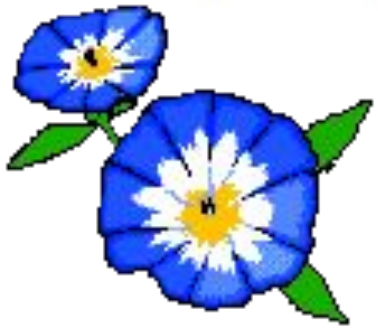
КОМПЬЮТЕРНЫЕ ВИРУСЫ

Во-первых, по среде обитания вирусы классифицируются следующим образом:

- сетевые вирусы, которые распространяются по сети;
- файловые вирусы, которые заражают файлы с расширением `.com`, `.exe`, `.bat`;
- загрузочные вирусы, которые заражают загрузочный сектор диска или сектор, содержащий программу загрузки системного диска;
- файлово-загрузочные, которые заражают загрузочные файлы.



Во-вторых, по способу заражения вирусы делятся на:

- резидентные. Эти вирусы после запуска остаются в оперативной памяти и начинают свою деятельность. Они перехватывают системные вызовы, чтобы заражать файлы в момент копирования или запуска. Даже если резидентный вирус был полностью удалён с жёсткого диска, оставшись в оперативной памяти, он тут же начнёт снова заражать файлы. Поэтому при лечении от такого вируса необходимо первым делом удалить его из оперативной памяти;
- нерезидентные (не заражают оперативную память и активны лишь некоторое время).

В-третьих, по результату воздействия вирусы классифицируют как:

- неопасные. Действуют как мелкие пакостники — засоряют память компьютера, размножаясь и совершая разные действия, такие как показ картинок или проигрыш разных мелодий;
- опасные. Эти вирусы нарушают работу компьютера, замедляют её, приводят к странным перезагрузкам, сбоям;
- крайне опасные. Могут уничтожить программы, стереть данные, разрушить загрузочные и системные области жесткого диска.

И четвёртая классификация — по алгоритму работы вирусов.

- паразитические. Такие вирусы изменяют содержимое файлов и секторов диска;
- мутанты. Эти вирусы крайне трудно обнаружить из-за применения в них алгоритмов шифрования, поскольку каждая следующая копия вируса не похожа на предыдущую;
- репликаторы (сетевые черви). Заражают твой компьютер, проникая через компьютерные сети;
- троянский конь. Этот вирус не размножается, как некоторые, а ворует ценную информацию — пароли, электронные деньги, номера банковских счетов;
- невидимки (stealth-вирусы). Эти вирусы, постоянно находясь в памяти компьютера, перехватывают обращения к заражённому файлу и быстро удаляют из него вирусный код, маскируя таким образом своё присутствие. Это трудно обнаруживаемые вирусы.

2. Классификация компьютерных антивирусов

«Евгений Касперский в 1992 году использовал следующую классификацию антивирусов в зависимости от принципа их действия:

- сканеры (устаревший вариант — «полифаги») — определяют наличие вируса по базе сигнатур, хранящей сигнатуры (программный код вируса) или контрольные суммы вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического анализатора;
- ревизоры — запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений;
- сторожа (мониторы) — отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции;
- вакцины — изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым. В современных (2007 г.) условиях, когда количество возможных вирусов измеряется сотнями тысяч, этот подход неприменим».