**Конспект урока на тему**

**«Компьютерные вирусы»**

**Цели урока:**

а) образовательная: изучение новой темы

б) развивающая: развитие познавательных интересов о компьютере

в) воспитательная: формирование правового мировоззрения

**Оборудование:**

а) аппаратное обеспечение: лекция, компьютеры, видеопроектор

Тип урока: изучение новой темы, в процессе рассказа идет демонстрация презентации «Компьютерные вирусы»

**План урока:**

Организационная часть.

Объяснение нового материала.

Определение компьютерного вируса.

Классификация компьютерных вирусов.

Типы вирусов (программные, загрузочные, макровирусы).

Пути заражения.

Антивирусные программы.

Методы защиты от компьютерных вирусов.

**Ход урока:**

Компьютерный вирус – это специально созданный программный код, встроенный в другую программу или документ, или определенные области памяти и предназначенный для выполнения несанкционированных действий.

**Классификация компьютерных вирусов. [слайд 2]**

1) 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.

2) 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.

3) Вирусы, поражающие драйверы, указанные в файле config.sys, и дисковые файлы DOS. Это ведет к прекращению загрузки компьютера.

4) Вирусы DIR, меняющие файловую структуру.

5) Невидимые или стелс-вирусы. Их очень трудно обнаружить. Простейший способ маскировки - при заражении файла вирус делает вид, что длина файла не изменилась.

6) 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.

7) Сетевые вирусы - поражают машины, работающие в сети, в том числе в сети Интернет.

8) Вирусы Word (6.0 и старше), Excel, Access, PowerPoint, - поражают документы и макросы программ из MS Office.

9) Вирусы Windows-95/98 - функционируют и портят данные в среде Windows-95/98.

**По особенностям алгоритма работы различают:**

Простейшие вирусы – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.

Вирусы-спутники (компаньоны) - вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.

Стелс-вирус (невидимка) – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.

Полиморфные вирусы (мутанты) – вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.

Макровирус – вирусы, которые заражают документы офисных приложений.

Троянская программа – программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению. Программы-шпионы попадают на компьютер с электронными червями или при посещении сайтов. Для создания видеоэффектов с web-страницы иногда загружаются на наш компьютер небольшие программы, которые и могут содержать программы-шпионы. Ещё такие программы могут проникать в компьютер, подключённый к большой сети предприятия, кабельной сети и так далее. Для проникновения они используют ошибки в программах защиты сети. Обычно шпионские программы - это коммерческие программы очень высокого качества и большой сложности. Часто они направлены на получение секретной информации о кодах электронных банковских карточек. Программа-шпион не должна себя обнаруживать в компьютере. Она должна отслеживать момент выхода компьютера в Интернет и по возможности незаметно передавать данные своему хозяину. Программа-шпион может иметь функции управления компьютером. Тогда по командам хозяина, получаемым во время сеансов связи с Интернет, шпион может передавать в Интернет какие-то файлы с Вашего компьютера или интересующую его хозяина информацию о Вашем компьютере.

Черви – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту. 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 фирус 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.

Почтовый червь - это вредоносная программа, находящаяся в файле, присоединённом к электронному письму. Авторы червя всячески побуждают Вас запустить на выполнение присоединённый файл с вирусом. Его маскируют под новую игру, обновление популярных программ (в том числе, например, под обновление антивирусной программы), фотографии и так далее. В ход идёт всё. Вплоть до расчёта ширины поля, в котором почтовая программа показывает имена присоединённых файлов. Длину имени файла подбирают так, чтобы она не помещалась полностью в этом поле и не было видно истинного расширения файла "EXE" или "COM". А в видимой части поля присоединённый файл может иметь ложное расширение, соответствующее графическому, звуковому или текстовому файлу.

Будучи запущен на Вашем компьютере, вредоносный червь первым делом рассылает свою копию по электронной почте, воспользовавшись Вашей адресной книгой. А затем делает с Вашим компьютером, что хочет. Может установить программу-шпиона, может испортить Вам винчестер или сделать что-нибудь ещё. Если раньше компьютерные вирусы могли рассчитывать только на вялотекущие хронические болезни компьютеров, то теперь им иногда удаётся вызвать пандемии. Например, в недалёком прошлом такое удалось сделать почтовому червю "I love you". Он смог за несколько дней поразить миллионы компьютеров по всему миру.

**Еще одна существующая классификация вирусов – по их деструктивным возможностям. [слайд 5]**

Безвредные вирусы – оказывают незначительное влияние на работу ПК, занимая часть системных ресурсов. Нередко пользователи даже не подозревают об их присутствии.

Неопасные вирусы – также занимают часть ресурсов компьютера, но об их присутствии пользователь знает хорошо. Обычно они проявляются в виде визуальных и звуковых эффектов и не вредят данным пользователя.

Опасные вирусы – программы, которые нарушают нормальную работу пользовательских приложений или всей системы.

Очень опасные вирусы – программы, задача которых заключается в уничтожении файлов, выводе из стоя программ и ОС или рассекречивании конфиденциальных данных.

**Все компьютерные вирусы бывают двух типов – резидентные и нерезидентные.**

Резидентные вирусы представляют собой программы, присутствующие в оперативной памяти либо хранящие там свою активную часть, которая постоянно заражает те или иные объекты операционной системы.

Нерезидентные вирусы загружаются лишь во время открытия зараженного файла или работы с инфицированным приложением.

**Признаки появления вируса [слайд 6]**

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.

**Антивирусные программы [слайд 9]**

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.

**Методы борьбы с компьютерными вирусами. [слайд 16]**

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 дискет (антивирусы и программы по обслуживанию дисков).

8. 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.

Домашнее задание: Выучить теорию по теме. Подготовиться к тесту.

Используемая литература:

Макарова Н.В. Программа по информатике (системно-информационная концепция). К комплекту учебников по информатике 5-11 класс. Санкт-Петербург: Питер.2000г.

Информатика. 5-11 класс. /Под ред. Н.В. Макаровой. – СПб.: Питер, 2001

И.Семакин, Л.Залогова, С.Русаков, Л. Шестакова Базовый курс 7-9 класс

Журнал для пользователей персональных компьютеров «Мир ПК»

Журналы «КомпьютерПресс».

Леонтьев В.П. «Новейшая энциклопедия персонального компьютера»