Методы защиты от компьютерных вирусов

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.

дополнительное определение (понятие)

Дополнительное определение (понятие)

Компьютерный вирус - это программный код, встроенный в другую программу, документ или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на компьютере.

Компьютерные вирусы бывают следующих типов:

1. Файловые вирусы.
2. Загрузочные вирусы.
3. Вирусы, поражающие драйверы.
4. Невидимые или стелс-вирусы
5. Самомодифицирующиеся вирусы
6. Сетевые вирусы.

Зараженными также оказываются носители информации 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).

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.

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.

Кроме вирусов, такими же 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:

1. Через зараженные носители информации (диски, флеш – карты и т.п.);
2. Через компьютерную сеть.

Признаки заражения компьютера:

1. Некоторые программы перестают работать или работают с ошибками;
2. Размер некоторых исполнимых файлов и время их создания изменяются. В первую очередь это происходит с командным процессором, его размер увеличивается на величину размера вируса;
3. На экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты;
4. Работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
5. Некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
6. Компьютер перестает загружаться с жесткого диска.

Методы борьбы с компьютерными вирусами:

1. 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.
2. Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.
3. Включение антивирусного протектора от загрузочных вирусов в CMOS Setup машины. Защита дискет от записи.
4. Использование только лицензионного программного обеспечения, а не пиратских копий, в которых могут находиться вирусы.
5. Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.
6. Применение антивирусных программ и обновление их версий.
7. Подготовка ремонтного набора дисков (антивирусы и программы по обслуживанию дисков).
8. Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.

Существует много программных средств антивирусной защиты. Они предоставляют следующие возможности:

1. Создание образа жесткого диска на внешних носителях.
   В случае выхода из строя данных в системных областях жесткого диска сохраненный образ диска может позволить восстановить если не все данные, то, по крайней мере, их большую часть. Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.
2. Регулярное сканирование жестких дисков в поисках компьютерных вирусов. Обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве. Антивирусная программа ищет вирус путем сравнения кода программы с кодами известных вирусов, хранящихся в базе данных. Для надежной работы надо регулярно обновлять базу данных.
3. Контроль за изменением размеров и других атрибутов файла. Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.
4. Контроль за обращениями к жесткому диску. Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, обращены на модификацию данных, записанных на жестком диске, антивирусная программа может контролировать обращения к нему и предупреждать пользователя о подозрительной активности.

Два простых правила, соблюдая которые легко предотвратить потерю ценной информации на случай сбоя или заражения машины вирусом:

Правило 1. Создав любой новый файл (содержащий, например, текст, программу или рисунок), обязательно сразу скопируйте его на носитель.

Правило 2. Любой носитель, побывавший в чужом ПК, обязательно проверьте антивирусными программами с обновленными антивирусными базами.

Контрольные вопросы:

1. Что такое компьютерный вирус ?
2. Укажите пути проникновения компьютерного вируса в компьютер.
3. Укажите основные признаки заражения компьютера.
4. Какие существуют методы борьбы с компьютерными вирусами?
5. Какие основные антивирусные программы Вы знаете?

Благодарю за внимание

Презентацию подготовила
преподаватель ГБОУ СПО «Баймакский сельскохозяйственный техникум»
Мусина Ж.М.