**Глава 3**

КОМПЬЮТЕРНЫЙ ВИРУС

***Компьютерный вирус*** - это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять нежелательные различные действия на компьютере. Программа, внутри которой находится вирус, называется «заражённой». Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы, «засоряет» оперативную память и т.д.).

Для маскировки вируса, действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определённых условий. После того, как вирус выполнит нужные ему действия, он передаёт управление той программе, в которой он находится, и она работает так же, как обычная. Тем самым внешне работа заражённой программы выглядит так же, как и не заражённой.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы, табличные процессоры и другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

ИСТОРИЯ ВИРУСОВ И ВСПЛЕСКИ КОМПЬЮТЕРНЫХ ВИРУСОВ

О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиальные идеи. Все остальные - «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, *догонять вирусную технологию*. Например, в 1989 году американский студент сумел создать вирус, который вывел из строя около 6000 компьютеров Министерства обороны США. Или примером может быть эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счёт несовершенства традиционных антивирусных средств. Кристоферу Пайну удалось создать вирусы Pathogen и Queeq, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса, и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры, заражённые программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними борется. Запустив её, пользователи вместо уничтожения вирусов уничтожили файлы множества фирм, убытки составили миллионы фунтов стерлингов.

ПРИЧИНЫ ПОЯВЛЕНИЯ ВИРУСОВ

Причины появления и распространения компьютерных вирусов, с одной стороны, скрываются в психологии человеческой личности и её теневых сторонах (зависти, мести), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

КЛАССИФИКАЦИЯ ВИРУСОВ

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания;
* способу заражения среды обитания;
* воздействию;
* особенностям алгоритма.

В зависимости от среды обитаниявирусы можно разделить на **сетевые, файлово-загрузочные, полиморфные, макровирусы и загрузочные.**

**Сетевые вирусы** распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, то есть в файлы, имеющие расширение COM и EXE.

**Файлово-загрузочные** вирусы могут внедряться в другие виды файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

**Полиморфные вирусы** - это вирусы, модифицирующие свой код в заражённых программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

**Макро - вирусы** являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

**Загрузочные вирусы** внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска.

По способу заражения вирусы делятся на **резидентные и нерезидентные**.

**Резидентный вирус** при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

**Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вируса можно разделить на следующие виды:

* Неопасные, не мешающие работе компьютера, но уменьшающие объём свободной памяти и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
* Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;
* Очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

**Простейшие вирусы** - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

**Вирусы - репликаторы**, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

**Вирусы-невидимки**, называемые стелс - вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращение операционной системы к поражённым файлом и секторам дисков и подставляют вместо своего тела незаражённые участки диска.

Наиболее трудно обнаружить **вирусы - мутанты**, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые **«троянские» программы**, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую структуру диска.

КАК ОПРЕДЕЛИТЬ ВИРУС НА КОМПЬЮТЕРЕ

Есть несколько признаков того, что на вашем компьютере завелся вирус:

1. Вас должно насторожить, если ваш *компьютер стал тормозить*. Если задачи выполняются дольше, чем обычно, то возможно, ваш компьютер заражен.
2. Будьте внимательны при появлении на компьютере *подозрительных приложений или программ*, о которых вы ничего не знаете. Если вы заметили, чтобы на компьютере появилось приложение или программа, которую вы не скачивали, будьте осторожны.
3. Еще один признак возможного заражения компьютера вирусом – это *странности в работе приложений или программ*. Если программы стали завершаться аварийно по непонятной причине, то, возможно, на вашем компьютере завелся вирус.
4. Зараженный компьютер может начать *перегреваться*. Если вы заметите такое, проверьте компьютер на вирусы, запустив антивирус.