Усенков Дмитрий Юрьевич

КОМПЬЮТЕРНЫЕ ВИРУСЫ: «БОРЬБА БРОНИ И СНАРЯДА»

Опять с утра у программиста болит голова и двоится в глазах. Да и компьютер явно нездоров – изображение на экране периодически переворачивается вверх ногами, а буквы осыпаются, как осенняя листва под порывами ветра: где-то в программах засел маленький злобный вирус. Придется спросить в аптеке панадол и для себя, и для электронного друга...

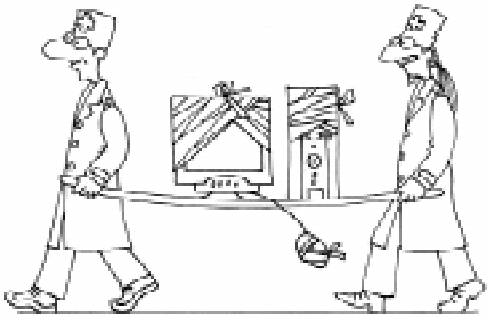
Среди множества компьютерных программ есть и такие, которые созданы и действуют отнюдь не с благими целями: незримо, «яко тать в нощи», проникают они на ваши диски, заражая имеющиеся там другие программы, размножаются, многократно копируясь, и вот уже, словно эпидемия чумы, «расползается» эта «информационная зараза» от диска к диску, от компьютера к компьютеру. Некоторые из таких программ ограничиваются мелким хулиганством, замедляя работу компьютера, вызывая «осыпание» выведенного на дисплей текста или выводя на экран картинки непристойного содержания. А некоторые, особо «злобные» экземпляры, способны портить, а то и вовсе уничтожать записанные на диске программы и данные. Имя этих «врагов Homo Computicus» известно, наверное, любому пользователю: это компьютерные вирусы.

Сам термин «вирус» в качестве названия заражающих компьютеры саморазмножающихся вредоносных программ, по аналогии с вирусами биологическими, предложил в 1984 году Ф. Коуэн в своей диссертации, с сообщением о которой он выступил на конференции по вопросам безопасности компьютерных систем. И хотя с тех пор прошло уже почти 15 лет, нельзя сказать, чтобы данная тема хоть сколько-нибудь потеряла актуальность. Так что же такое – компьютерные вирусы и как с ними бороться? Об этом и пойдет наш дальнейший разговор.

1. ОТКУДА ОНИ БЕРУТСЯ?

Прежде всего, любой компьютерный вирус – это программа, способная в ходе исполнения создавать собственные копии и «привязывать» их к другим файлам таким образом, чтобы при их запуске на «здоровом» компьютере первым получил управление именно вирусный фрагмент, который немедленно возьмет ситуацию в «Стране Электронии» под свой контроль. А это означает, что, в противоположность извечному вопросу курицы или яйца, у любой вирусной эпидемии существует (правда, к сожалению, далеко не всегда обнаружимый на практике) источник – вирус-прародитель, написанный и вручную запущенный в работу конкретным автором.

Причины, по которым программисты вдруг становятся на путь «абстрактного зла», могут быть различными. Перечислить все их здесь вряд ли удастся, но наиболее распространенные из них следующие.



Да и компьютер явно нездоров...

• *Вредность характера.* Есть, знаете ли, такие люди, сущность которых великолепно характеризуется поговоркой: «У соседа сдохла корова. Казалось бы, какое мне дело? А приятно!». Склонность к хулиганству у них, что называется, «в крови», только одни из них ломают скамейки в парке, а другие (в минимально необходимой степени научившиеся программированию) – пишут вирусы специально, чтобы подпортить настроение другим пользователям.

• *Самомнение и нездоровое стремление к славе.* Обычно такие «вирусописатели» – это школьники и студенты, только что освоившие программирование на ассемблере или другом «системном» языке (Си, Паскале или даже VisualBASIC'е). Хочется показать всем: мол, вот я какой, даже вирус могу собственный сконструировать! Подобные «творения», как правило, не содержат в себе каких-либо особенных алгоритмических хитростей, пишутся по одним и тем же типовым «схемам» (а то и вовсе берется готовый исходный листинг – его можно «скачать» с некоторых BBS, если знать, с каких, и к нему дописывается другая подпрограмма, активизируемая при заражении), и отличаются огромным количеством ошибок в исполняемом коде, которые иной раз и причиняют наибольшую часть вреда.

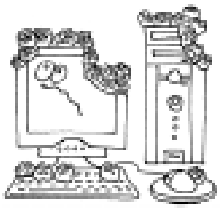
Откуда они берутся?

• *Обиженные и мстители.* Очень часто вирус является «последним подарочком» руководству фирмы от программиста, обиженного незаконным (во всяком случае по его мнению) увольнением или недостаточной оплатой уже проделанной работы. А в некоторых случаях вирусы пишутся и в знак протеста против государственной политики, например, один из макровирусов, заражающих документы WinWord, вставлял в тексты призыв к прекращению Францией ядерных испытаний.

Еще один возможный источник вирусов – компьютерное пиратство. Говорят, что некоторые программисты встраивают в свои творения скрытые вирусы, «молчащие» в легально распространяемых копиях и «пробуждающиеся», если попытаться взломать защиту от несанкционированного копирования. Однако это, скорее всего, «страшилки» с целью отвадить рядового «юзера» от пользования ворованным «софтом», поскольку подобная защита от пиратства – это все равно что подключить к охранной сигнализации ядерную бомбу: вору, конечно бы, и поделом, но ведь пострадают и ни в чем не повинные окружающие! Ну, а ежели подобная, с позволения сказать, «защита» будет кем-то реализована, ... думаю, каждому ясно, что с ее создателем следовало бы сделать.

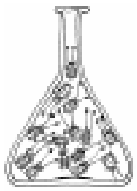
И наконец, скажем пару слов по поводу легенды о самозарождении вирусов. Согласно классическим канонам, этого не бывает и быть не может. Но пару лет назад в журнале «Техника молодежи» появилась любопытная статья Л. Щекотовой «Жить и умереть в компьютере», повествующая об одном эксперименте профессора Делавэрского университета Томаса С. Рэя. Суть его сводилась к попытке создать модель эволюции, «запустив» в некую «виртуальную среду», названную Тьеррой, экземпляр саморазмножающейся (но не заражающей другие!) программы, потомки которой, исчерпав доступные ресурсы свободной памяти, должны были вступить в конкуренцию друг с другом за выживание. При этом в системе действавали «мутации» (в случайный момент произвольным образом изменялся случайно выбранный код в теле какой-либо из программ) и «естественный отбор» (уничтожение экземпляров программ, ставших неработоспособными в результате «мутаций», а также «состарившихся» – совершивших определенное число размножений). Результаты оказались ошеломляющими. Из единственного типового «предка» в скором времени образовались

(заметим, самопроизвольно!) совершенно другие виды «псевдоживотных», среди которых были и такие, которые перешли на паразитический «образ жизни», внедряясь в другие программы-жителей Тьерры и заставляя их воспроизводить себе подобных. Более того, появились среди них и такие, которые самостоятельно «освоили» хитроумный алгоритмический трюк – «раскручивание петли», известный не каждому программисту и заключающийся в выполнении за один заход по три процессорных команды. Вообще же, по мнению Рэя, Тьерра – это уже не модель жизни, не ее имитация. Это – сама жизнь, только существующая в информационном мире, а не в материальном. Так что, хотя пока самозарождение компьютерных вирусов считается невозможным, теоретически такая опасность все-таки существует.



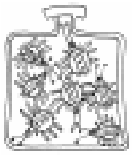
2. ВИДЫ ВИРУСОВ

Компьютерные вирусы принято разделять на несколько классов по принципу распространения заражения ими. Рассмотрим кратко эти классы.



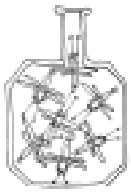
• *Загрузочные (boot-вирусы).* Загрузочные вирусы заражают загрузочный сектор дискет или жесткого диска, помещая в нем команды запуска на исполнение самого вируса, который находится где-то в другом месте этого диска. Сразу после включения питания компьютер обращается к загрузочному сектору, и в результате сразу после загрузки операционной системы в оперативной памяти оказывается и вирус, который затем во время работы с ПЭВМ начинает заражать загрузочные секторы всех дискет, с которыми пользователь производит обмен информацией. Соответственно, заражение «здоровой» машины происходит, если при ее запуске или перезапуске в дисководе окажется зараженная дискета (безразлично, системная или нет) и компьютер обращается к ней в попытке загрузить операционную систему.

• *Файловые вирусы.* Эти вирусы заражают исполняемые файлы (с расширениями .com, .exe, .sys) путем дописывания своей основной части («тела») в конец заражаемой программы, а «головы» – в его начало. Когда ничего не подозревающий пользователь запускает такую программу на выполнение, «голова» вируса передает управление «телу», и таким образом вирус попадает в память ПЭВМ, а затем уже исполняются переписанные из начала программы в ее конец несколько первых байтов (место которых заняла «голова» вируса), и, наконец, управление передается на оставшуюся часть самой программы. Вирус же, оставаясь в памяти в течение всего времени работы, заражает любой запущенный после этого исполняемый файл. При выключении питания компьютера и последующем его включении (а также при перезапуске по кнопке Reset) вирус в памяти уничтожается (поскольку ОЗУ при этом обнуляется), но «горячий» перезапуск по Ctrl+Alt+Del некоторые модификации вирусов способны «пережить» совершенно спокойно. Передача файловых вирусов с одного компьютера на другой происходит при переносе пользователем зараженных файлов и их последующем запуске (если же зараженная программа будет заархивирована, находящийся в ней вирус превратится в «мину замедленного действия» и «проснется» сразу, как только вы распакуете архив и запустите эту программу). Характерный признак заражения файла – увеличение его длины по отношению к прежней.



• *Файлово-загрузочные вирусы.* Это своего рода помесь первых двух типов, заражающая как исполняемые файлы, так и загрузочные секторы. При этом файловый механизм в основном обеспечивает распространение вируса между компьютерами (поскольку сегодня редко кто загружается с дискет), а boot-механизм – возобновление вируса в памяти после выключения/включения питания или после перезапуска по Reset.

• *Bat-вирусы* (не путать с boot). Это наиболее простые вирусные программы. После запуска вирус создает командный файл с расширением .bat и добавляет его вызов в файл autoexec.bat, получая, таким образом, возможность попасть в ОЗУ после включения или перезапуска (альтернатива boot-механизму). Кроме того, некоторые файловые и файлово-загрузочные вирусы также способны изменять содержимое autoexec.bat, например, дописывая строку с командой форматирования винчестера сразу после очередного запуска ЭВМ. Использованный здесь способ заражения вряд ли способен породить крупные «эпидемии» и скорее служит средством для «удержания позиций в отдельно взятом компьютере» либо дополнительным эффектом в вирусах другого типа.



• *Макро-вирусы.* Когда-то считалось, что текстовые файлы не способны служить разносчиками «инфекции». Но с появлением офисных программ для Windows (таких как WinWord, Excel, Access и других) положение резко изменилось. Дело в том, что фирма Microsoft реализовала в них довольно прогрессивную идею программирования макрокоманд, когда допускается возможность присвоить какой-либо клавише не только ту или иную последовательность символов (именно так понимается макрос, например, в текстовом редакторе Лексикон), но и вызов достаточно сложной программы, написанной на встроенном БЕЙСИКоподобном языке программирования. С одной стороны, это существенно увеличило потенциальные возможности программ, позволяя наращивать их практически любыми новыми функциями, а с другой – породило возможность создавать на этом встроенном языке вирусные программы. Ведь макросы сохраняются и в файле шаблона normal.dot (который, по умолчанию, вызывается в качестве «базы» при создании любого нового текста в WinWord) и в созданных на его основе doc-файлах, а макрос с именем autoexec автоматически получает управление сразу после открытия в WinWord содержащего его файла или при запуске самого WinWord, если этот макрос содержится в normal.dot. Так что, как легко заметить, здесь налицо все классические условия для «сна», заражения и распространения вирусов! В последнее время, когда почти весь документооборот практически во всех организациях выполняется при помощи WinWord, электронных таблиц Excel и пр., макро-вирусы уверенно выходят на первые позиции по числу заражений.

• *«Черви».* В некоторых современных версиях архиваторов предусмотрена возможность создания аналога autoexec: можно добавить в архив текстовый файл, содержащий команды, которые будут выполнены сразу после распаковки данного архива. Таким образом, вполне можно создать вирус, написав некую программку, способную дописывать к имеющимся на диске архивам свои копии в виде com-программы и сопровождать их автоматически срабатывающими при разархивации командами запуска такой com-программы. Подобные вирусы уже реализованы, по имеющейся у автора информации, для архиваторов ARJ и ZIP; думается, что сравнительно недавно появившийся архиватор RAR также представляет собой «лакомый кусок» для вирусописателей, поскольку предоставляет возможность создания сценариев процесса распаковки самораспаковывающихся архивов. Отметим, что «черви», по сути, очень близки к макровирусам.

В дополнение к этой классификации отметим еще несколько отличительных особенностей, характеризующих некоторые файлово-загрузочные вирусы.

• *Полиморфизм.* Большинство вирусов, созданных в прежние годы, при саморазмножении никак не изменяются, так что «потомки» являются абсолютно точной копией «прародителя», что и позволяет легко их обнаруживать по характерной для каждого последовательности байтов. Однако в последнее время создатели вирусов реализовали идею шифровки тела вируса (чтобы нельзя было деассемблировать та-

кой вирус – превратить его исполняемые коды обратно в исходный листинг с целью изучения его работы и создания «противоядия»). В этом случае вирус включает в себя также и расшифровщик – коротенькую подпрограммку, расшифровывающую составляющие его коды для их исполнения процессором. А при заражении другого файла шифровка производится с другим «паролем», так что для нескольких разных копий одного и того же вируса невозможно (не произведя расшифровку) отыскать характерную байтовую последовательность.

• *«Стелс»-технология.* Этот термин появился по аналогии с названием технологии разработки американского бомбардировщика, невидимого на экране радара. Стелс-вирус, находясь в памяти компьютера, перехватывает почти все векторы прерываний (то есть переписывает адреса вызова служебных подпрограмм операционной системы на свои). В результате при попытке контроля длины зараженного файла ДОС выдает старую, «правильную» длину вместо истинной, а при просмотре в деассемблере коды вируса исключаются им из рассмотрения.

Упомянем также (для полноты картины) еще несколько видов разрушительных программ, не являющихся вирусами, поскольку не способны к саморазмножению.

• *«Логические бомбы».* Такая программа добавляется к какой-либо полезной программе и «дремлет» в ней до определенного часа. Когда же показания системного счетчика времени данного компьютера станут равными установленному программистом значению часов, минут и секунд (или превысят их), производится какое-либо разрушающее действие, например, форматирование винчестера. Это – один из распространенных вариантов мести обиженных программистов своему руководству.

• *Программы-вандалы.* Самый простой способ напакостить всем и вся. Пишется программа-разрушитель (например, все тот же форматировщик винчестера), ей дается название, такое же, как у другой, полезной программы, и она размещается, скажем, на BBS в качестве «обновленной версии». Ничего не подозревающий пользователь обрадованно «скачивает» ее на свой компьютер и запускает, а в результате – лишается всей информации на жестком диске. Подобная история случилась сравнительно недавно, когда форматировщик был «замаскирован» под новую версию популярного архиватора ZIP.

Разговор о видах вирусов можно подытожить следующим выводом. Возможность распространения компьютерных вирусов возникает только тогда, когда имеется подходящая для этого «среда», обладающая как минимум следующими тремя особенностями:

а) имеется место, где вирус может сохраняться, когда компьютер выключен;

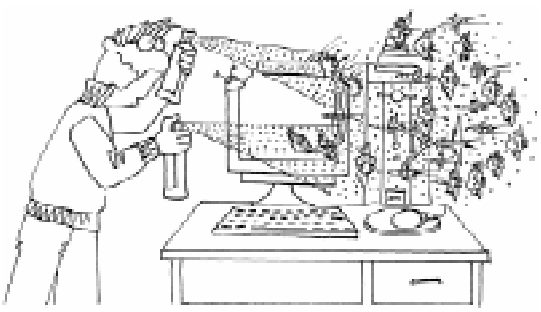
б) существует «носитель инфекции» – файл или служебная область диска, причем существует реальная возможность переноса его на другие компьютеры (на дискетах или по сети) и активизации (запуска программы или передачи управления с загрузочного сектора);

в) есть возможность возобновления (реактивизации) вируса после включения либо перезапуска компьютера (для макровирусов – после запуска программы, в среде которой они паразитируют).

Таким образом, передача вируса в чисто текстовых (ASCII-формат) или в графических файлах невозможна (если только какой-либо разработчик ПО не предусмотрит для них «встроенные макросы» вроде того, как это произошло для документов Word), а зараженные исполняемые файлы, документы WinWord и загрузочные сектора дискет являются лишь «резервуарами инфекции» и совершенно безопасны до тех пор, пока вы не запустите зараженную программу на исполнение, не загрузите doc-файл в WinWord или не загрузитесь с зараженной дискетки.

3. СРЕДСТВА ПРОТИВОДЕЙСТВИЯ

Для борьбы с компьютерными вирусами используются специальные программы – антивирусы, которые мы рассмотрим в основном на примере разработок известной в этой области фирмы «Диалог-Наука».



Средства противодействия

Антивирусные средства можно разделить на несколько типов.

• *Детекторы.* Это простейший вариант – программа, которая только обнаруживает присутствие вируса, но не лечит его (а зачастую даже не распознает конкретный тип вируса, сообщая лишь о факте заражения). Примером является детектор BOOTCHEK, в котором заложены копии всех возможных вариантов байтового содержимого загрузочного сектора для НЕЗАРАЖЕННЫХ дискет. Если загрузочный сектор проверяемой дискеты совпадает с одним из имеющихся, дискета считается здоровой, иначе – выдается сообщение о наличии boot-вируса. Разумеется, подобный класс программ сегодня считается безнадежно устаревшим.

• *Фаги.* Такие программы содержат в себе характерные последовательности байтов для всех отлавливаемых вирусов. Анализируемые файлы просматриваются на наличие таких характерных строк, и при их наличии предпринимаются действия по лечению зараженного файла, соответствующие данной характерной строке. Пример такой программы – всем известный aidstest (тоже, впрочем, ныне используемый очень редко).

Особо среди фагов следует выделить программу DrWeb, в которой реализован совершенно иной принцип «отлова» вирусов. При проверке файла, кроме поиска характерных строк, DrWeb имитирует (эмулирует) его исполнение и отслеживает все подозрительные действия, которые проверяемая программа пытается производить при работе. В отличие от прочих антивирусов, DrWeb способен проверять содержимое архивов, временно распаковывая их и просматривая каждый исполняемый файл, а также с высокой вероятностью обнаруживать новые вирусы, для которых неизвестны характерные байтовые строки, только по попытке выполнения ими заражающих действий. Кроме того, сразу после запуска DrWeb прежде всего тестирует оперативную память и при наличии в ней активного вируса уничтожает его, лишая, таким образом, стелс-вирусы возможности маскировки (aidstest же в подобной ситуации часто оказывается «в дураках», поэтому запускать его рекомендуется с заведомо «здоровой» и защищенной от изменений системной дискеты после перезагрузки с нее же). Современные же 32-разрядные версии DrWeb предусматривают в своем комплекте также резидентный модуль SpIDer Guard, загружающийся автоматически сразу после включения (перезапуска) компьютера и проверяющий все файлы в момент их копирования, открытия и пр., а также письма e-mail при их получении. Такой контроль в сочетании с периодической общей проверкой содержимого диска при помощи DrWeb, ставит достаточно надежный противовирусный заслон, в том числе при работе в локальной сети.

• *Ревизоры.* Такая программа (пример – антивирус ADinf) при первом вызове фиксирует и записывает в отдельном файле все сведения о существующих на винчестере файлах (расположение, длины, контрольные суммы), а также подробную информацию о содержимом загрузочного сектора. При последующих вызовах производится сверка запомненной информации с сохраненной, и если выяснится, что, например, длина какого-то исполняемого файла увеличилась или какой-то файл исчез с диска (возможно, стерт вирусом, а не удален самим пользователем), ревизор тут же поднимет тревогу, выдав на экран соответствующее предупреждение.

• *Сторожа.* Программа-сторож загружается в память компьютера сразу после его включения (или перезапуска) и постоянно отслеживает все действия других программ, выявляя среди них подозрительные (например, при попытке записи на диск у

пользователя запрашивается дополнительное разрешение с указанием информации типа: «программа XXX пытается произвести запись на диск»). Современные сторожа обычно работают в комплексе с фагами, как это и сделано в 32-разрядной версии DrWeb+SpIDer.

• *Вакцины.* Здесь за основу взята та же идея, что и при гомеопатии: «подобное излечивается подобным». Защищаемые файлы специально заражаются (часто – с помощью безвредных, то есть не предусматривающих разрушительные действия вирусов), чтобы «обмануть» настоящий вирус, создав у него «впечатление», что данный файл уже заражен (в большинстве вирусов предусмотрен контроль для предотвращения повторного заражения одного и того же файла). Способ довольно надежный и, главное, «самодействующий» – пустил «вакцинный вирус» гулять по миру, и все, но антивирусы других типов нередко принимают «подшитую» к программам вакцину за настоящий вирус и в попытке лечения могут испортить программу. Поэтому сегодня вакцины практически не используются.

Профилактика – лучшее лечение

• *«Убийцы» и контролеры макросов.* Специфические средства, ориентированные на борьбу только с макровирусами. Например, распространяемая «Диалог-Наукой» программа «Пристав» подключается «внутрь» WinWord и при наличии в открываемом файле макро-вируса выдает предупреждение. Другая программа с говорящим само за себя названием mkiller просматривает все находящиеся в данной поддиректории doc-файлы и удаляет из них все без исключения макросы, не разбираясь, «кто прав, кто виноват», – способ, что называется, радикальный. И наконец, в новых версиях WinWord предусмотрены собственные средства противодействия: начиная с версии 7.0 (она же – версия 95) пользователя предупреждают о наличии в открываемом документе любых макросов если помечен соответствующий флажок в настройках.

• *Аппаратно-программные средства.* В принципе, любая программа-антивирус может быть «обманута» каким-либо новым вирусом, создатель которого специально предусмотрел эту ситуацию. Вирус может даже изменить коды антивируса прямо в оперативной памяти так, что он откажется проверять файлы или даже начнет их портить. Поэтому и был создан аппаратно-программный комплекс Sheriff, включающий в себя, кроме специальной программы, также электронную плату, устанавливаемую внутри корпуса компьютера. Защита данных в этом случае ведется комплексно – не только от вирусов, но и от программ-вандалов и от «логических бомб» и даже от ошибочных действий самого пользователя. Грубо говоря, определенная область диска, в которой находятся исполняемые программы и прочие неизменяемые данные, просто-напросто объявляется закрытой для любых изменений, а все прочее дисковое пространство («открытое») отводится для хранения изменяемых файлов (документов, файлов конфигурации и прочих данных, которые, вспомним, заражению практически не подвержены, за исключением макровирусов).

4. ПРОФИЛАКТИКА – ЛУЧШЕЕ ЛЕЧЕНИЕ

Какие меры нужно предпринимать, чтобы не заразить компьютер? Исходя из рассмотренных выше типовых механизмов заражения, можно дать пользователям следующие рекомендации.

• Прежде всего, старайтесь пользоваться легальным программным обеспечением и относитесь с должной осторожностью к «новым версиям» популярных программ, распространяемым как «бесплатные» или «условно бесплатные».

• Любую дискету, побывавшую в другом компьютере, перво-наперво проверьте антивирусом, даже если вы целиком и полностью доверяете владельцу этого компьютера. (Забывчивых выручит SpIDer, но лучше и перестраховаться.)

• Если у вас «под началом» несколько компьютеров (например, учебный класс), рекомендуется выделить один из них (не подключенный к локальной сети!) в качестве «карантинного», и любые незнакомые программы запускать прежде всего на нем – это позволит выявить программы-«вандалы».

• Периодически (скажем, раз в неделю) проверяйте весь жесткий диск. При работе с DrWeb'ом можно установить следующий порядок: изредка (скажем, раз в два-три месяца) проверять все файлы, включая архивы; раз в неделю проверять все исполняемые файлы, исключая архивы; при поступлении новых программ и архивов надо проверять их прежде, чем запустить или распаковать.

• Любые важные для вас данные (в особенности уникальные) обязательно копируйте на дискеты и держите их в резерве. (Еще лучше использовать для резервного копирования CD-RW, тем более что их стоимость сегодня заметно снизилась.)

• Тщательно следите за тем, чтобы при включении и перезапуске компьютера в дисководе не стояла забытая дискетка. (Это должно быть у вас отработано, что называется, на уровне «безусловного рефлекса», а еще лучше, если позволяет имеющаяся на вашей ПЭВМ версия BIOS, совсем отключить загрузку с дискет.)

Интернет: опасность!

• Если заражение произошло, то нужно, «вылечив» содержимое винчестера, проверить все имеющиеся дискеты и иные съемные носители, а при наличии локальной сети провести такую проверку на всех входящих в нее компьютерах.

• Совет для учителя (хотя и несколько «драконовский»): если вы не уверены, что кто-то из учеников не принесет в класс зараженную дискетку с игрой, можно просто отключить питание дисководов у всех ученических машин, оставив подключенным дисководы только на компьютере учителя и передавая информацию исключительно по локальной сети.

5. ИНТЕРНЕТ: ОПАСНОСТЬ!

Если раньше мало кто из простых пользователей работал с компьютерными сетями, то ныне приобщение к Интернету стало массовым даже в нашей не слишком-то «продвинутой» в этом плане стране. Какие опасности могут подстерегать пользователя сети?

Прежде всего, остается в силе все сказанное ранее касательно обычных вирусов: переписывая из Интернет любые исполняемые программы, архивы и документы типа doc-файлов для WinWord, помещайте их в специально выделенный подкаталог и, прежде чем использовать, обязательно проверьте антивирусом. Остается и уже упомянутая опасность «напороться» на программу-вандала, «выдаваемого» за что-нибудь полезное; правда, в Интернет это происходит реже, чем в прежних BBS, поскольку владельцами Интернет-серверов являются чаще всего организации, а не частные лица. Но есть и ряд специфических опасностей, присущих только сети.

• *«Логические бомбы» – скрипты и апплеты.* Современные версии браузеров (программ для работы с WWW-страницами) поддерживают возможность размещать на Интернет-страницах небольшие программы, переправляемые пользователю в виде текстового листинга и исполняемые уже на пользовательском компьютере. Такие программы называются скриптами и пишутся

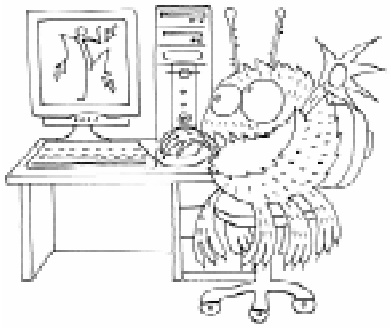
на специальном языке программирования JavaScript и на основе VisualBASIC. И хотя основные функции доступа к содержимому вашего диска здесь отключены, некоторые мелкие неприятности это может доставить. Кстати, в последнее время создатели некоторых сайтов (как правило, из разряда «только для взрослых») освоили любопытный вариант скриптов (на базе JavaScript), способных при открытии такой Web-страницы не только «прописать» адрес данного сайта в качестве «домашнего» (естественно, не спрашивая у посетителя разрешения), но и внести его непосредственно в системный реестр Windows в качестве «базового»: такие «фокусы» уже можно считать настоящим вирусом и привлекать владельцев таких сайтов к предусмотренной за такие деяния ответственности.

• *«Троянские кони».* Это модули, присоединяемые к каким-либо нормальным программам, распространяемым по сети, или «забрасываемые» в ваш компьютер несанкционированным способом. Цель «троянского коня» – воровать ценную информацию (пароли доступа, номера кредитных карточек и т. п.) и передавать ее тому, кто этого «коня» запустил. Рядовые пользователи Интернет, впрочем, встречаются с данной проблемой довольно редко, – чаще всего это проблема владельцев серверов и провайдеров. Однако же, если кто-то похитит у вашего провайдера ваши login и пароль входа в Интернет, чтобы воспользоваться ими, денежки будут уходить именно с ВАШЕГО счета...

• *Почтовые вирусы.* Сегодня электронная почта приобретает все большую популярность. Но вместе с этим значительно увеличилась и опасность проникновения вирусов через этот удобный канал глобального распространения. (Еще большую опасность, кстати, представляет собой популярный чат-клиент ISQ или, в просторечном наименовании, «аська».) Чаще всего заражение начинается с получения неизвестно от кого письма, содержащего исполняемую программу-«зародыш» (частенько очень хитро «замаскированную»: файл имеет, например, вид <имя>.jpg .exe, где перед завершающим и определяющим тип «исполняемая программа» указанием «.exe» записано большое число пробелов; Windows отображает для таких длинных имен только начало, пользователь воспринимает присланное как обычный файл с JPEG-картинкой и активизирует его клавишей Enter или двойным щелчком мыши для просмотра, тем самым запуская программу). Когда ничего не подозревающий пользователь запустит такую программу на исполнение, содержащийся в ней вирус «прописывается» в системе и, обращаясь к содержимому адресной книги, начинает тайком от вас рассылать всем абонентам свои копии-зародыши в качестве вложений. Впрочем, сегодня Outlook Express позволяет принимать письма в формате HTML, в том числе содержащие скрипты и обращения к серверным программным компонентам, причем с возможностью автозапуска скрипта в момент просмотра полученного письма, так что налицо еще одна потенциальная «лазейка» для вирусописателей.

6. ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ И РЕАЛЬНАЯ ВИРУСНАЯ ОПАСНОСТЬ

В заключение стоит, пожалуй, подумать и о будущем (возможно, что уже ближайшем). Сегодня человечество, по сути, стоит на пороге радикального изменения в информационных технологиях, способного коренным образом изменить не только чисто техническую сторону нашей жизни, но и само мировоззрение. Этот порог носит название «виртуальная реальность». Потенциальные возможности виртуальной реальности поистине колоссальны, и современные реализации на базе этой технологии игр, испытательных полигонов и прочего составляют лишь вершину айсберга. Если же задействовать механизмы VR «на полную мощность», человечество способно открыть для себя мир, свободный от ограничений материи, пространства и времени, мир, состоящий из информации и управляемый только информацией. Фактически это будет своего рода возвращением к магии, когда пользователь сможет одной лишь словесной формулировкой управлять не только окружаю-



Виртуальная реальность и реальная вирусная опасность

щим его виртуальным миром, но и изменять самого себя (точнее, свой виртуальный образ) так, как ему заблагорассудится.

Однако чем больше возможностей предоставляет та или иная технология, тем больше и скрытые в ней опасности. Не будем здесь говорить обо всех аспектах проблемы и затронем только то, что непосредственно касается темы данной статьи. Так, уже сегодня делаются первые попытки компьютеризации в хирургии и, в частности, первые эксперименты по проведению операций дистанционно посредством Интернет. Пока чаще всего это заключается лишь в участии в той или иной сложной операции консилиума профессоров, территориально находящихся в разных городах и обменивающихся информацией с хирургом, непосредственно производящим операцию, с помощью конференц-связи. В будущем же предполагается проведение операций (например, в удаленных селениях) роботами, дистанционно управляемыми хирургом. К чему может привести внезапное «вмешательство» вируса, думается, можно предположить уже сейчас.

То же касается управления военными объектами: в истории уже были случаи, когда третья мировая война чуть было не началась из-за сбоя компьютера. (Впрочем, это уже проблемы не только вирусные – сидя на бочке с порохом, взлететь на воздух рискует и некурящий.)

И, наконец, такой факт. Несколько лет назад американскими учеными было заявлено о ведении работ по вживлению микропроцессора в организм человека (пока с целями реализации очувствленных протезов), а также о том, что современная наука не видит принципиальных трудностей с вживлением процессора непосредственно в мозг, в том числе с подключением к глобальной сети баз данных. Сегодня же эксперименты по вживлению электронных компонентов в человеческий организм стало реальностью (примером являются эксперименты Кевина Варвика, профессора кафедры кибернетики Ридингского университета, Великобритания, и Мелоди Мо из Джорджиевского университета). К чему может привести распространение вируса в этом случае – остается только гадать. Как минимум – к появлению в известном заведении «имени Кащенко» соответствующего отделения «под началом» докторов Касперского и Веба...

Может быть, кому-то из читателей покажется, что автор чересчур сгущает краски: мол, это все если и будет, то очень не скоро. И все же, как бы то ни было, проблема компьютерных вирусов остается. А решать ее можно, пожалуй, только одним способом: путем ликвидации первопричин, побуждающих вирусописателей, как потенциальных, так и практикующих, создавать свои неприглядные «творения». Иначе «борьба брони и снаряда» будет лишь и дальше наращивать обороты.

Усенков Дмитрий Юрьевич,
старший научный сотрудник
Института информатизации
образования РАО.