**План-конспект урока по информатике: «Компьютерные вирусы»**

Цели урока:

* помочь учащимся получить представление о компьютерных вирусах, их основных видах, способах проникновения и распространения в компьютерах и компьютерных системах, дать основные знания о способах обнаружения вирусов и защиты от них, научить пользоваться антивирусными программами.
* воспитание информационной культуры учащихся, внимательности, аккуратности, дисциплинированности, усидчивости.
* развитие познавательных интересов, навыков работы с мышью и клавиатурой, самоконтроля, умения конспектировать.

Тип урока: лекция.

## Конспект урока по информатике

Орг. момент.  
Приветствие, проверка присутствующих. Объяснение хода урока.

Актуализация знаний.

Компьютерные вирусы не зря так названы - их сходство с «живыми» вирусами поражает. Они так же распространяются, живут, действуют, так же умирают. Разница лишь в том, что в качестве мишени выступают не люди и не животные, а компьютеры. Контактируя между собой посредством дискет, компакт дисков, локальных сетей, Интернет и других средств «общения», они, как и человек, заражают друг друга.

Теоретическая часть.

Компьютерным вирусом называется программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. На сегодняшний день известно 6 основных типов вирусов: файловые, загрузочные, призраки (полиморфные), невидимки, скрипт-вирусы и макро-вирусы. Следует отличать вирусы от вредоносных кодов. К ним относятся Интернет-черви и программы, получившие название «Троянские кони».

Основные симптомы вирусного поражения: замедление работы некоторых программ, увеличение размеров файлов (особенно выполняемых), появление не существовавших ранее подозрительных файлов, уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы), внезапно возникающие разнообразные видео и звуковые эффекты. При всех перечисленных выше симптомах, а также при других странных проявлениях в работе системы (неустойчивая работа, частые самостоятельные перезагрузки и прочее) следует немедленно произвести проверку системы на наличие вирусов.

Зарождение компьютерных вирусов

О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были. Интересно, что идея компьютерных вирусов появилась намного раньше самих персональных компьютеров. Точкой отсчета можно считать труды известного ученого Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, о которых стало известно в 1940-х годах. В 1951 году он предложил способ создания таких автоматов. А в 1959 году журнал Scientific American опубликовал статью Л.С. Пенроуза, посвященную самовоспроизводящимся механическим структурам. В ней была описана простейшая двумерная модель самовоспроизводящихся механических структур, способных к активации, размножению, мутациям, захвату. Позднее другой ученый Ф.Ж. Шталь реализовал данную модель на практике с помощью машинного кода на IBM 650.

Упрощенно процесс заражения вирусом программных файлов можно представить следующим образом. Код зараженной программы обычно вирус получил управление первым, до начала работы программы - вирусоносителя. При передаче управления вирусу он каким-то способом находит новую программу и выполняет вставку собственной копии в начало или добавляет ее в конец этой обычно еще не зараженной программы. Если вирус дописывается в конец программы, то он то он корректирует код программы, чтобы получить управление первым. Для этого первые несколько байтов запоминаются в теле вируса, а на их место вставляется команда перечода на начало вируса. Этот способ является наиболее распространенным. Получив управление, вирус восстанавливает “спрятанные” первые  
байты, а после обработки своего тела передает управление программе - вирусоносителю.

Основными результатами в процессе развития вредоносных кодов стали:

* абсолютное лидерство электронной почты в качестве главного источника вирусной опасности;
* технологическая диверсификация вирусов;
* доминирование скрипт и макро-вирусов над другими типами вредоносных программ;
* попытки создать вирусы для мобильных телефонов;
* широкое распространение вирусов, использующих “дыры” в системе безопасности Internet Explorer;
* появление нового поколения вирусов, имеющих способность самообновления модулей через Web сайты и электронные конференции
* появление вирусов, использующих дополнительные потоки файловой системы NTFS
* дальнейшее развитие вирусов для Linux

Антивирусные программы

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

С давних времен известно, что к любому яду  рано  или  поздно можно найти противоядие. Таким противоядием в  компьютерном  мире стали программы, называемые антивирусными. Данные программы  можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры - это резидентные программы, которые  оповещают пользователя о всех попытках  какой-либо  программы  записаться на диск, а уж тем более отформатировать его ,  а  также  о других подозрительных действиях (например о попытках изменить установки CMOS). При этом выводится запрос о разрешении или  запрещении данного действия. Принцип работы этих программ  основан  на перехвате соответствующих  векторов  прерываний.  К  преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению,  как  к известным, так  и неизвестным вирусам, тогда как  детекторы  пишутся  под  конкретные, известные на данный момент программисту  виды.  Это  особенно актуально сейчас, когда появилось  множество  вирусов-мутантов, не имеющих постоянного кода. Однако, программы-фильтры не могут  отслеживать вирусы, обращающиеся непосредственно к  BIOS,  а  также BOOT-вирусы, активизирующиеся ещс до запуска  антивируса,  в  начальной стадии загрузки DOS, К недостаткам  также  можно  отнести частую выдачу запросов на осуществление какой-либо операции:  ответы на вопросы отнимают у  пользователя  много  времени  и  действуют  ему  на  нервы.  При  установке    некоторых    антивирусов-фильтров могут возникать  конфликты  с  другими  резидентными программами, использующими те же прерывания, которые  просто  перестают работать. Наибольшее распространение в нашей стране  получили  программы-детекторы, а вернее программы, объединяющие в себе детектор  и доктор. Наиболее известные представители этого класса - Aidstest, Doctor Web, MicroSoft AntiVirus.

Антивирусы-детекторы расчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле  вируса  с кодами проверяемых программ.Такие программы нужно  регулярно  обновлять, так как они быстро устаревают и  не  могут  обнаруживать новые виды вирусов.

Ревизоры - программы, которые анализируют  текущее  состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов  данных  ревизора.  При  этом проверяется состояние BOOT-сектора, таблицы FAT,  а  также  длина файлов, их время создания, атрибуты, контрольная сумма.  Анализируя сообщения программы-ревизора, пользователь может решить,  чем вызваны изменения: вирусом или нет. При выдаче такого рода  сообщений не следует предаваться панике, так как причиной  изменений, например, длины программы может быть вовсе и не  вирус.

К последней группе относятся самые неэффективные антивирусы - вакцинаторы. Они записывают в  вакцинируемую  программу  признаки конкретного вируса так, что вирус считает ее уже зараженной.

Подведение итога урока.