Классификация компьютерных вирусов

Большая популярность персональных компьютеров вместе со стремительным развитием сети Интернет способствовала появлению большого количества различных вредоносных программ – **вирусов**. **Вирусы** порой делают работу на компьютере невыносимой (глюки, сбои, утечка информации, "торможение" системы), а порой и вообще грозят "падению" операционной системы и уничтожению полезной информации. Попытаемся разобраться, что же такое вирус, как с ним бороться и какие **виды вирусов** нам угрожают...

Что такое вирус

Компьютерный вирус – это специально написанная программа небольшого размера, способная "внедряться" в тело какой-либо другой программы, перехватывать управление, чаще всего саморазмножаться с задачей прекращения работы компьютера или уничтожения информации. Устрашающе, правда?

Как вирус проникает в компьютер

Вирусы попадают на жесткий диск компьютера или его оперативную память: переносные хранилища данных – гибкие дискеты, CD и DVD диски, флэшки, но самое большое количество компьютерных вирусов попадает на наши с вами компьютеры через сеть Интернет.

Написанием этих самых вирусов занимаются как одиночки, так и группы хакеров. Результат всегда один и тот же - падение операционной системы, потеря или кража полезной информации (паролей, ключей) несмотря на совершенно разные на первый взгляд мотивы написания вирусов. Несмотря на то, что создание и тем более распространение данных программ является незаконным для большинства стран, вирусописание процветает. Во всяком случае, в ближайшее будущее...

Чаще всего **вирусы** поражают исполняемые файлы с расширением exe, com, sys, bat и загрузочные секторы компьютерных дисков.

Классификация вирусов

В большой количество разнообразных вирусов, обитающих в настоящее время в сети Интернет несложно запутаться. Но все, же **компьютерные вирусы** принято классифицировать. Разложим по полочкам...

По среде обитания

1. сетевые вирусы (они распространяются по разным компьютерным сетям);
2. файловые вирусы (заражают исполняемые файлы программ – com, exe, bat.);
3. загрузочные вирусы (заражают загрузочный сектор диска (boot-sector) или сектор, содержащий программу загрузки системного диска – Master Boot Record);
4. файлово-загрузочные (действуют, так же как и загрузочные вирусы)

По способу заражения

1. резидентные (такой вирус при инфицировании ПК оставляет в оперативке свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК);
2. нерезидентные (не заражают оперативную память и могут быть активными ограниченное время)

По результату воздействия

1. неопасные (как правило, эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);
2. опасные (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);
3. очень опасные (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

По алгоритму работы

1. паразитические (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);
2. мутанты (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);
3. репликаторы (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);
4. троянский конь (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т.д.);
5. невидимки (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.