8.7. Виды компьютерных вирусов, их классификация

Первые сообщения о возможности создания компьютерных вирусов относятся к 1984 г., когда сотрудник Лехайского университета Фред Коэн сделал сообщение на эту тему на седьмой национальной конференции США по компьютерной безопасности. Он же является автором первой серьезной работы, посвященной математическим исследованиям жизненного цикла и механизмов размножения компьютерных вирусов. В то же время это выступление не нашло отклика у специалистов по безопасности, которые не придали сообщению большого значения. Однако уже в 1985 г. стали появляться сообщения о реальных фактах проявления компьютерных вирусов.

Промышленная ассоциация по компьютерным вирусам только за 1988 г. зафиксировала почти 90 тысяч вирусных атак на персональные компьютеры США. Количество инцидентов, связанных с вирусами, вероятно, превосходит опубликованные цифры, поскольку большинство фирм умалчивает о вирусных атаках. Причины молчания: такая информация может повредить репутации фирмы и привлечь внимание хакеров.

С 1987 г. были зафиксированы факты появления компьютерных вирусов и в нашей стране. Масштабы реальных проявлений "вирусных эпидемий" в настоящее время оцениваются сотнями тысяч случаев "заражения" ПК. Хотя некоторые из вирусных программ оказываются вполне безвредными, многие из них имеют разрушительный характер. Особенно опасны вирусы для персональных компьютеров, входящих в состав локальных вычислительных сетей.

Способ функционирования большинства вирусов - это такое изменение системных файлов ПК, чтобы вирус начинал свою деятельность при каждой загрузке персонального компьютера. Некоторые вирусы инфицируют файлы загрузки системы, другие специализируются на различных программных файлах. Всякий раз, когда пользователь копирует файлы на машинный носитель информации или посылает инфицированные файлы по сети, переданная копия вируса пытается установить себя на новый диск.

Некоторые вирусы разрабатываются так, чтобы они появлялись, когда происходит некоторое событие вызова: например, пятница 13-е, 26 апреля, другая дата, определенное число перезагрузок зараженного или какого-то конкретного приложения, процент заполнения винчестера и т. д.

После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто не замечает, что его ПК заражен и не успевает принять соответствующих адекватных мер.

Для анализа действия компьютерных вирусов введено понятие жизненного цикла вируса, который включает четыре основных этапа,

Для реализации каждого из этапов цикла жизни вируса в его структуру включают несколько взаимосвязанных элементов:

- часть вируса, ответственная за внедрение и инкубационный период;
- часть вируса, осуществляющая его копирования и добавление к другим файлам (программам);
- часть вируса, в которой реализуется проверка условия активизации его деятельности;
- часть вируса, содержащая алгоритм деструктивных действий;
- часть вируса, реализующая алгоритм саморазрушения.

Следует отметить, что часто названные части вируса хранятся отдельно друг от друга, что затрудняет борьбу с ними.

Объекты воздействия компьютерных вирусов можно условно разделить на две группы:

1. С целью продления своего существования вирусы поражают другие программы, причем не все, а те, которые наиболее часто используются и / или имеют высокий приоритет в информационной технологии (следует отметить, что сами программы, в которых находятся вирусы, с точки зрения реализуемых ими функций, как правило, не портятся).
2. Деструктивными целями вирусы воздействуют чаще всего на данные, реже - на программы.

К способам проявления компьютерных вирусов можно отнести:

- замедление работы персонального компьютера, в том числе его зависание и прекращение работы;
- изменение данных в соответствующих файлах;
- невозможность загрузки операционной системы;
- прекращение работы или неправильная работа ранее успешно функционирующей программы пользователя;
- увеличение количества файлов на диске;
- изменение размеров файлов;
- нарушение работоспособности операционной системы, что требует ее периодической перезагрузки;
- периодическое появление на экране монитора неуместных сообщений;
- появление звуковых эффектов;
- уменьшение объема свободной оперативной памяти;
- заметное возрастание времени доступа к винчестеру;
- изменение даты и времени создания файлов;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов);
- загорание сигнальной лампочки дисковода, когда к нему нет обращения пользователя;
- форматирование диска без команды пользователя и т. д.

Следует отметить, что способы проявления необязательно вызываются компьютерными вирусами. Они могут быть следствием некоторых других причин, поэтому вычислительные средства ИТ следует периодически комплексно диагностировать.

В настоящее время существует огромное количество вирусов, которые можно классифицировать по признакам,

1. **По виду среды обитания** вирусы классифицируются на следующие виды:

- **загрузочные** внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- **файловые** внедряются в основном в исполняемые файлы с расширениями .COM и .EXE;
- **системные** проникают в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов;
- **сетевые вирусы** обитают в компьютерных сетях;
- **файлово-загрузочные** (многофункциональные) поражают загрузочные секторы дисков и файлы прикладных программ.

2. **По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяются:**
   - **безвредные вирусы**, не оказывающие разрушительного влияния на работу персонального компьютера, но могут переполнять оперативную память в результате своего размножения;
   - **неопасные вирусы** не разрушают файлы, но уменьшают свободную дисковую память, выводят на экран графические эффекты, создают звуковые эффекты и т. д. ;
   - **опасные вирусы** нередко приводят к различным серьезным нарушениям в работе персонального компьютера и всей информационной технологии;
   - **разрушительные** приводят к стиранию информации, полному или частичному нарушению работы прикладных программ и пр.
3. **По способу заражения среды обитания** вирусы подразделяются на следующие группы:
   - **резидентные вирусы** при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия вплоть до выключения или перезагрузки компьютера.
   - **нерезидентные вирусы** не заражают оперативную память персонального компьютера и являются активными ограниченное время.
4. **Алгоритмическая особенность построения вирусов** оказывает влияние на их проявление и функционирование. Выделяют следующие виды таких вирусов:
   - **репликаторные**, благодаря своему быстрому воспроизводству приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала;
   - **мутирующие** со временем видоизменяются и самопроизводятся. При этом, самовоспризводясь, воссоздают копии, которые явно отличаются от оригинала;
   - **стэлс-вирусы (невидимые)** перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие "обманывать" резидентные антивирусные мониторы;
   - **макровирусы** используют возможности макроязыков, встроенных в офисные программы обработки данных (текстовые редакторы, электронные таблицы и т. д.).