллера НМД
13h	Проверка НМД
14h	Проверка контроллера НМД
15h	Получить тип НМД или НГМД
16h	Проверка замены диска
17h	Установка типа дискеты
18h	Установка среды носителя данных для форматирования
19h	Парковка головок (только для НМД)
1Ah	Форматирование НМД с интерфейсом ESDI

Как видите, вирус может прочитать, записать и отформатировать дорожку диска. Используя команды 0Ah и 0Bh, разработанные для диагностических целей, вирус может изменить контрольные суммы секторов данных, которые обычно подсчитываются, записываются и проверяются автоматически.

SillyRE.666

Опасный шифрованный вирус.
После загрузки в память своей резидентной копии вирус записывает "мусор" в 11 сектор нулевой дорожки (головка с номером 1), пользуясь для этого операцией длинной записи. Обычно на этом месте диска находится первая копия таблицы размещения файлов FAT

С помощью функций прерывания INT 13h вирус может получить доступ к внутреннему буферу, расположенному непосредственно в дисковом накопителе. Другой “лакомый кусочек” для вирусов - прерывание INT 76h, которое вырабатывается при завершении операции в контроллере жесткого диска. Вирус может перехватывать это прерывание для реализации стелс-технологии.

Прерывания INT 25h и INT 26h

Операционная система MS-DOS предоставляет для работы с файловой системой и логическими дисками свои средства. Это прерывания INT 25h, INT 26h, а также ряд функций прерывания INT 21h. Кроме того, программа может работать с дисковыми устройствами через соответствующий драйвер, обращаясь к нему косвенно с помощью функций интерфейса IOCTL. Все эти средства были нами подробно описаны в 19 томе “Библиотеки системного программиста”. С помощью прерываний INT 25h и INT 26h любая программа (а также вирус) может, соответственно, прочитать и записать любой сектор логического диска. Используя эти прерывания, вирусу ничего не стоит, например, подменить загрузочный сектор логического диска, выполнив таким образом заражение этого диска. Так как эти два прерывания используются MS-DOS для выполнения операций с логическими дисками, многие вирусы пытаются их перехватить, чтобы получить контроль над операциями ввода/вывода (например, для реализации стелс-механизма).

MIREA.4156

Полиморфный вирус.
Выполняет поиск EXE-файлов, чтение из файла и запись в файл через прерывания INT 25h и INT 26h. Файлы могут быть поражены в любом подкате логического диска.
Содержит ошибки, из-за которых неработоспособен на диске с 12-разрядной таблицей размещения файлов FAT.
Иногда по окончании своей работы, может выдать текст:

Заранее прошу извинения.
Чистая случайность, что ЭТО попало к Вам.

По классификации Е.Касперского это типичная "студенческая" программа, причем в наихудшем ее исполнении:

- портит оверлеи (если не повезет то и резиденцы тоже),
- портит забитый до отказа диск,
- содержит большое число ошибок,
- имеет большой размер,
- и тд.

Чего еще можно ожидать от студента МИРЭА.

Ничего гадкого, кроме распространения программа не делает (я на это надеюсь, хотя от "студенческой" можно ожидать всего из-за ее крайней примитивности и большого числа ошибок).

МИРЭА - хороший ВУЗ!!!

МИРЭА - это звучит гордо!!!

МИРЭАзм не объяснить, в нем надо жить !!!

Перехват прерываний можно выполнить разными способами. Можно напрямую отредактировать таблицу векторов прерываний. Можно также воспользоваться услугами функций 25h и 35h прерывания INT 21h, предназначенных, соответственно, для установки нового вектора прерывания и получения текущего вектора прерывания.

Однако антивирусные программы тщательно проверяют таблицу векторов прерываний, поэтому для их изменения вирусы используют различные изощренные приемы. Например, вирус может подменить первые несколько команд обработчика прерывания, сохранив эти команды в своем теле. При этом, несмотря на то что таблица векторов прерываний остается нетронутой, прерывание оказывается перехваченным. Такая методика, разумеется, может быть использована для перехвата любых прерываний, а не только прерываний INT 25h и INT 26h.

Функции прерывания INT 21h

Что касается функций прерывания INT 21h, предназначенных для работы с файловой системой, то их набор является полным и позволяет выполнять практически любые операции над файлами и каталогами.

Пользуясь этими функциями, вирусы могут беспрепятственно изменять загрузочные файлы программ, дописывая к ним новый код и редактируя заголовок файла. При этом стелс-вирусы маскируют внесенные изменения, перехватывая многие функции прерывания INT 21h и возвращая ложную информацию, например, о размере файла.

Интерфейс GENERIC IOCTL

Еще одно средство, которое может быть использовано вирусами для внесения изменений в файловую систему, это интерфейс общего управления вводом/выводом GENERIC IOCTL.

Этот интерфейс реализован в рамках функции 44h прерывания INT 21h (операция с кодом 0Dh), которая обеспечивает механизм взаимодействия между прикладным программным обеспечением и драйверами блочных устройств.

Указанная функция позволяет программам (и вирусам) читать и изменять параметры устройств, выполнять чтение, запись, форматирование и проверку дорожек диска на низком уровне с помощью драйвера устройства.

При вызове функции регистры процессора загружаются следующим образом:

Регистр	Описание содержимого
AH	44h
AL	0Dh
BL	Номер устройства НМД или НГМД
CH	Код категории устройства: 08h - дисковое устройство
CL	Операция: 40h - установить параметры устройства; 60h - получить параметры устройства; 41h - записать дорожку; 61h - прочитать дорожку; 42h - форматировать дорожку; 62h - проверить дорожку
DS:DX	Указатель на блок параметров

Через регистры DS:DX функции передается адрес подготовленного блока параметров, формат которого зависит от выполняемой операции. Из приведенного выше описания видно, что набор выполняемых функцией операций более чем достаточен для того чтобы с его помощью вирусы могли сделать любые изменения логических структур файловой системы.

Вирусы в загружаемых драйверах

Драйвер является расширением операционной системы, предназначенным, как правило, для работы с тем или иным периферийным устройством. Обычно в составе любой операционной системы имеется набор драйверов, предназначенных для разных устройств.

Что касается операционной системы MS-DOS, то для нее все драйверы можно разделить на встроенные в ядро и подгружаемые через файл CONFIG.SYS.

Встроенные и подгружаемые драйверы после загрузки объединяются в цепочку, адрес которой можно найти с использованием недокументированных средств, описанных нами в 18 томе "Библиотеки системного программиста".

Для того чтобы понять, каким образом вирус может заразить драйвер, вспомним, что в самом начале драйвера находится заголовок следующего формата:

Смещение, байт	Размер, байт	Описание
0	4	Указатель на заголовок драйвера, следующего в цепочке. Если смещение адреса следующего драйвера равно 0FFFFh, это последний драйвер в цепочке
4	2	Атрибуты драйвера
6	2	Смещение программы стратегии драйвера
8	2	Смещение программы обработки прерывания для драйвера
0Ah	8	Имя устройства для символьных устройств или количество обслуживаемых устройств для блочных устройств

Обратите внимание на поля смещений программы стратегии и обработки прерывания драйвера. Эти поля используются операционной системой MS-DOS для вызова драйвера.

Вызов драйвера представляет собой двухступенчатый процесс.

Вначале операционная система вызывает программу стратегии, пользуясь смещением, полученным из заголовка драйвера (поле со смещением 6). Перед этим она формирует в своей области данных запрос, передавая программе стратегии адрес соответствующего блока данных в регистрах ES:BX. Программа стратегии обычно очень проста, так как ее задача заключается в запоминании адреса блока данных, содержащего запрос, в области памяти, принадлежащей драйверу.

Запрос операционной системы к драйверу содержит заголовок, имеющий фиксированный формат и длину 13 байт, а также структуру переменного размера и формата, которые зависят от выполняемой функции (переменная область запроса). Формат первой области запроса приведен ниже:

Смещение, байт	Размер, байт	Описание
0	1	Общий размер блока запроса в байтах
1	1	Номер устройства. Используется для блочных устройств; указывает, с каким именно устройством (из числа обслуживаемых данным драйвером) будет работать операционная система
2	1	Код команды, которую требуется выполнить
3	2	Слово состояния устройства. Заполняется драйвером перед возвращением управления операционной системе

5	8	Зарезервировано
---	---	-----------------

На втором этапе операционная система MS-DOS вызывает программу обработки прерывания, взяв ее смещение из заголовка драйвера (поле со смещением 8). Программа обработки прерывания анализирует код команды, расположенный в фиксированной области запроса (поле со смещением 2) и выполняет ее.

Заражение драйвера, загруженного в оперативную память, выполняется достаточно просто. Вирус находит в цепочке драйверов жертву и изменяет заголовок драйвера, либо подменяет несколько команд, расположенных в начале программ стратегии и обработки прерывания. После этого вирус становится способен контролировать выполнение всех команд, поступающих в драйвер.

Dir-II (1,2)

Неопасные резидентные вирусы, встраивающиеся в цепочку дисковых драйверов.

Вирусы записывают свой код в последний кластер диска. Для файлов с расширениями имени COM и EXE устанавливают указатели первого кластера данных на последний кластер диска, содержащий вирусный код

Заражение файла с драйвером выполняется примерно также, как и заражение файла обычной исполнимой программы с расширением имени EXE. Для определения смещения программ стратегии и прерывания вирус должен проанализировать заголовок драйвера, который находится в самом начале файла, содержащего драйвер. Дальнейшие действия вируса очевидны - замена нескольких начальных команд и дописывание в конец файла вирусного кода.

ExeHeader.Dragon

Инстиллируется в память и внедряется в цепочку дисковых драйверов. Содержит в своем теле строку "DRAGON-2 Anti"

Операционная система Microsoft Windows версии 3.1

Первые версии операционной системы Microsoft Windows представляли из себя не более чем надстройку над MS-DOS и потому воспринимались как красивые, но не слишком нужные оболочки для работы с файловой системой. Однако версия 3.1 этой операционной системы, в которой впервые была применена технология масштабируемых шрифтов True Type, получила громадную, ни с чем не сравнимую популярность. В большой степени это произошло еще и потому, что многие ведущие производители программных средств создали для Microsoft Windows очень хорошие приложения, ставшие в последнее время просто незаменимыми.

Однако многие согласятся с тем, что надежность операционной системы Microsoft Windows версии 3.1 (и ее более поздняя модификация Microsoft Windows for Workgroups версии 3.11) не слишком высока. Некорректно написанная программа может полностью нарушить работоспособность всей системы, что приведет к необходимости перезагрузки компьютера.

Как устроена операционная система Microsoft Windows версии 3.1?

Полный ответ на этот вопрос займет очень много места. Интересующихся подробностями мы отсылаем к томам с 11 по 17 включительно нашей “Библиотеки системного программиста”, в которых мы рассмотрели различные аспекты программирования для Microsoft Windows.

Если же сказать кратко, то Microsoft Windows создает одну системную виртуальную машину для запуска всех приложений Microsoft Windows, и по одной виртуальной машине для каждой программы MS-DOS. Каждая такая виртуальная машина имеет собственное виртуальное адресное пространство, что позволяет (теоретически) исключить их взаимное влияние друг на друга. Однако на практике такое влияние все же есть. Именно оно приводит к такой ситуации, когда аварийное завершение одной из программ приводит к аварийному завершению всей операционной системы.

Вы можете спросить - а при чем тут вирусы?

Но ведь вирус - это программа, а раз обычная программа может влиять на все остальные и даже на операционную систему в целом, то и вирус тоже сможет. И еще как.

Нелегкий груз совместимости

Мы не сделаем открытия, если скажем, что успех новой операционной системы в большой степени определяется ее способностью выполнять старые программы. Операционная система никому не нужна сама по себе - она используется только как рабочая среда для запуска прикладных программ. И если пользователи, установив новую операционную систему, обнаружат что все их любимые программы перестали работать, они едва ли будут довольны.

Осознавая этот факт, Microsoft при создании операционной системы Microsoft Windows приложила много усилий для обеспечения совместимости с программами MS-DOS. При этом вольно или невольно она обеспечила прекрасную совместимость почти со всеми вирусами, разработанными в свое время для MS-DOS.

Как сделать, чтобы программы MS-DOS хорошо чувствовали себя в среде виртуальной машины, создаваемой для них операционной системой Microsoft Windows?

В лучшем случае виртуальная машина должна быть сделана так, чтобы работающая в ее среде программа и не подозревала, что машина на самом деле “не настоящая”. Для этого программам должно быть позволено все, что и раньше. И хотя теперь программы несколько ограничены в правах, так как имеют доступ только к своему виртуальному пространству оперативной памяти, диски и файловая система для них доступны как и раньше. Аналогично, программы (и вирусы) могут напрямую работать с портами периферийных устройств, что также не повышает устойчивости системы к вирусам.

Отыщи всему начало...

Строго говоря, операционная система Microsoft Windows версии 3.1 не является... операционной системой. Скорее это очень большая программа MS-DOS, которая составлена с использованием расширителя DOS (нам кажется, что это был DOS Extender фирмы Phar Lap). О расширителях DOS вы можете узнать из 6 тома “Библиотеки системного программиста”, который называется “Защищенный режим работы процессоров Intel 80286/80386/80486”).

Расширитель DOS при запуске программы переводит процессор в защищенный режим работы, обеспечивая при этом интерфейс с обработчиками прерываний, функциями BIOS и DOS, рассчитанные на реальный режим работы процессора. При этом программа получает, с одной стороны, возможность воспользоваться преимуществами защищенного режима работы процессора (такими, например, как прямая адресация расширенной памяти), с другой стороны - возможность работы с файловой системой средствами прерываний MS-DOS. Удобно и практично.

Так как Microsoft Windows версии 3.1 не может работать без MS-DOS, то вирусы могут сделать многое еще до старта этой операционной системы. Например, вирусы могут удобно расположиться в главной загрузочной записи MBR или загрузочной записи Boot Record, перехватить и взять под свой контроль ключевые прерывания BIOS и MS-DOS.

Поэтому операционная система Microsoft Windows версии 3.1 по своей “питательности” для вирусов ни в чем не уступает MS-DOS. И хотя на сегодняшний день мы не наблюдаем лавинообразного роста вирусов, специально ориентированных на операционную систему Microsoft Windows версии 3.1, вы не должны расслабляться. Даже если вы давно забыли команды MS-DOS и работаете только с приложениями Microsoft Windows, вам по-прежнему угрожают несколько тысяч старых вирусов, созданных “в стиле” MS-DOS.

Откуда не ждали

В начале этой книги мы рассказали вам о макрокомандных вирусах, которые являются последним “достижением” в этой области. Хотя эти вирусы родились в среде Microsoft Windows версии 3.1, они не пользуются (пока) “слабостями” этой операционной системы. Потенциально такие вирусы могут существовать в среде любой операционной системы, если для нее созданы приложения, работающие с объектными документами, содержащими наряду с обычными данными последовательности макрокоманд.

Можно даже сказать, что макрокомандные вирусы живут не в среде операционной системы, а в среде прикладных программ, работающих с документами. Так как в последнее время разрабатываются кросс-платформные операционные системы и приложения, потенциально любая операционная среда может оказаться подвержена заражению макрокомандными вирусами.

Операционная система Microsoft Windows 95

Несмотря на значительный прогресс в области пользовательского интерфейса, более устойчивую работу за счет разделения виртуальных адресных пространств отдельных приложений и реальной мультзадачности, операционная система Microsoft Windows 95 устойчива к вирусам не более, чем Microsoft Windows версии 3.1.

Причина все та же - эта операционная система очень хорошо совместима с программами MS-DOS, “привыкшим” к бесконтрольному владению компьютером.

Несмотря на то что Microsoft хорошо спрятала MS-DOS версии 7.0 от пользователя, вирусы найдут ее функции и логические структуры данных без особого труда, точно также как и привычные вам файлы CONFIG.SYS и AUTOEXEC.BAT. Заразив главную загрузочную запись и резидентные программы, запускаемые через файл AUTOEXEC.BAT, вирусы смогут доставить вам немало хлопот, повредив, например, другие программные файлы, файлы данных или даже всю файловую систему.

К сожалению, файловая система Microsoft Windows 95 по-прежнему не имеет никакой защиты, поэтому вирусные программы, работающие, например, в среде виртуальной машины MS-DOS, смогут повредить ее без особого труда, воспользовавшись, например, вполне “легальными” функциями прерывания INT 21h.

Добавьте к сказанному выше возможность заражения макрокомандными вирусами, и вы поймете, что единственная гарантия предохранения компьютера с операционной системой Microsoft Windows 95 от вирусов - это грамотное использование антивирусных программ.

Операционная система IBM OS/2

Операционная система IBM OS/2 защищена от вирусов намного лучше всех других описанных выше операционных систем. В самом деле, на настоящий момент не существует вирусов, разработанных специально для IBM OS/2. В отличие от Microsoft Windows и Microsoft Windows 95 эта операционная система является полнофункциональной и работает, разумеется, без всякой помощи со стороны MS-DOS, которой может даже не быть на диске.

Все программы, запускаемые в среде OS/2, работают в отдельных адресных пространствах, и потому не могут повлиять друг на друга. Подробнее о том как устроена и работает операционная система IBM OS/2 Warp версии 3.0, а также о том как ее установить и настроить, вы можете узнать из 20 тома нашей серии “Библиотека системного программиста”, который называется “Операционная система IBM OS/2 Warp”.

А как же, спросите вы, совместимость с программами MS-DOS?

Эта совместимость имеется, хотя в наиболее ответственных случаях ее можно отключить.

Операционная система способна работать с различными файловыми системами, самыми важными из которых является файловая система FAT и HPFS. Первая из них

используется операционной системой MS-DOS и нужна главным образом как раз для совместимости. Вторая является высокопроизводительной файловой системой HPFS (High Performance File System), специально разработанной для OS/2.

В ответственных случаях вы можете работать только с файловой системой HPFS, запретив пользователю запускать программы MS-DOS. Для этого в файле CONFIG.SYS необходимо указать следующую строку:

PROTECTONLY=YES

В этом случае оперативная память в пределах первого мегабайта адресного пространства будет использоваться для запуска программ OS/2.

Учтите, что если вы запретите запуск программ MS-DOS, вы не сможете запускать в среде IBM OS/2 и приложения Microsoft Windows.

Дополнительно можно усилить защиту, указав в файле CONFIG.SYS такую строку:

IOPL=NO

При этом обычные (несистемные) программы не будут иметь доступ к портам периферийных устройств.

В том случае, если вы работаете в среде IBM OS/2 с программами MS-DOS или приложениями Microsoft Windows, существует опасность поражения программных файлов вирусами, разработанными для операционной системы MS-DOS. Такие вирусы могут оставаться резидентными в памяти во время работы сеанса DOS и способны повредить программные файлы, расположенные на диске. Хотя, разумеется, возможностей для повреждения файловой системы у них будет намного меньше, чем в среде MS-DOS. В частности, вирусы не смогут воспользоваться прерыванием INT 13h для перезаписи главной загрузочной записи и не смогут повредить системные области файловой системы HPFS.

Если компьютер с операционной системой IBM OS/2 используется в качестве файл-сервера IBM LAN Server, загружается драйвер 386 HPFS, который дополнительно повышает защищенность файловой системы HPFS, позволяя указывать права доступа к каталогам и файлам. Вы можете защитить каталоги, содержащие программные файлы, от записи, и при этом вирусы не смогут их повредить.

Операционная система Microsoft Windows NT

Операционная система Microsoft Windows NT предназначена для высокопроизводительных файл-серверов (в варианте Microsoft Windows NT Advanced Server), а также для элитных рабочих станций класса High End (вариант Microsoft Windows NT Workstation).

Оба варианта снабжены надежной системой защиты, непреодолимой для вирусов и злоумышленников, поэтому операционная система Microsoft Windows NT сертифицирована для использования в государственных и правительственных учреждениях.

Если объем оперативной памяти в вашем компьютере равен или превышает 16 Мбайт, а объем диска - 500 Мбайт, вам нужна высокая надежность, совместимость с программами MS-DOS и приложениями Microsoft Windows, прекрасные средства работы в локальных или глобальных сетях, подумайте об операционной системе Microsoft Windows NT версии 3.51 или более новой.

Файловая система NTFS, примененная в Microsoft Windows NT, позволяет вам управлять доступом к программным файлам и файлам данных. Защитив каталоги с прогрфаммными файлами от записи, вы надежно защитите их от нападения вирусов, в том числе и от тех, что разработаны для MS-DOS.

В отличие от своих предшественников, операционная система Microsoft Windows NT является полнофункциональной и не нуждается в услугах MS-DOS. В корневом каталоге нет файлов AUTOEXEC.BAT и CONFIG.SYS. Нет также резидентных программ, получающих управление на этапе загрузки операционной системы.

Несмотря на то что Microsoft Windows NT может работать с файловой системой FAT, в ответственных случаях мы советуем вам ограничиться файловой системой NTFS, которая на сегодняшний день является наиболее развитой и защищенной.

Опера ционная систем а Novell NetWare

Мы уже рассказывали вам о том, как следует организовывать антивирусную защиту локальных сетей, в частности, созданных на базе операционной системы Novell NetWare.

В этом разделе мы еще раз напомним вам об одном уязвимом месте этой весьма и весьма хорошо защищенной операционной системы.

Речь идет о том, что вирусы могут подсмотреть пароль супервизора, когда тот вводит его на рабочей станции.

Как это можно сделать?

Напомним, что для входа в сеть супервизор (как и любой другой пользователь) запускает с сетевого диска программу LOGIN.EXE и вводит в ответ на приглашение свое имя и пароль.

Процесс ввода пароля таит в себе опасность, так как коды введенных символов имени и пароля проходят через буфер клавиатуры, расположенных в области данных BIOS. Вирус, загруженный резидентно в оперативную память, может организовать сканирование этого буфера с целью обнаружения имени и пароля. В этом нет ничего трудного.

Затем, пользуясь программным интерфейсом сетевой оболочки рабочей станции MS-DOS, вирус может попытаться определить привилегии пользователя. И если пользователь ввел пароль супервизора, вирус может получить полный доступ над файл-сервером. Заметим, что подобную процедуру вирусы могут проделать не только с файл-сервером Novell NetWare, но и с файл-серверами, созданными на базе других сетевых операционных систем.

Например, он может записать новую plm-программу в системный каталог и включить ее имя в файл STARTUP.NCF, который интерпретируется на этапе загрузки операционной системы Novell NetWare. Такая программа может иметь права на чтение или запись в любой каталог файл-сервера.

Более подробную информацию о процессе подключения пользователя к файл-серверу Novell NetWare вы можете получить из 9 тома нашей серии книг “Библиотека системного программиста”, который называется “Локальные сети персональных компьютеров. Работа с сервером Novell NetWare”.

Для того чтобы избежать подобной неприятности, супервизор должен входить в сеть, только загрузив свою рабочую станцию с чистой заклеенной системной дискеты, свободной от вирусов. На эту же дискету нужно переписать программу LOGIN.EXE, предварительно убедившись, что она сама не заражена. Это можно сделать, например, при помощи программ Doctor Web и Aidstest из антивирусного комплекта АО “ДиалогНаука”.

Ни при каких обстоятельствах не следует входить в сеть пользователем с правами супервизора, если нет полной уверенности, что рабочая станция не заражена вирусами.

ЛИТЕРАТУРА

1. Фролов А.В., Фролов Г.В. Библиотека системного программиста. М.: ДИАЛОГ-МИФИ, 1991-1996
- Т.16. Модемы и факс-модемы. Программирование для MS-DOS и Windows.
- Т.18, 19. MS-DOS для программиста.
- Т.20. Операционная система IBM OS/2 Warp.
2. Фролов А.В., Фролов Г.В. Персональный компьютер. Шаг за шагом. М.: ДИАЛОГ-МИФИ, 1994-1996
- Т.1. Введение в MS-DOS, MS Windows, MS Word for Windows.
- Т.2. Операционная система Microsoft Windows. Руководство пользователя.
- Т.3. Сети компьютеров в вашем офисе.
- Т.4. Что вы должны знать о своем компьютере.
3. Д.Н. Лозинский, Д.Ю. Мостовой, И.А. Данилов, В.С. Ладыгин, Д.Г. Зуев, Ю.Н. Фомин. Антивирусный комплект АО “ДиалогНаука”. Руководство пользователя. М.: ДИАЛОГ-МИФИ, 1995-1996
4. Survivor's Guide to Computer Viruses. Virus Bulletin, 21 The Quadrant, Abingdon, OX14 3YS, England, 1993
5. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 1991

6. Безруков Н.Н. Компьютерная вирусология: справочное
руководство. - Киев: Укр. сов. энцикл., 1991