Вирусы и антивирусы

Компьютерные вирусы являются программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызвать уничтожение программ и данных.

Классификация вирусов

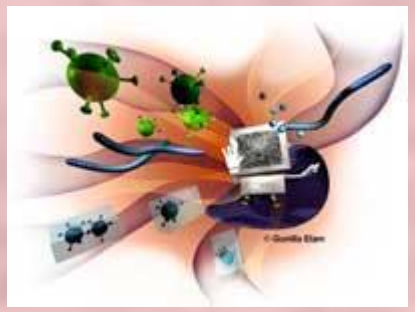
- по среде обитания;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Классификация вирусов по среде обитания

- **Файловые вирусы**, которые внедряются в выполняемые файлы (*.COM, *.EXE, *.SYS, *.BAT, *.DLL).
- **Загрузочные вирусы**, которые внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).
- **Макро-вирусы**, которые внедряются в системы, использующие при работе так называемые макросы (например, Word, Excel).
- Существуют и сочетания - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему и их труднее обнаружить.

Классификация вирусов по способам заражения

- ***Резидентный*** *вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем 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 лишь ограниченное время.*



По деструктивным возможностям

- ***безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);*
- ***неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;*
- ***опасные** - вирусы, которые могут привести к серьезным сбоям в работе;*
- ***очень опасные**, могущие привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти и т.д.*

Классификация вирусов по особенностям алгоритма

- ***компаньон-вирусы*** *(companion) - Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением COM. При запуске такого файла OS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл;*
- ***вирусы-«черви»*** *(worm) - вариант компаньон-вирусов. «Черви» не связывают свои копии с какими-то файлами. Они создают свои копии на дисках и в подкаталогах дисков, никаким образом не изменяя других файлов и не используя COM-EXE прием, описанный выше;*
- ***«паразитические»*** *- все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов.*
- ***«стелс»-вирусы*** *(вирусы-невидимки, stealth), представляют собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме того, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы;*
- ***макро-вирусы*** *- вирусы этого семейства используют возможности макроязыков (таких как Word Basic), встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).*

Прочие вредные программы

- *К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий или при каждом запуске уничтожающая информацию на дисках, "завешивающая" систему и т.п. Большинство известных троянских коней являются программами, которые "подделываются" под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.*
- **"злые шутки" (hoax). К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К "злым шуткам" отностяся, например, программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит)**

Сравнительный обзор современных антивирусных средств защиты

- ***сканеры*** *– основной элемент любого антивируса, осуществляет, если можно так выразиться, пассивную защиту. По запросу пользователя или заданному распорядку производит проверку файлов в выбранной области системы. Вредоносные объекты выявляет путем поиска и сравнения программного кода вируса. Примеры программных кодов содержатся в заранее установленных сигнатурах (наборах, характерных последовательностей байтов для известных вирусов). В первую очередь к недостаткам данных программ относится беззащитность перед вирусами, не имеющими постоянного программного кода и способными видоизменяться при сохранении основных функций. Также сканеры не могут противостоять разновидностям одного и того же вируса, что требует от пользователя постоянного обновления антивирусных баз. Однако наиболее уязвимое место этого инструмента – неспособность обнаруживать новые и неизвестные вирусы, что особенно актуально, когда посредством e-mail новоявленная угроза способна заразить тысячи компьютеров по всему миру за считаные часы;*

Сравнительный обзор современных антивирусных средств защиты

- ***мониторы*** *– в совокупности со сканерами образуют базовую защиту компьютера. На основе имеющихся сигнатур проводят проверку текущих процессов в режиме реального времени. Осуществляют предварительную проверку при попытке просмотра или запуска файла. Различают файловые мониторы, мониторы для почтовых клиентов (MS Outlook, Lotus Notes, Pegasus, The Bat и другие, использующие протоколы POP3, IMAP, NNTP и SMTP) и специальные мониторы для отдельных приложений. Как правило, последние представлены модулями проверки файлов Microsoft Office. Основное их достоинство – способность обнаруживать вирусы на самой ранней стадии активности;*

Сравнительный обзор современных антивирусных средств защиты

- ***ревизоры*** *– сохраняют в отдельную базу данные о состоянии на определенный момент критических для работы областей системы. Впоследствии сравнивает текущие файлы с зарегистрированными ранее, позволяя таким образом выявлять любые подозрительные изменения. Преимущество ревизоров заключается в низких аппаратных требованиях и высокой скорости работы. Дело в том, что ревизору вообще не требуется антивирусная база, восприятие и различие производятся только на уровне неизменности изначальных файлов. Это позволяет эффективно восстанавливать систему, поврежденную деятельностью вредоносных модулей. Недостаток ревизоров состоит в невозможности оперативно реагировать на появление вируса в системе. Кроме того, при проверке исключаются новые файлы, чем пользуются многие вирусы, заражающие только заново создаваемые файлы;*