Вирусы.

Труфанова Марина Юрьевна
учитель информатики ГБОУ СОШ №913

Цели урока:

1. Познакомиться с историей появления первых компьютерных вирусов.
2. Познакомиться с видами компьютерных вирусов, каналами их распространения и способами защиты от вирусов.

Виды вирусов

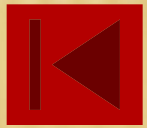
- Файловые вирусы.
- Макровирусы.
- Сетевые вирусы
- Защита от вирусов
- Каналы распространения вирусов
- Немного истории

Компьютерные вирусы являются вредоносными программами. Которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активация компьютерного вируса может вызывать уничтожение программ и данных

ФАЙЛОВЫЕ ВИРУСЫ.

- **Файловые вирусы** различными способами внедряются в исполнимые файлы и обычно активируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным.

- Практически все загрузочные файлы и файловые вирусы **резидентны**, т.е. они находятся в оперативной памяти компьютера и в процессе работы пользователя могут осуществлять опасные действия (стирать данные на дисках, изменять названия и другие атрибуты файлов). Лечение таких файлов очень затруднено.



ФАЙЛОВЫЕ ВИРУСЫ.

- Файловый нерезидентный вирус целиком размещается в исполняемом файле. Он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.
- Файловый резидентный вирус отличается от нерезидентного тем, что заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память ПЭВМ.

МАКРОВИРУСЫ.

- **Макровирусы** являются разновидностью компьютерных вирусов, созданной при помощи специальных макроязыков, встроенных в популярные офисные приложениях наподобие MS Word, MS Excel, MS Access, MS PowerPoint, Corel Draw и др.

- После загрузки заражённого документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения Более того, макросы могут незаметно совершить гораздо более опасные действия: изменить содержание документа, стереть файл или директорию. Вредоносные макросы, обладающие способностью создавать свои копии и совершающие некоторые действия без ведома пользователя и называются макровирусами.

СЕТЕВЫЕ ВИРУСЫ.

- К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, подтолкнуть пользователя к запуску зараженного файла.
- Сетевые вирусы прошлого распространялись в компьютерной сети и, как правило, так же как и компаньон-вирусы, не изменяли файлы или сектора на дисках. Они проникали в память компьютера из компьютерной сети, вычисляли сетевые адреса других компьютеров и рассылали по этим адресам свои копии.

АНТИВРУСЫ

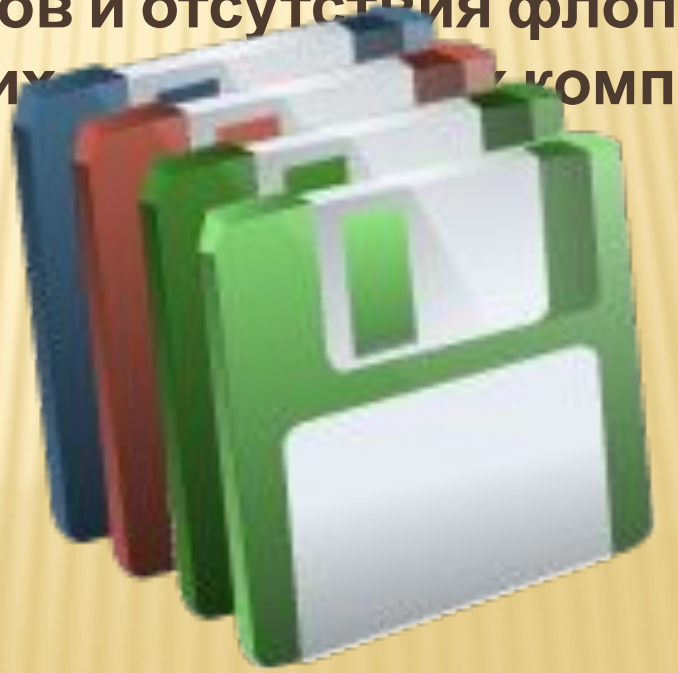
Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом (например, с помощью вакцинации).

АНТИВРУСЫ

- **Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать сотни тысяч вирусов, но ни одна из них не даст 100 % защиты.**
- **Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы.**

КАНАЛЫ РАСПРОСТРАНЕНИЯ.

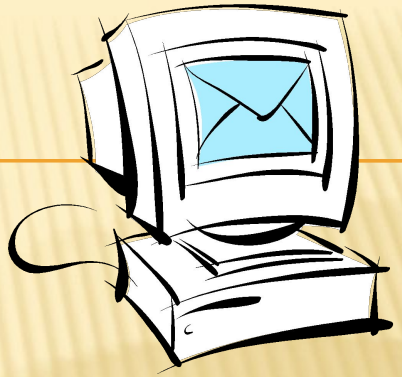
- **Дискеты**
  - **Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих компьютерах.**



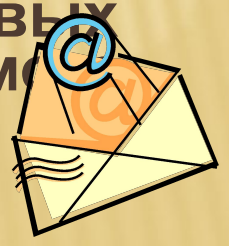
КАНАЛЫ РАСПРОСТРАНЕНИЯ.

- **Флеш-накопители (флешки)**
  - **В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной и заражения для компьютеров, не ключённ ернет**

КАНАЛЫ РАСПРОСТРАНЕНИЯ.



- **Электронная почта**
  - Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самих себя дальше.



КАНАЛЫ РАСПРОСТРАНЕНИЯ.

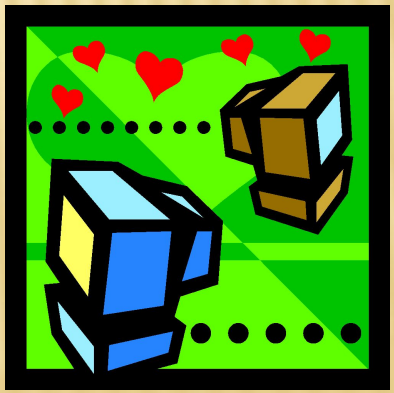
- **Системы обмена мгновенными сообщениями**
  - **Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.**

КАНАЛЫ РАСПРОСТРАНЕНИЯ.

- **Веб-страницы**
  - **Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.**

КАНАЛЫ РАСПРОСТРАНЕНИЯ.

- **Интернет и локальные сети (черви)**
  - Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости).



ИСТОРИЯ.

- С появлением первых персональных компьютеров Apple в 1977 году и развитием сетевой инфраструктуры начинается новая эпоха истории вирусов. Появились первые программы-вандалы, которые под видом полезных программ выкладывались на BBS, однако после запуска уничтожали данные пользователей. В это же время появляются троянские программы-вандалы, проявляющие свою деструктивную сущность лишь через некоторое время или при определённых условиях.

ИСТОРИЯ.

- Другие вирусы для Apple II были созданы студентом Техасского университета A&M Джо Деллинджером в 1981 году. Они были рассчитаны на операционную систему MS-DOS 3.3 для этой ПЭВМ. Вторая версия этого вируса «ускользнула» от автора и начала распространяться по университету. Ошибка в вирусе вызывала подавление графики популярной игры под названием CONGO, и в течение нескольких недель все («пиратские») копии этой игры перестали работать. Для исправления ситуации автор запустил новый, исправленный вирус, предназначенный для «замещения» предыдущей версии. Обнаружить вирус можно было по наличию в памяти счётчика заражений: «(GEN 0000000 TAMU)», по смещению $B6E8, или в конце нулевого сектора заражённого диска

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ.

- Первая эпидемия 1987 года была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Амджатом и Базитом Алви (Amdjat и Basit Faroog Alvi) в 1986 и был обнаружен летом 1987. По данным McAfee, вирус заразил только в США более 18 тысяч компьютеров. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ.

- Вторая эпидемия, берущая начало в Лехайском университете (США), разразилась в ноябре. В течение нескольких дней этот вирус уничтожил содержимое нескольких сот дискет из библиотеки вычислительного центра университета и личных дискет студентов. За время эпидемии вирусом было заражено около четырёх тысяч компьютеров.
- Последняя вирусная эпидемия разразилась перед самым Новым годом, 30 декабря. Её вызвал вирус, обнаруженный в Иерусалимском Университете (Израиль). Хотя существенного вреда этот вирус не принёс, он быстро распространился по всему миру.
- В пятницу 13 мая 1988 сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом Jerusalem — в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей пандемии — сообщения о заражённых компьютерах поступали из Европы, Америки и Ближнего Востока.

СПАСИБО ЗА ВНИМАНИЕ.