Некоторые соображения по поводу компьютерных вирусов

А. А. ЧИЖОВ

В последнее время в газетах и журналах часто появляются сообщения о компьютерных вирусах. Что же это такое с профессиональной точки зрения? Как может быть „устроен" вирус, что может натворить, как его обнаружить?

Профессиональной информации о вирусах крайне мало. Доходит до того, что многие, в том числе и программисты, считают, что это настоящий вирус, который физически уничтожает компьютеры и дискеты. Это, конечно же, не так. Компьютерный вирус – это программа. Программа небольшая (обычно 0.5–3 Кбайт), сложная, тщательно составленная и опасная.

Теперь о вирусах более серьезно. Вирусом будем называть программу, которая самостоятельно может размножаться, переносить себя на диски и дискеты, прикреплять к программам, передавать по сети. Обычно такая программа создается для того, чтобы нарушить работу компьютера.

„Жизнь" вируса представляет собой некий цикл, по осуществлении которого он перемещается с одной дискеты (программы) на другую. Цикл состоит из этапов загрузки, запуска, настройки, включения, внедрения.

В память ПК вирус загружется вместе с программой, в которой он находится. При этом запуск программы включает в себя и запуск вируса. Перед реализацией своего злого умысла вирус настраивается: переписывает себя на другое место в памяти, модифицирует операционную систему или выполняет какие-то другие действия по своему обустройству в ПК. Чтобы пользователь ПК не мог определить, откуда к нему попал вирус, вредительству предшествует „инкубационный период", который может продолжаться несколько дней, недель, месяцев. После окончания „инкубационного периода" вирус включается и начинает вредить. Как во время „инкубационного периода", так и после своего пробуждения вирус пытается переписывать себя в подходящие программы. Каждый вирус создан для внедрения в определенные типы программ.

Сначала рассмотрим различные типы вирусов, затем чем вирусы могут навредить, каким образом их можно обнаружить и как с ними бороться. Я вижу следующие типы вируса:

1. Вирус, внедренный в операционную систему на системном диске или дискете.

2. Вирус, внедренный в прикладную или системную программу.

3. Вирус, внедренный в объектную библиотеку какого-либо компилятора.

4. Вирус, внедренный в сетевой драйвер (программу обеспечения работы сети).

1. Вирус в операционной системе. Этот тип вируса прикрепляется к системной части дискеты или жесткого диска („винчестера"). В системную часть дисковой операционной системы (ДОС) входят загрузчик, находящийся в нулевом секторе диска (или раздела ДОС на „винчестере"), два скрытых файла ДОС (IBMBIO.COM и IBMDOS.COM для PC DOS, IO.SYS и MSDOS.SYS для MS DOS) и командный процессор COMMAND.COM.

Вряд ли вирус может внедриться в загрузчик, так как загрузчик должен размещаться в одном секторе диска емкостью 512 байт. В загрузчике практически нет свободного места.

Другое дело – скрытые файлы ДОС. Вирус может прикрепиться к любому из этих файлов, при этом его дальнейшее поведение может быть различным. Само прикрепление происходит просто – вирус может дописать себя в конец одного из файлов. При запуске каждого из скрытых файлов управление передается на начало файла, в котором стоит команда перехода на инициализатор соответствующей части ДОС, вместо которой вирус может поставить переход на свое начало, а после настройки запустить инициализатор ДОС. Наиболее действенным может быть прикрепление вируса ко второму скрытому файлу – IBMDOS.COM (MSDOS.SYS), так как, во-первых, в конце первого файла находится конфигуратор системы, обрабатывающий файл CONFIG.SYS, что мешает прикреплению вируса, во-вторых, в момент запуска первого скрытого файла ДОС еще не функционирует. В момент же запуска второго скрытого файла ДОС уже частично функционирует, полностью сформированы драйверы ввода-вывода.

После того как вирус вместе с программой-„носителем" попал в память ПК, ему необходимо настроиться на конкретную версию ДОС и остаться резидентно в памяти ПК. Это можно сделать двумя методами. Первый метод – вирус переносит себя в конец поля памяти, доступного ДОС, изменяет внутренние поля ДОС и базовой системы ввода-вывода так, чтобы они не знали о существовании памяти, которую занимает вирус. Второй метод предполагает изменение внутренних полей ДОС, которые используются при вычислении ее размера. При этом вирус становится как бы частью самой ДОС. Естественно, что вирус должен очень хорошо знать внутреннюю структуру и адреса некоторых полей ДОС, причем для разных версий. Вирус, загруженный вторым методом, значительно труднее обнаружить.

Третий файл ДОС – командный процессор – может быть использован для внедрения вируса несколькими методами. Командный процессор состоит из двух частей: резидентной и подзагружаемой. Вирус может прикрепляться как к этим

двум частям, так и использовать другие пути: он может переносить себя на самый конец свободного поля памяти ПК, может потребовать у ДОС отдельный блок памяти, располагающийся сразу после резидентной части командного процессора. В файле командного процессора вирус может находиться как в его начале (что наиболее вероятно, так как просто реализуется), так и в середине – между резидентной и подзагружаемой частями. Второй способ маловероятен, так как при размножении вирусу требуется раздвижка файла, а это сложная операция.

Так как вирус расположен в ДОС, то и попадать в компьютер он может только во время загрузки ДОС. Вирус может при попытке записи на носители переносить себя на новые дискеты (диски). При этом вирус должен проверять, что дискета (диск) – системная, т. е. содержит ДОС. Распространяться такой вирус будет очень медленно на компьютерах с диском типа „винчестер" и очень быстро на компьютерах без такого диска. Это связано с тем, что если на компьютере есть „винчестер", то запуск ДОС обычно производится с него. Вирус же может установиться на компьютер (и на „винчестер") только после запуска ДОС с зараженной дискеты. Таким образом, у нас этот вирус опасен в основном для тех, у кого нет „винчестера", например для пользователей советских ПК, опасность для пользователей ПК с „винчестером" мала.

2. Вирус в программе. Второй тип вируса – внедряющийся в отдельно взятую прикладную или системную программу. Это может быть файл типа .COM или .EXE. В связи с более гибкой структурой файлов типа .EXE вирус легче внедрить в файл именно этого типа. Существуют два метода сделать это: между таблицей настройки на место загрузки и собственно программой и после собственно программы в конце файла.

Внедрение вируса между таблицей настройки и собственно программой имеет факторы, как облегчающие внедрение, так и затрудняющие его. Среди факторов, облегчающих внедрение, можно выделить следующие: фиксированное местонахождение вируса в программе, а значит, меньшая настройка при внедрении вируса, автоматическое выделение места под вирус в памяти ПК при загрузке зараженной программы, возможность использования для хранения вируса в памяти тот же блок памяти, который использует и сама программа, за счет чего значительно труднее идентифицировать наличие вируса – он не занимает отдельных блоков памяти.

Факторы, затрудняющие использование этого метода, связаны в основном с процессором внедрения вируса: для внедрения вируса надо раздвинуть файл, что часто невозможно для программ на дискетах и обычно требует долгого переписывания файлов, так как в ДОС нет средств для раздвижки файлов. После загрузки вируса, внедренного в середину .EXE-файла, он практически не может остаться на том месте, на которое загрузился, так как это место принадлежит другой программе, в то время как вирус должен остаться резидентно в памяти компьютера. Поэтому он должен перенести себя на конец свободного поля памяти, после чего необходимо подвинуть программу, в которую внедрялся вирус, на то место, на которое она была бы загружена при отсутствии вируса. Перенесение программы требует повторной настройки на место загрузки, для чего должен быть заново прочитан с диска заголовок .EXE-файла. Таким образом, видно, что подключение вируса в середину .EXE-файла возможно, но трудоемко.

Вирус можно внедрить и в конце .EXE-файла. При этом вирус должен переносить себя на конец свободного поля памяти ПК, другого места для него нет. Но можно прикрепить вирус к концу не каждого .EXE-файла. Например, практически нельзя прикрепить вирус к программе, имеющей оверлейную структуру, так как она может просто не поместиться в память целиком.

В принципе, вирус можно внедрить и в файл типа .COM, но при этом возникает много проблем при запуске вируса и последующем запуске программы, к которой он прикреплялся.

3. Вирус в объектной библиотеке. Вирус, прикрепленный к объектной библиотеке какого-либо компилятора, – наиболее изощренный вид вируса. Такой вирус автоматически внедряется в

ОТВЕТСТВЕННОСТЬ ЗА НЕЛЕГАЛЬНОЕ КОПИРОВАНИЕ

Суд штата Флорида принял решение, по которому не только корпорации, но и конкретные чиновники несут ответственность, если служащие нелегально копируют программное обеспечение.

ВИРУСЫ ПОРАЖАЮТ ПК MACINTOSH

Компьютерные вирусы поразили ПК типа Macintosh фирмы Apple в NASA и в торговых офисах фирмы Apple. Представитель Apple объявил, что фирма проведет расследование с целью найти автора вируса и привлечь его к ответственности. Вирус не поражает файлов с данными, но все приложения, включая системные файлы, приходится стирать, чтобы избавиться от вируса. Представитель фирмы рекомендует оригинальные программные диски держать защищенными против записи. Вирус проявляет себя различными способами на 2-, 4- или 7-й день: модифицируя программы, стирая файлы, вызывая сбои во время печати, зависание системы, исчезновение вспомогательных резидентных программ и пр. Представитель фирмы назвал этот вирус „весьма изощренным".

любую программу, составленную программистом, работающим с зараженной библиотекой.

Внедряется вирус в библиотеку следующим способом. В объектную библиотеку добавляется модуль, содержащий в себе вирус, оформленный в виде подпрограммы. Затем в модуль, который должен получать управление от ДОС в сформированной программе, вставляется вызов подпрограммы, содержащей вирус. При этом корректируется таблица глобальных имен, используемых в библиотеке. При компоновке какой-либо программы модуль с вирусом автоматически подключается к программе и всегда будет запускаться при ее запуске.

Вирус этого типа после запуска ищет в компьютере объектные библиотеки компилятора, и если находит, то модифицирует их. Положение библиотек на „винчестере" (а только при наличии „винчестера" вирус будет эффективным) обычно можно определить по параметру LIB, записанному в поле описания обстановки (environment), устанавливаемому командой SET.

Обнаружить этот вирус практически невозможно. Единственный способ – периодический контроль содержимого библиотеки по контрольной сумме или размеру.

4. Вирус в сетевом драйвере. Возможно создание вируса, внедряемого в сетевой драйвер. Такой вирус переносит себя по сети на другой компьютер. Возможность перенесения по сети, конечно, зависит от вида сети – один вирус обычно может заражать только сеть одного вида с однотипными драйверами обслуживания сети.

Самый простой способ переноса такого вируса – передача по сети нового варианта сетевого драйвера. Для этого необходимо, чтобы зараженный драйвер вызвал от незараженного абонента сетевой драйвер (или его часть), добавил в него вирус и передал обратно. При последующем запуске сетевого драйвера будет запущен уже новый, зараженный драйвер.

Процесс заражения сопровождается довольно большими передачами по сети, поэтому вирус может быть обнаружен за счет не только изменения размера сетевого драйвера или его контрольной суммы, но и обнаружения лишних передач по сети.

Включение вируса. Способов включения каких-либо вредительских функций вируса несколько. Естественно, включение вируса должно происходить не сразу после его занесения в компьютер. У вируса должен быть „инкубационный период" для того, чтобы не сразу стало известно, откуда он появился. Мне кажется, что существуют три основных способа включения вируса.

Первый – по наступлению конкретной даты. Этот способ эффективен на Западе и не очень эффективен у нас. Советские компьютеры и дешевые западные (типа PC XT) не снабжаются часами, а опыт показывает, что лишь очень небольшая часть пользователей правильно устанавливает при запуске компьютера дату и время. За счет этого включения вируса по наступлению конкретной даты не очень эффективно у нас. Второй способ включения вируса – по счетчику обращений к зараженной программе (дискете). Этот способ может быть использован для маскировки момента заражения. Кроме того, вирус может быть включен постоянно с момента его внедрения в зараженную программу, но изменения, вносимые им в работу системы, должны быть небольшие, нарастающие со временем, так чтобы он не был обнаружен сразу. Возможно сочетание всех трех способов.

О вреде вируса. Что может вирус сделать плохого? После пробуждения вирус может либо сразу уничтожить все доступные ему данные, либо постепенно их изменять. Первый вариант неэффективен на ПК без „винчестера", а значит, не очень эффективен у нас, так как советские ПК в настоящее время в основном выпускаются без „винчестеров". Второй вариант наиболее тяжел для последующего восстановления системы.

Самое уязвимое место ДОС – файловая система. Испортить ее возможно, например, произвольно меняя данные в буферах ДОС. Доступ к этим буферам можно получить, запросив у ДОС их адрес в памяти. В принципе существует очень много способов порчи файловой системы, и какой конкретно способ будет использован, зависит от вероломства разработчика вируса.

Обнаружение вируса. Обнаружение вируса должно вестись в соответствии со способом его внедрения в компьютер. Если вирус переносит себя на конец свободного поля памяти ПК (а это самый простой способ внедрения вируса при любом способе его хранения на носителе), то следует производить проверку на размер памяти, необходимо проверить, не переустановлены ли некоторые векторы прерывания на эту область памяти. Нужно учитывать, что в последних вариантах ПК фирмы IBM, в том числе в ПК семейства PS/2, конец поля памяти используется базовой системой ввода-вывода для хранения своих данных.

Если вирус прикрепляет себя к ДОС, то его обнаружение возможно на основе вычисления размеров различных частей ДОС с учетом версии ДОС, всех драйверов ввода-вывода, добавленных во время загрузки системы, числа буферов ввода-вывода и т. д.

Вирус, находящийся в отдельном блоке памяти, выделенном ДОС, должен отлавливаться сразу после загрузки ДОС, когда в памяти ком-

ВИРУСЫ В МОСКВЕ

От советских пользователей ПК Commodor Amiga и Atari ST стало известно о том, что были зарегистрированы вирусы для этих машин. Владельцы ПК Amiga вычищали вирусы вручную, стирая их со стартовой дорожки дискет. Владельцы ST смогли воспользоваться вирус-детектором, который не только убивает вирусы, но также иммунизирует диски. По крайней мере, с тремя типами вирусов – A, B, C – детектор справляется.

пьютера нет еще ни одной резидентной программы. Позднее отловить вирус сложно, так как его надо отличить от резидентной программы, загруженной пользователем. Для обнаружения такого вируса необходимо просмотреть все блоки памяти и определить, все ли блоки памяти используются реальными программами. Наличие резидентных программ может быть обнаружено как по использованию блоков памяти, так и по изменению размера свободного поля памяти после выполнения подозрительной программы.

Можно обнаружить присутствие вируса на дискете с ДОС. Для этого необходимо иметь дискету, на которой записана только ДОС и больше ничего. Подсчитав „вручную" контрольную сумму всех данных на незараженной дискете, можно затем установить наличие вируса. Для этого надо обратиться к такой дискете, например, запуском командного процессора, после чего подсчитать контрольную сумму. В принципе, этого может оказаться недостаточно в случае, если вирус переносится на дискету только при записи на нее. В этом случае на дискете должен быть еще один короткий тестовый файл. Он переписывается на дискету, устанавливаются правильная дата и время его создания, и после этого проверяется контрольная сумма. Можно также сравнить дискету в ДОС, на которую производилась запись, с контрольной дискетой, защищенной по записи, на которой заведомо нет вируса.

Напутствия. Напоследок мне хотелось бы еще раз добавить: бойтесь вирусов — это может быть серьезно. Надо думать об этом заранее, поздно будет искать средства защиты после исчезновения информации с вашего „винчестера"! В СССР уже появились вирусы на ПК типа Commodore Amiga и Atari 1040ST (на момент написания статьи). Компьютеров этого типа немного, и вреда вирусы не нанесли.

Компьютерные вирусы сравнивают со СПИДом. Подобно этой опасной болезни нашего времени они будут наказывать в первую очередь тех, кто ведет беспорядочный образ жизни — бесконтрольное переписывание программ. Вспоминайте почаще о том, что существует авторское право (не имеющее, правда, у нас юридической силы, но должна же быть и совесть!), и ваш компьютер будет здоров, вы без опасения сможете с ним общаться.

ВИРУС-ДЕТЕКТОР, ЗАЩИЩАЮЩИЙ СЕТИ

Институт безопасности компьютеров (США) на конференции (июнь 1988 г.) для пользователей IBM и DEC продемонстрировал образцы компьютерных вирусов и вирус-детекторов (программы, выявляющие и убивающие вирус). Программа, представленная этим институтом, обеспечивает безопасность сетей Ethernet и MacVAX.