## §12. КОМПЬЮТЕРНЫЕ ВИРУСЫ

### 12.1. ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС

Среди огромного разнообразия видов компьютерных программ существует одна их разновидность, заслуживающая особого упоминания. Главное отличие этих программ от всех остальных состоит в том, что они вредны, т.е. предназначены для нанесения ущерба пользователям ЭВМ. Это - компьютерные вирусы.

Компьютерным вирусом называется программа, обычно малая по размеру (от 200 до 5000 байт), которая самостоятельно запускается, многократно копирует свой код, присоединяя его к кодам других программ («размножается») и мешает корректной работе компьютера и/или разрушает хранимую на магнитных дисках информацию (программы и данные).

Существуют вирусы и менее «злокачественные», вызывающие, например, переустановку даты в компьютере, музыкальные (проигрывающие какую-либо мелодию), приводящие к появлению на экране дисплея какого-либо изображения или к искажениям в отображении дисплеем информации, «осыпанию букв» и т.д.

Создание компьютерных вирусов можно квалифицировать с юридической точки зрения как преступление.

Интересны причины, заставляющие квалифицированных программистов создавать компьютерные вирусы, ведь эта работа не оплачивается и не может принести известности. По-видимому, для создателей вирусов это способ самоутверждения, способ доказать свою квалификацию и способности. Созданием компьютерных вирусов занимаются квалифицированные программисты, по тем или иным причинам не нашедшие себе места в полезной деятельности, в разработке прикладных программ, страдающие болезненным самомнением или комплексом неполноценности. Становятся создателями вирусов и те молодые программисты, которые испытывают. трудности в общении с окружающими людьми, не встречают признания со стороны специалистов, которым чужды понятие морали и этики компьютерной сферы деятельности.

Существуют и такие специалисты, которые отдают свои силы и талант делу борьбы с компьютерными вирусами. В России - это известные программисты Д.Лозинский, Д.Мостовой, П.А.Данилов, Н.Безруков и др. Ими исследованы многие компьютерные вирусы, разработаны антивирусные программы, рекомендации по мерам, предотвращающим уничтожение вирусами компьютерной информации и распространение эпидемий компьютерных вирусов.

Главную опасность, по их мнению, представляют не сами по себе компьютерные вирусы, а пользователи компьютеров и компьютерных программ, не подготовленные к встрече с вирусами, ведущие себя неквалифицированно при встрече с симптомами заражения компьютера, легко впадающие в панику, что парализует нормальную работу.

### 12.2. РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ

Рассмотрим подробнее основные особенности компьютерных вирусов, характеристики антивирусных программ и меры зашиты программ и данных от компьютерных вирусов в наиболее распространенной операционной системе MS DOS.

По приближенным оценкам к 1997 г. существовало около 7000 различных вирусов. Подсчет их осложняется тем, что многие вирусы мало отличаются друг от друга, являются вариантами одного и того же вируса и, наоборот, один и тот же вирус может менять свой облик, кодировать сам себя. На самом деле основных принципиальных идей, лежащих в основе вирусов, не очень много (несколько десятков).

Среди всего разнообразия вирусов следует выделить следующие группы:

**•загрузочные** (boot) **вирусы** заражают программу начальной загрузки компьютера, хранящуюся в загрузочном секторе дискеты или винчестера, и запускающиеся при загрузке компьютера;

• **файловые вирусы** в простейшем случае заражают пополняемые файлы, но могут распространяться и через файлы документов (системы Word for Windows) и даже вообще не модифицировать файлы, а лишь иметь к ним какое-то отношение;

**• загрузочно-файловые вирусы** имеют признаки как загрузочных, так и файловых вирусов;

• **драйверные вирусы** заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.

Из вирусов, функционирующих не на персональных компьютерах под операционной системой MS DOS, следует упомянуть **сетевые вирусы,** распространяющиеся в сетях, объединяющих многие десятки и сотни тысяч компьютеров.

Рассмотрим принципы функционирования загрузочных вирусов. На каждой дискете или винчестере имеются служебные сектора, используемые операционной системой для собственных нужд, в том числе сектор начальной загрузки. В нем помимо информации о дискете (число дорожек, число секторов и пр.) хранится небольшая программа начальной загрузки, о которой уже рассказывалось в настоящей главе.

Простейшие загрузочные вирусы, резидентно находясь в памяти зараженного компьютера, обнаруживают в дисководе незараженную дискету и производят следующие действия:

• выделяют некоторую область дискеты и делают ее недоступной операционной системе (помечая, например, как сбойную - bad);

• замещают программу начальной загрузки в загрузочном секторе дискеты, копируя корректную программу загрузки, а также свой код, в выделенную область дискеты;

• организуют передачу управления так, чтобы вначале выполнялся бы код вируса и лишь затем - программа начальной загрузки.

Магнитные диски компьютеров винчестерского типа обычно бывают разбиты на несколько логических разделов. Программы начальной загрузки при этом имеются в MBR (Master Boot Record - главная загрузочная запись) и в загрузочном разделе винчестера, заражение которых может происходить аналогично заражению загрузочного сектора дискеты. Однако, программа начальной загрузки в MBR использует при переходе к программе загрузки загрузочного раздела винчестера, так называемую таблицу разбиения (Partition table), содержащую информацию о положении загрузочного раздела на диске. Вирус может исказить информацию Partition table и таким образом передать управление своему коду, записанному на диск, формально не меняя загрузочной программы.

Теперь рассмотрим принципы функционирования **файловых вирусов.** Файловый вирус не обязательно является резидентным, он может, например, внедриться в код исполняемого файла. При запуске зараженного файла вирус получает управление, выполняет некоторые действия и возвращает управление коду, в который он был внедрен. Действия, которые выполняет вирус, включают поиск подходящего для заражения файла, внедрение в него так, чтобы получить управление при запуске файла, произведение некоторого эффекта, например, звукового или графического. Если файловый вирус резидентный, то он устанавливается в памяти и получает возможность заражать файлы и проявляться независимо от первоначального зараженного файла.

Заражая файл, вирус всегда изменит его код, но далеко не всегда производит другие изменения. В частности, может не изменяться начало файла и его длина (что раньше считалось признаком заражения). Например, вирусы могут искажать информацию о файлах, хранящуюся в служебной области магнитных дисков -таблице размещения файлов (FAT - file allocation table), - и делать таким образом невозможной любую работу с файлами. Так ведут себя вирусы семейства «Dir».

**Загрузочно-файловые вирусы** используют принципы как загрузочных, так и файловых вирусов, и являются наиболее опасными.

### 12.3. АНТИВИРУСНЫЕ СРЕДСТВА

К настоящему времени накоплен значительный опыт борьбы с компьютерными вирусами, разработаны антивирусные программы, известны меры защиты программ и данных. Происходит постоянное совершенствование, развитие антивирусных средств, которые в короткий срок с момента обнаружения вируса -от недели до месяца - оказываются способными справиться с вновь появляющимися вирусами.

Создание антивирусных программ начинается с обнаружения вируса по аномалиям в работе компьютера. После этого вирус тщательно изучается, выделяется его сигнатура - последовательность байтов, которая полностью характеризует программу вируса (наиболее важные и характерные участки кода), выясняется механизм работы вируса, способы заражения. Полученная информация позволяет разработать способы обнаружения вируса в памяти компьютера и на магнитных -дисках, а также алгоритмы обезвреживания вируса (если возможно, удаления вирусного кода из файлов - «лечения»).

Известные ныне антивирусные программы можно разделить на несколько типов, перечисленных ниже.

• **Детекторы**. Пх назначение - лишь обнаружить вирус. Детекторы вирусов могут сравнивать загрузочные сектора дискет с известными загрузочными секторами, формируемыми операционными системами различных версий, и таким образом обнаруживать загрузочные вирусы или выполнять сканирование файлов на магнитных дисках с целью обнаружения сигнатур известных вирусов. Такие программы в чистом виде в настоящее время редки.

**• Фаги.** Фаг - это программа, которая способна не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных программ и восстановить их работоспособность (если возможно). Известнейшим в России фагом является Aidstest, созданный Д.Лозинским. К январю 1997 года эта программа была способна обнаружить и обезвредить около 1600 вирусов. Еженедельно появляются новые версии этой программы, рассчитанные на обезвреживание десятков новых вирусов.

Очень мощным и эффективным антивирусным средством является фаг Doctor Web (созданный И.Даниловым). Детектор этого фага не просто сканирует файлы в поисках одной из известных вирусных сигнатур. Doctor Web реализует эвристический метод поиска вирусов, может находить и обезвреживать, так называемые, полиморфные вирусы (не имеющие определенной сигнатуры), проверять файлы, находящиеся в архивах. Для нахождения вирусов Doctor Web использует программную эмуляцию процессора, т.е. он моделирует выполнение остальных файлов с помощью программной "модели микропроцессора 1-8086 и тем самым создает среду для проявления вирусов и их размножения. Таким образом, программа Doctor Web может бороться не только с полиморфными вирусами, но и с вирусами, которые только еще могут появиться в перспективе. Специалисты рекомендуют использовать Aidstest и Doctor Web в комплексе.

• **Ревизоры**. Программа-ревизор контролирует возможные пути распространения программ-вирусов и заражения компьютеров. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов и должны входить в арсенал каждого пользователя. Ревизоры являются единственным средством, позволяющим следить за целостностью и изменениями файлов и системных областей магнитных дисков. Наиболее известна в России программа-ревизор ADinf, разработанная Д.Мостовым.

• **Сторожа**. Сторож - это резидентная программа, постоянно находящаяся в памяти компьютера, контролирующая операции компьютера, связанные с изменением информации на магнитных дисках, и предупреждающая пользователя о них. В состав операционной системы MS DOS, начиная с версии 6.0, входит сторож VSAFE. Однако, из-за того, что обычные программы выполняют операции, похожие на те, что делают вирусы, пользователи обычно не используют сторожа, так как постоянные предупреждения мешают работе.

**• Вакцины.** Так называются антивирусные программы, ведущие себя подобно вирусам, но не наносящие вреда. Вакцины предохраняют файлы от изменении и способны не только обнаружить факт заражения, но и в некоторых случаях «вылечить» пораженные вирусами файлы. В настоящее время антивирусные программы-вакцины широко не применяют, так как в прошлые годы некоторыми некорректно работающими вакцинами был нанесен ущерб многим пользователям.

Помимо программных средств защиты от вирусов существуют и специальные дополнительные устройства, обеспечивающие надежную защиту определенных разделов винчестера. Примером такого рода устройств является плата Sheriff (разработанная Ю.Фоминым). Несмотря на кажущееся обилие программных антивирусных средств, даже все вместе они не обеспечивают полной защиты программ и данных, не дают 100%-ной гарантии от воздействия вирусных программ. Только комплексные профилактические меры защиты обеспечивают надежную защиту от возможной потери информации. В комплекс таких мер входит:

• регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера);

• избегание использования случайно полученных программ (старайтесь пользоваться только законными путями получения программ);

• входной контроль нового программного обеспечения, поступивших дискет;

•сегментация жесткого диска, т.е. разбиение его на логические разделы с разграничением доступа к ним;

• систематическое использование программ-ревизоров для контроля целостности информации;

• при поиске вирусов (который должен происходить регулярно!) старайтесь использовать заведомо чистую операционную систему, загруженную с дискеты. Защищайте дискеты от записи, если есть хоть малая вероятность заражения.

При неаккуратной работе с антивирусными программами можно не только переносить с ними вирусы, но и вместо лечения файлов безнадежно их испортить. Полезно иметь хотя бы общее представление о том, что могут и чего не могут компьютерные вирусы, об их жизненном цикле, о важнейших методах защиты.