Все больше разнородных слухов, все больше «компьютерных гуру", от компетентности которых зачастую зависит благополучие фирмы. К сожалению, не у всякого менеджера есть хороший консультант...

Проблема вирусов - это прежде всего один из аспектов общей проблемы защиты информации в ЭВМ.

Наша страна стремительно входит в век информатики, пролетая «большими скачками» этапы, стоившие другим десятилетий проб и болезненных ошибок. Хорошо известно, что остановка компьютерных систем любого крупного банка Запада на несколько дней - это его неизбежный финансовый крах. Надо, наконец, попытаться использовать чужой опыт, не ожидая, пока гроза разразится где-нибудь в сети ЭВМ московских банков.

К тому же, наслышанные о разных экзотических и фатальных ситуациях с треклятыми компьютерами, многие управляющие не решаются, введя машинную обработку данных, оставить старое бумажное хозяйство. Таким образом, сплошь и рядом, учреждения вместо ожидаемого выигрыша получают от введения ЭВМ двойное бремя делопроизводства.

И это - огромная проблема для делового человека - как определить позицию своего бизнеса, своего дела относительно возможных нововведений, связанных с ЭВМ.

Компьютер - это просто инструмент, который может быть надежен как отбойный молоток и способен хорошо делать свое дело, но для этого нужно, для начала, хорошо продумать все - и продумать до деталей.

И пока юристы в разделе «Компьютер и право», будут подводить законодательную базу под явления компьютерной преступности, мы, в свою очередь, постараемся освещать различные аспекты защиты данных и способы эффективной «организации обороны».

ПЯТНИЦА, 13-е

Вирусы и противодействие им: обобщая плоды мирового опыта и применяя собственные эффективные средства, автор, специалист по «компьютерной безопасности», обсуждает способы борьбы с «электронной чумой» и рассказывает о видах программ-вредителей, механизмах заражения и излечения

Тем из читателей, кто не уверен в своем знании ЭВМ, автор хотел бы порекомендовать: если вы заподозрили что-то неладное и считаете, что ваш компьютер заражен, не пытайтесь на свой страх и риск запускать диагностические и сервисные программы. Это может значительно усугубить ситуацию. Лучше выключить компьютер, запереть его на ключ (лучшая защита от любопытных и энергичных!) и связаться с консультационной фирмой, в компетентности которой вы не сомневаетесь.

К счастью, практика показывает, что далеко не во всех подобных случаях виноваты вирусы. Причиной непонятного поведения машины может стать и неплотно вставленная в магистраль ЭВМ плата расширения, и конфликтующие между собой адаптеры (особенно - на стареньких IBM PC/XT), и многие другие программные конфликты и аппаратные сбои.

Что же такое вирус? Попробуем определить это.

Вирусом называется программа, предназначенная для нарушения работы различных частей компьютера, которая распространяется посредством «при-клеивания» самой себя к другим программам.

Вирус использует "принцип прозрачности": маскирует факт своего появления в операционной системе.

Распространненым вариантом такого вируса является «временная бомба». Это программа, которая, попав в компьютер, старается начать размножаться и «ждет» до определенного момента времени, после чего она включается и производит те или иные действия. Иногда эти действия могут быть вполне безобидными, а иногда могут приносить тот или иной вред.

Вирусы производят как видимый пользователю эффект, так и невидимый, скрытый.

«Видимые» пользователю эффекты могут заключаться в «зависании» ЭВМ (вирус Black Friday), имитации падения букв на экране (вирус 1701/1704), рисовании геометрических фигур (Black Friday, Bouncing Ball), проигрывании мелодии (Jankey-1, 2, 3).

«Скрытые» вирусы также можно заметить, например, по неожиданному обращению ЭВМ к дисководу. Это особенно заметно в случае работы с дискетами.

Троянским конем называется программа, цель которой - сделать невозможным использование хранящейся в компьютере информации путем ее уничтожения (перезаписи) или шифрования (крипто-графирования).

Троянский конь предназначен для единственного акта разрушения, что отличает его от долгожителя-вируса, распространяющегося в ЭВМ и внедряющегося в различные программы.

Иногда троянский конь располагается на диске совершенно открыто и, вдобавок, в целях привлечения внимания, носит либо имя, схожее с именем какой-нибудь полезной сервисной программы, либо экзотически-провоцирующее имя (скажем, LOVE_ME.COM), вызывающее у программиста неодолимое желание тут же ее запустить.

Последним приемом также пользуются, чтобы выманить у пользователя его пароли доступа, которые игриво запрашивает такая программа, имитируя затем системный сбой и исчезая с диска.

Будучи запущенным, троянский конь наносит удар. Троянские кони - это наиболее агрессивные и опасные программы для вашего компьютера.

Наиболее существенное различие между вирусом и троянским конем заключается в том, что вирус, вообще говоря, является более долгоживущей программой, чем троянский конь (помните легенду о Трое?). Однако в последнее время создатели программ-злоумышленников стали сочетать классические черты и того, и другого вида, порождая так называемых «гибридов». В целях упрощения изложения будем применять термин «вирус» по отношению ко всем видам этих «злых» программ, давая, если нужно, уточнения в каждом конкретном случае.

Особняком в нашем обсуждении стоят так называемые

«червяки». Эти программы ничего не разрушают, но быстро размножаются и передаются по сетям, стараясь заполонить собой диски и забрать под размножение и пересылку самих себя как можно больше ресурсов ЭВМ. Ситуация осложняется тем, что сеть обычно обслуживают без вмешательства человека программы-администраторы, для которых «червяк» - просто одна из обычных программ, которую надо обслужить.

Нашумевший инцидент 1988 года, о котором сообщалось также в отечественных средствах информации, касался не вируса, а именно «червяка», написанного Р.Моррисом (мл.) и распространившегося по сетям ЭВМ в США. Суд присяжных приговорил Морриса к крупному штрафу, и, в довершение бед, он был исключен из университета, где учился.

У каждого семейства ЭВМ - свои вирусы, основанные на особенностях конкретной операционной системы.

Существуют IBM-совместимые, Macintosh-совместимые и UNIX-совместимые семейства вирусов.

Опыт показывает, что наиболее многочисленны и агрессивны вирусы для тех ОС, в которых отсутствуют (полностью или частично) средства защиты информации. Примером такой операционной системы является MS-DOS, которая разрабатывалась как однопользовательская и однозадачная.

Примером хорошо защищенной от вирусов ОС является UNIX, где реализована удачная схема защиты. ОС, где не могут одновременно существовать несколько программ (например, DOS 3.3 для Apple II), также «не в силах» быть инфицированной.

В ОС, подобной UNIX, программа-разбойник оказывается в положении бомжа, приехавшего в славный город на Неве. Бомж может свободно бродить по улицам и спать в подвалах. Но, стоит ему проголодаться и придти в магазин или в гостиницу, как от него потребуют визитку или паспорт. Примером является среда MS-Windows. Подхватив инфекцию, Windows в большинстве случаев прекращает работу и повисает при запуске, волей-неволей заставляя пользователя доискиваться до причин. Тем самым условия размножения и существования вируса становятся весьма непростыми.

Дальнейшее изложение в данной статье будет посвящено именно MS-DOS - самой массовой и самой уязвимой.

МЕТОДЫ И ОБЪЕКТЫ ВИРУСНОЙ АТАКИ

Мы рассмотрим различные части программного обеспечения в среде MS-DOS и то, каким образом они могут быть атакованы вирусными программами.

I. Программа начальной загрузки (Initial program loader).

Одно из наиболее уязвимых мест MS-DOS. Вирус легко может переписать начальный загрузчик (сохраняя оригинал!), а может и сам замаскироваться под эту программу (Рис.1). Главная неприятность заключается в полном отсутствии средств защиты в момент выполнения программы начальной загрузки (исключение составляют так называемые «иммунные» компьютеры со встроенными в BIOS и DOS функциями защиты).

II. Исполняемые файлы (расширение EXE)

Применяемый метод заражения в отношении исполняемых файлов - дописать вирус в конец файла, изменив при этом необходимые параметры в заголовке файла (Рис.2). Существует и другая возможность: включить тело вируса между таблицей настройки (relocation table) и собственно программой (memory image). На сегодняшний день автору ничего не известно о реализации подобной схемы.

III. Командные файлы (расширение COM)

MS-DOS так устроена, что относит любой файл в отсутствие EXE-заголовка (EXE-header) (обратите на это особое внимание!) к командным. Вирусы заражают эти файлы, добавляя себя в конец или в начало программы, конечно, с последующей передачей управления самому себе (Рис.3).

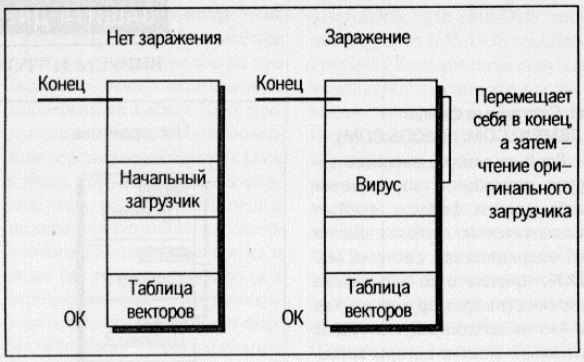

Рис.1

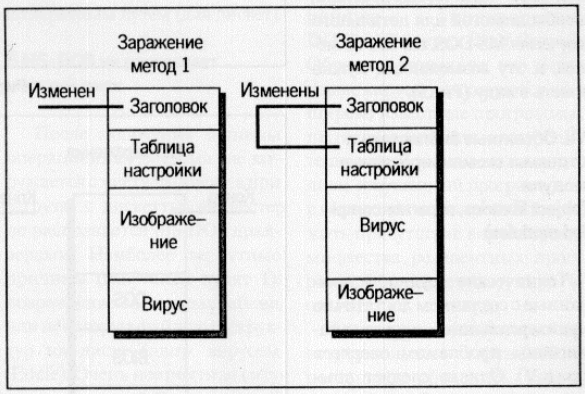

Рис.2

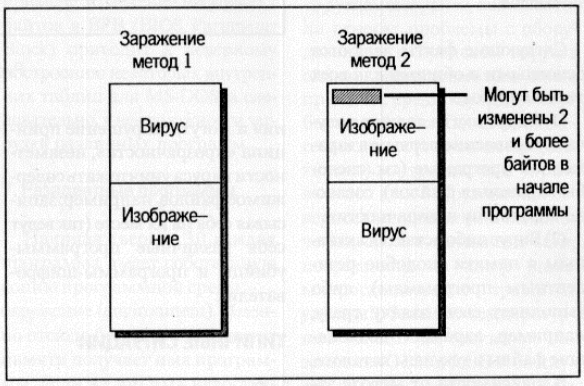

Рис.3

IV. Драйверы устройств

К сожалению, и эти очень полезные программы могут быть атакованы вирусами. Излюбленный метод заражения - записать себя последним в связанном списке драйверов для данного файла, причем, «умные» вирусы могут поставить себя и первым в этом списке (Рис.4). Вообще говоря, это - достаточно сложная операция.

V. Оверлейные файлы

Заражение этих файлов вполне возможно, однако из-за сильной зависимости структуры файла от индивидуальных черт трансляторов и оверлейных схем, внедрение вируса в процесс оверлейной подкачки требует решения ряда весьма труднопреодолимых технических проблем.

VI. Системные файлы (IBMBIO.COM, IBMDOS.COM).

Вообще говоря, создание вируса, способного «приклеить» себя к этим файлам, требует исключительно глубоких знаний об операционной системе MS-DOS, причем в ее нескольких версиях (например, версии 3.xx и 4.xx на сегодня). Думается, не слишком многие авторы вирусных программ затрачивают большое количество времени, необходимогой для детального изучения MS-DOS, но, тем не менее, и эту возможность нужно иметь в виду (Рис.5).

VII. Объектные библиотеки и отдельно скомпилированные модули (object libraries, separate compiled modules)

Технические трудности, связанные с созданием достаточно «универсального» вируса, аналогичны проблемам оверлеев (см.п.V). Однако следует помнить о принципиальной возможности осуществления подобных замыслов.

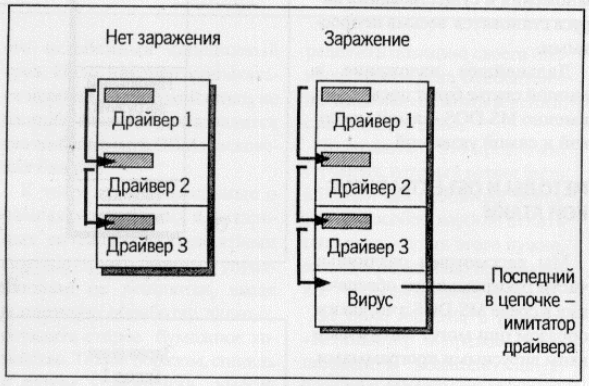

Рис.4

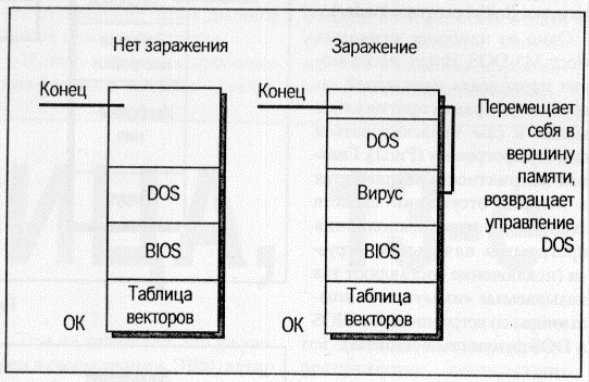

Рис.5

Следующие факты являются основными и общими для всех типов вирусов:

(1) Вирус всегда должен получать управление первым в зараженной программе (см. способы заражения файлов), согласно «принципу прозрачности».

(2) Вирус либо остается активным в памяти (подобно резидентным программам), либо выполняет свою задачу сразу, например, заражает подходящие файлы в текущем каталоге.

В зависимости от метода заражения активно используются либо средства MS-DOS (чтение, запись файла), либо средства BIOS (чтение, запись диска).

Излюбленными ресурсами вычислительной системы, подвергающимися атаке вируса (нарушения работы) являются диск, видеопамять (формирующая изображение на мониторе). К сожалению, есть хорошие шансы, что многие из этих «фокусов» читатели уже видели в действии. Хочу предупредить также о малоизвестном факте: некоторые вирусы используют игру случайных чисел для выбора стратегии своего поведения и могут,в нарушение принципа «прозрачности», незаметности вируса уничтожать содержимое файлов, например, записывая себя на их месте (так ведут себя различные программы-убийцы и программы-шифровали).

ТИПИЧНЫЕ СИТУАЦИИ

После краткого теоретического введения пора перейти к практическим ситуациям, в которых нужно быть предельно внимательным и аккуратным. Хотелось бы, прежде чем перейти к более подробному обсуждению, еще раз посоветовать: никогда не пользуйтесь услугами самодеятельных экспертов. После них обычно практически ничего не удается восстановить (структура диска уничтожается полностью).

Приведем ряд часто встречающихся на практике ситуаций.

1. Машина находится в бесконечном цикле автоматического рестарта.

Несколько возможных причин: вирусы типа Vienna (DOS-G2), machine-rebooter, COM-killer (1-of-8 Virus), некоторые самозагружаемые вирусы (bootable viruses).

Возможно, повреждена (или заражена) программа начальной загрузки, то же самое можно ожидать и в отношении системных файлов, командного интерпретатора (обычно COMMAND.COM), инсталлируемых драйверов устройств, программ, вызываемых из файла AUTOEXEC.BAT. Метод, описанный ниже, является подходящим (с некоторыми изменениями) практически во всех ситуациях:

(а) загрузить операционную систему с «чистой» системной дискеты (это копия дистрибутивной дискеты DOS). Вы должны всегда иметь по меньшей мере две таких дискеты, с обязательным наличием наклейки защиты от записи;

(б) использовать замечательную утилиту PC Tools (Central Point Software) или Norton Utilities (Peter Norton Computing) для последовательной проверки (сравнить с оригиналами, сверить размер, дату и т.д.) начального загрузчика (он обычно занимает один сектор дискеты), управляющей программы загрузки (Master Boot Record) для жесткого диска, системных файлов и т.д. Если вы не любите проводить время за просмотром шестнадцатиричного дампа (и вообще заниматься детальной проверкой), то можно рекомендовать метод «последовательного исключения подозреваемых»: начать загрузку MS-DOS в самой простой конфигурации, а затем, добавляя по одной программе в конфигурационный файл (CONFIG.SYS, или AUTOEXEC.BAT), вы можете попытаться постепенно приблизиться к месту «крушения». Вообще говоря, после инициализации жесткого диска (или дискеты) настоятельно рекомендуется немедленно сделать копию управляющей программы загрузки (хранящей также информацию о разделении (partitions) вашего жесткого диска), используя утилиту, подобную Saveboot. Не нужно полагаться на широко разрекламированные программы типа Norton Disk Doctor (Peter Norton Computing), Mace Utilities и другие. Поверьте опытному программисту, что они действуют разумно только в очень простых случаях, которые не так уж часто встречаются на практике. Вспомните русскую пословицу: «береженого Бог бережет». Желательно в конце рабочего дня, используя утилиту MIRROR (производства Central Point Software), сделать копию таблиц размещения файлов (FAT - File Allocation Table), справочник корневого каталога (root directory). Это дает дополнительную возможность для удачного восстановления поврежденной структуры диска. Возможные причины: вирусы типа "Vienna", COM-Killer (1-of-8 Virus) и некоторые самозагружаемые вирусы (bootable Viruses).

2. Обнаружена разница между активной (имеющейся) и используемой компьютером памятью.

Поясним на примере: компьютер имеет 640 Кбайт памяти, а использует только 638 Кбайт. Это легко обнаружить, например, с помощью популярной программы Norton Commander (Peter Norton Computing). К сожалению, всего несколько программ могут показать вам истинные причины этого:

(а) память была уменьшена до старта MS-DOS;

(б) последний контрольный блок памяти уменьшен в размерах. Здесь можно порекомендовать программу SYSMAP, эффективно анализирующую распределение памяти.

Для случая (а) существуют две причины: 1) самозагружаемый вирус; 2) многие новые компьютеры (в частности,на базе процессора Intel 80386), многие ROM-cards дисковых контроллеров используют пространство на вершине памяти (обычно размером 1-2 Кбайта) для своих внутренних целей (стек, временный буфер и т.п.). Рекомендуется тщательно изучить системную документацию, чтобы получить точное представление о том, как может происходить загрузка MS-DOS на вашей машине (к сожалению, чаще всего вы не найдете никакой информации об этом, и только опытный программист из анализа POST-code, ROM-on-card, сможет найти ответ).

Случай б) более неприятен. Можно достаточно уверенно утверждать, что наиболее вероятная причина этого - перемещение вируса в конец памяти (эта техника активно используется в последнее время, например, в вирусах Eddie, Jankee-1, 2, 3). Вы можете легко определить причину с помощью SYSMAP: посмотрите, какие вектора прерываний указывают на конец памяти (выше MS-DOS). Если номер одного из них равен 021h (33 десятичное), тогда присутствие вируса на вашем компьютере обнаружено (INT 021h - диспетчер системных функций MS-DOS). Как поступить в этом случае? Борьба с резидентными вирусами обычно похожа на очистку вашего дома от мусора, но помните, что оперативная память должна быть нейтральной, т е. в ней не должно быть никаких вирусных программ, ну, а дальше - существует огромное множество программ-дезинфекторов.

3. Сообщение с просьбой вставить дискету с COMMAND.COM.

Вообще говоря, это сообщение появляется после частичного или полного стирания транзитной части командного интерпретатора. Однако ,если есть уверенность, что предыдущая программа не могла стереть эту часть COMMAND.COM, тогда, вероятно ,- это новый источник ваших неприятностей. Вставьте защищенную от записи дискету и понаблюдайте: наиболее агрессивные вирусы пытаются неоднократно вполнить запись на диск (контроллер сбрасывается не один раз, как в случае вируса Eddie). Загрузите SYSMAP и посмотрите распределение памяти, а затем действуйте аналогично пункту 2б).

4. Сообщение о защите дискеты по записи

При загрузке файла с дискеты и, скажем, выполняя команду DIR, вы неожиданно получаете собщение о наличии защищенного диска в дисководе (случай, когда дискета с закрытой прорезью для светодиода). Это следствие ошибки, характерной для ранних версий вирусов (например, 1701/1704-Virus или COM-killer), которые не умели управлять поведением MS-DOS в критических ситуациях. Считайте, что вам повезло: чистка машины для данных версий вирусов - достаточно простое занятие.

5. Сообщение MS-DOS об отсутствии файла

После просмотра текущей директории вы набираете имя какого-нибудь файла и получаете сообщение от MS-DOS что файл не найден. Это может означать только одно, что действует вирус подобный программам Datacrime, Black Friday, 1168/1280 Virus. Еще не поздно и стертые файлы можно восстановить, а ваш компьютер - очистить от инфекции. Помните при этом, что очищение всегда проводится только с защищенных, проверенных дискет. Хочу предупредить вас том, что новейшие версии вирусов (серия Data Crime), помимо стирания файлов, часто восполняют теперь и полное уничтожение их содержимого. Постарайтесь всегда и везде где только возможно (а в черные дни обязательно) использовать защиту от записи и форматирования программынм способом (напр., FLU-SHOT, VACCINE, SOFTKEY) или аппаратным путем (для дискет).

6.MS-DOS не распознает жесткий диск

После включения машины операционная система не загружается с жесткого диска, а при загрузке с дискетты винчестер не распознается MS-DOS драйверами. Наиболее вероятные причины (см. также пункт 1): повреждение системных таблиц или некоторых файловых структур на диске (напр. вирусом Eddie). Очень неприятная ситуация: предстоит тщательный поиск поврежденных мест, к примеру, изменение нескольких байтов в BPB (BIOS Parameter Block) приводит к неверному построению некоторых внутренних таблиц для MS-DOS, а следовательно, к невозможности загрузки различных программ.

7. Резидентные программы.

Начиная с версии 3.0, каждая программа имеет собственную копию программной среды - окружение (environment). Именно отсюда большинство утилит памяти получает имя программы. Если же это имя недоступно и нет других предположений, тогда принято считать программу неизвестной (unknown). Почти все вирусы, использующие стандартные приемы резидентных программ (TSR-technique), являются неизвестными (ведь они - инородное тело). Это может послужить сигналом тревоги. Для проверки ваших подозрений посмотрите перехваченные вектора прерываний, обращая внимание на следующие: 08h (таймер), 013h (диск), 01Ch (user ticks), 021h (MS-DOS диспетчер), 028h (MS-DOS multitasking idle). Большинство вирусов используют именно эти прерывания (например, Jerusalem, Data-Crime I, II, 1701/1704-Virus). К сожалению, и обычные программы часто применяют аналогичные приемы, поэтому для любой постоянно используемой программы у вас должна быть техническая документация согласно стандарту коммерческого программного обеспечения. При отсутствии таковой следует искать другие источники, например, использовать электронную энциклопедию INT90.LST (автор - Ralf Brown). Обратите внимание, что некоторые вирусы маскируются под широко известные программы, пытаясь притупить вашу бдительность. Последнее замечание: лишь искушенный программист в состоянии мгновенно обнаружить присутствие вируса среди множества резидентных программ (подскажет интуиция и опыт!).

Я описал лишь некоторые из встречающихся ситуаций и постарался объяснить, как и почему надо действовать там или здесь. Очень часто, как автор указывал ранее, пользователи относят проблемы с оборудованием к проискам вирусов, однако, здесь возможны иные причины, среди которых могут быть конфликты адаптеров, несовместимость (полная или частичная) контроллеров и управляемого ими оборудования, неверное соединение или подключение, сбой в питающей сети, повреждение на плате (даже микроскопические трещины ужасны!), большие температурные колебания, отсутствие заземления ЭВМ и т.д. В этом случае рекомендуется тщательнее читать приходящую документацию или получить консультацию у специалистов.

В заключительной части статьи я хотел бы еще раз напомнить: **безопасность - это прежде всего внимание**.

Следование приведенным ниже рекомендациям позволит вам не только обезопаситься от возможного проникновения вирусов в ваш компьютер, но и в случае, если он все-таки прорвется через все оборонительные

бастионы, быстро восстановить все повреждения и сохранить в целости все программы и данные.

Правило I.

Никогда не используйте неизвестного программного обеспечения. Это справедливо для всех программ типа «freeware», т.е., свободно распространяемых. Попросите программистов проверить эти программы перед их использованием или используйте вирус-детекторы. Известно много случаев, когда при демонстрации красивых картинок и звучании приятной мелодии уничтожается хранящаяся на диске информация.

Правило II

Не работайте с оригиналами. Все оригинальные программы должны быть защищены от записи и храниться в месте, доступном малому числу людей. Вы должны работать только с рабочими копиями.

Правило III

Перед окончанием работы обязательно сделайте копии программ или данных.

Правило IV

В конце недели обязательно сделайте копию всего жесткого диска. Если и случится страшная неприятность (например, кто-то переформатировал ваш жесткий диск), то вы, в этом случае, потеряете только одну неделю работы, а не многомесячный труд.

Правило V

Используйте утилиты распределения памяти. Как можно быстрее получите их, изучите и применяйте постоянно (например, SYSMAP, VTSR, MEM, MMAP и т.д.).

Правило VI

Защищайте наиболее важные из программ. Используйте для этой цели вирус-протекторы (например, VPCINST - Virus Protection Code Installation). Они не только восстановят (очистят) ваши программы в случае заражения, но и сообщат о проникновении вируса на вашу машину.

Правило VII

Предупредить несанкционированный доступ к вашим данным.

Это - одна из наиболее трудных задач, стоящих перед владельцем персонального компьютера. На сегодняшний день удовлетворительных решений нет, однако наиболее подходящие пути решения этой проблемы следующие:

(1) закрыть ЭВМ на ключ, убрать в бронированную комнату;

(2) использовать системы "пароль на входе" (аппаратно и/или программно);

(3) ввести ограничения для использования (просмотра, чтения, записи и т.д.) дискового пространства, т е. использовать права доступа.

(4) на машинах классах IBM-PC/AT можно запретить загрузку MS-DOS с дискеты (например, программа LOCKDISK).

(5) можно приобрести дополнительную программно-аппаратную защиту (Security cards).

Обзор отечественной литературы, посвященной вирусным заболеваниям персональных ЭВМ, к сожалению, наводит на грустные размышления. Практически все опубликованные статьи носят либо чисто описательный характер (как мы вчера с вирусом сражались!), либо это - теоретические размышления, большей частью не подкрепленные необходимыми выводами и достаточным практическим опытом. Ниже приводятся краткие замечания к четырем статьям, доступным большинству читателей на русском языке. Я полагаю, что положительные стороны этих статей читатель оценит сам, мне же хотелось бы зафиксировать внимание на недостатках и характерных ошибках.

1.*Абрамов С. и др., Компьютерный вирус; Микропроцессорные средства и системы; 2, 1989.*

а) Описание того, как авторы впервые в жизни боролись с вирусом, представляет интерес только для их домашних, но никак не для большинства обычных пользователей, которые нуждаются в более конкретных рекомендациях и советах.

б) Из статьи следует, что с вирусом Vienna борьба продолжалась несколько дней, в то время как профессиональная сервисная служба затрачивает от 0.3 до 3 часов на восстановление данных, включая время написания программы-дезинфектора, если существующие версии оказываются бессильны.

в) Невозможна полная классификация типов вирусов, о построении которой говорят авторы, а уж тем более их различных схем заражения, по причине быстрого развития компьютерной индустрии.

2.*Чижов А., Некоторые соображения по поводу компьютерных вирусов; В мире персональных компьютеров, 1, 1988.*

а) Неверная классификация вирусов (собственно говоря неясно, какие критерии использовал автор для создания классификации).

б) Плохое представление о внутреннем устройстве MS-DOS, и, следовательно, неправильное понимание механизмов действия различных типов вирусов.

в) Схемы заражения различных типов файлов, по меньшей мере, неполны и изобилуют грубыми неточностями, например, вопреки утверждению автора, командные файлы легче и больше заражаются вирусами.

г) Обнаружить резидентный вирус, используя предложения автора, вам удастся разве только в «двенадцатую ночь», поскольку так и осталось неясным, что же надо искать (программа SYSMAP облегчает данную задачу на 90%);

3. *Карасик И., К вопросу о компьютерных вирусах; В мире персональных компьютеров, 3, 1989.*

Карасик И., Несколько слов о компьютерных вирусах. Интеркомпьютер 1, 1989

а) Недостаточно глубокое знание DOS и BIOS. Например, для компьютеров фирмы IBM бессмысленно использовать 1701/1704 Virus, так как фирма поставляет маломощный динамик для своих машин (звуковой эффект вируса будет отсутствовать).

б) Предложенное выдергивание дискового контроллера из работающего компьютера или запись на аппаратно-защищенные дискеты свидетельствует о веселом настроении автора, но никак не о его профессиональной квалификации.

г) Многие неточности и ошибки сводят на нет и то немногое положительное, что имеется в этих статьях. Например, автор утверждает, что реальная длина файла больше указанной в его описании. Ничего подобного. Просто смешиваются два понятия: длина файла (в байтах) и занятое данным файлом дисковое пространство (в кластерах). Что касается способов размещения вируса в программе, не изменяя явно ее длину, то они существуют. Но как их реализовать, знает только сама фирма MICROSOFT и хакеры, изучившие MS-DOS буквально под «микроскопом».

4. Безруков Н.Н., Компьютерная вирусология; КИИГА, 1990.

Пространный обзор, который, вопреки утверждению в предисловии его автора, можно назвать только популярным, но никак не профессиональным изложением, которое бы осуществляло перспективное исследование проблемы и разработку инновационных методов. Пожалуй, это пособие сможет стать со временем своеобразной историографией вирусов.

Безусловно, в небольшой статье трудно рассказать о многих методах защиты и схемах вирусных программ. В последнее время авторы вирусов стали применять все более тонкую и изощренную технику, что обусловлено появлением более полной информации о MS-DOS.

Тем не менее, автору хотелось бы надеяться, что в этой статье предлагается эффективный подход к проблеме безопасности для персональных компьютеров. Известно, что многие пользователи испытывают просто-таки панический страх перед вирусами, однако хочу заверить читателя, что *квалификация лучших специалистов по защите информации много выше, чем самого талантливого автора самого страшного вируса - и эти специалисты думают о вас и вашей безопасности.*

Дмитрий Стефанков