Компьютерные вирусы. Антивирусные программы.

Компьютерный вирус — это специально написанная небольшая программа, которая может приписывать себя к другим программам (то есть заражать их), а также выполнять различные вредные действия на компьютере.

В результате заражения происходят следующие феномены, которые являются признаками заражения компьютера (они обусловлены деструктивными свойствами вирусов):

некоторые программы перестают работать или работают с ошибками;
размер некоторых исполнимых файлов и время их создания изменяются. В первую очередь это происходит с командным процессором, его размер увеличивается на величину размера вируса;
на экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты;
работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
компьютер перестает загружаться с жесткого диска.
Зараженными также оказываются дискеты с завирусованного компьютера, и компьютеры, связанные с ним по сети.

Вирусы поражают прежде всего exe и com файлы программ и не поражают текстовые файлы DOS (txt файлы).

Кроме вирусов, деструктивными свойствами обладают троянские программы. Если вирус проникает в компьютер незаметно, то троянскую программу пользователь сам записывает на диск, полагая, что это полезная программа. Но при определенных условиях она может начать свою разрушительную работу.

Пути заражения компьютера вирусами:

Через зараженные дискеты;
Через компьютерную сеть.
Других путей нет. Самозародиться вирусы не могут — это программа, специально написанная человеком для разрушения программного обеспечения компьютера и его системных областей. Типичный размер вируса составляет от десятков байт до десятков килобайт.

Компьютерные вирусы бывают следующих типов:

Файловые вирусы, поражающие exe и com файлы, иногда только com. Первым заражается командный процессор, а через него все остальные программы. Наиболее опасны резидентные вирусы, которые остаются в оперативной памяти постоянно. Заражение происходит при запуске зараженной программы (хотя бы однократном), то есть когда вирус получает управление и активизируется. Такие вирусы портят программы и данные, но иногда могут уничтожить содержимое всего жесткого диска.
Загрузочные или бутовые вирусы — поражают загрузочные сектора жестких дисков и дискет. Они наиболее опасны для компьютера, так как в результате их разрушительной работы компьютер перестает загружаться, иногда сразу после заражения, которое происходит даже при выводе оглавления зараженной дискеты.
Вирусы, поражающие драйверы, указанные в файле config.sys, и дисковые файлы DOS. Это

ведет к прекращению загрузки компьютера.
Вирусы DIR, меняющие файловую структуру.
Невидимые или стелс-вирусы. Их очень трудно обнаружить. Простейший способ маскировки - при заражении файла вирус делает вид, что длина файла не изменилась.
Самомодифицирующиеся вирусы. Они меняют свою структуру и код по случайному закону и их очень трудно обнаружить. Их называют также полиморфными. Две копии одного и того же вируса этого типа могут не содержать одинаковых последовательностей байт.
Сетевые вирусы — поражают машины, работающие в сети, в том числе в сети Интернет.
Вирусы Word (6.0 и старше), Excel, Access, PowerPoint, — поражают документы и макросы программ из MS Office.
Вирусы Windows — функционируют и портят данные в среде Windows.
Один из самых опасных из всех известных вирусов из Интернета — вирус "Чернобыль". Вирус активизируется 26 апреля, но модификации вируса могут принести вред и 26 числа каждого месяца. Кроме порчи информации на диске, он перепрограммирует BIOS (CMOS Setup) компьютера и компьютер перестает загружаться. Приходится обращаться в мастерскую и восстанавливать BIOS.

Вирус ILOVEYOU филиппинского происхождения, распространялся по E-mail. Он вывел из строя 45 млн. компьютеров во всем мире, в том числе в Пентагоне, ЦРУ, ФБР в США, Форин-офисе Великобритании и в других крупнейших странах. Вскоре вирус мутировал, так как были созданы его разновидности, и нанес дополнительный ущерб. Основная вирусная атака произошла 4 мая 2000 г. Вирус уничтожал графические jpg и звуковые mp3 файлы. Материальный ущерб составил около 10 миллиардов $ (USD). В России ущерб был сравнительно невелик — около 1000 компьютеров.

Методы борьбы с компьютерными вирусами:

Резервное копирование всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вирусной атаки. Создание системной и аварийной дискеты.
Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.
Включение антивирусного протектора от загрузочных вирусов в CMOS Setup машины.
Защита дискет от записи.
Использование только лицензионного программного обеспечения, а не пиратских копий, в которых могут находиться вирусы.
Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.
Применение антивирусных программ и обновление их версий.
Подготовка ремонтного набора дискет (антивирусы и программы по обслуживанию дисков).
Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.
Наиболее эффективны российские программы Dr. Web, ADinf, AVP, BootCHK и зарубежные Norton Antivirus, Dr. Solomon, причем наши программы лучше. Антивирусная база AVP для DOS и для Windows содержит информацию о более чем 28000 вирусов. Причем она ежедневно обновляется. Информация содержится на сайте в интернете http://www.avp.ru/. Есть также Dr.Web для DOS и для Windows на более 20000 вирусов.

Лечение дисков производится только при загрузке машины с системной дискеты, иначе не будут удалены резидентные вирусы.

Для запуска программы Dr.Web для DOS надо запустить файл drweb.exe и после проверки ОЗУ компьютера нажать F5 и указать путь тестирования. Для лечения диска надо нажать

Ctrl-F5 и указать путь тестирования. Если указана "*", то это означает тестирование всего жесткого диска. Для тестирования дискет надо указать путь a: или b:. Для тестирования CD-ROM надо указать путь d:. Для начала тестирования — Enter. После окончания тестирования выход из программы — Alt-X. Программа Drweb содержит эвристический анализатор вирусов и является наиболее эффективной. После окончания работы программы надо создавать файл отчета report.dwb и просматривать его.

Формат команды для запуска программы AidsTest для тестирования жесткого диска: aidstest * /g /f /s, для дискеты: aidstest a: /g /f /s или aidstest b: /g /f /s.

Однако программа AidsTest сильно устарела и имеет лишь историческое значение.

Для запуска антивирусной программы AVP для DOS надо запустить файл avp.exe в каталоге AVP_DOS, затем выбрать область тестирования (диски C: или A:) и указать мышью кнопку "Пуск". Программа AVP весьма эффективна и имеет очень высокую скорость работы.

Еще более эффективна программа AVP для Windows. После окончания тестирования выход из программы — Alt+X. После окончания работы программы надо создавать файл отчета report.txt и просматривать его.

В заключение темы приведем два простых правила, соблюдая которые Вы легко предотвратите потерю ценной информации на случай сбоя или заражения машины вирусом:

Создав любой новый файл (содержащий, например, текст, программу или рисунок), обязательно сразу скопируйте его на дискету.
Любую дискету, побывавшую на чужой машине, обязательно проверьте антивирусными программами с обновленными антивирусными базами.