**Тема: «Компьютерные вирусы».**

**Цели:** рассмотреть классификацию компьютерных вирусов, их возможности, способы защиты от компьютерных вирусов.

**Ход работы:**

*Теоретические сведения*:

**Компьютерный вирус** – это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.

Классификация компьютерных вирусов по среде обитания:

**Файловые.** Вирусы данного вида любыми способами проникают в выполняемые файлы (характер для распространенного типа вирусов), или же сами создают файлы-двойники (носят название компаньон-вирусов), или же в своей работе используют особенности устройства файловой системы (носят название линк-вирусов).

**Загрузочные.** Вирусы данного вида помещают себя в загрузочный сектор жесткого диска, или в сектор с системным загрузчиком hard-диска, или же меняют указатель на активный загрузочный сектор винчестера. Вы наверняка встречались с баннером, который [заблокировал Windows и требовал отправить смс](http://www.spravkapc.ru/reshenie-problem/228--windows-.html). Так вот, это работа загрузочного вируса.

**Макро.** Вирусы данного вида заражают электронные таблицы и файловые документы ряда популярных редакторов.

**Сетевые.** Вирусы этого вида для своего распространения используют протоколы, либо команды компьютерных сетей, а также электронной почты.

Однако имеются и сочетания данных перечисленных видов вирусов.

Второй уровень разделения вирусов – **вид заражаемой операционной системы**. Каждый сетевой или файловый вирус заражает файлы ОС:

* DOS,
* Windows,
* Win95/NT,
* OS/2 и прочие.

Макро-вирусы заражают документы таких редакторов, как:

* Word,
* Excel.

***Загрузочные вирусы*** разделяются согласно конкретным форматам размещения системных данных в boot-секторах жесткого диска.

### *Классификация вирусов по особенностям алгоритма работы.*

**Резидентный.** При заражении компьютера в оперативной памяти оставляет свою резидентную часть, перехватывающую обращения ОС к объектам заражения для внедрения в них. Данный вид вирусов располагаются в памяти и проявляют активность до перезагрузки операционной системы или выключения компьютера. Нерезидентный вирус не заражает память компьютера, а активность его ограничена временем. Ряд вирусов даже при размещении в памяти небольших резидентных программ не распространяются. Подобные вредоносные утилиты называются нерезидентными. К резидентным вредоносным программам можно отнести макро-вирусы, так как они присутствуют в памяти компьютера постоянно во время работы зараженного редактора. В этом случае роль операционной системы переходит редактору, а активность вируса ограничена временем работы редактора. В многозадачных ОС время активности резидентного ДОС-вируса ограничивается временем работы зараженного ДОС-окна, а в ряде ОС активность ограничена временем инсталляции драйверов.

**Вирусы, использующие стелс-алгоритмы.** Они полностью или частично скрывают в системе. Самым распространенным стелс-алгоритмом считается перехват запросов операционки на чтение, либо запись зараженных объектов. Стелс-вирусы временно лечат их или же вместо себя «подставляют» незараженные участки данных. Ярким примеров использования этих алгоритмов в случае с макро-вирусами является отсутствие возможности вызова меню просмотра макросов. Одними из первых загрузочных стелс-вирусов является вирус Brain, а файловых стелс-вирусов – Frodo.

**Вирусы с самошифрованием и полиморфичностью.** Практически все типы вредоносных утилит используют данные алгоритмы работы для максимального усложнения процедуры детектирования вируса. Полиморфик-вирусы очень сложно обнаружить из-за отсутствия сигнатур, то есть отсутствия хотя бы одного постоянного участка кода. Чаще всего 2 образца такого вредоносного ПО не будут иметь ни одного схожего фрагмента кода. Данная ситуация достигается за счет шифрования основного тела вируса, а также модификации программы-расшифровщика.

**Вирусы, использующие нестандартные приемы.** Применение нестандартных приемов обусловлено необходимостью спрятать тело вируса как можно глубже в ядре операционной системе, защиты от обнаружения резидентсткой копии, затруднения лечения от вируса.

### *Классификация компьютерных вирусов по деструктивным возможностям*

**Безвредные**, не влияющие на работу компьютера, за исключение уменьшения свободного места на диске.Неопасные, влияющие лишь на уменьшение свободного места на жестком диске и на графические, звуковые и иные эффекты.

**Опасные**, приводящие к серьезным сбоям в функционировании компьютера.

**Очень опасные вирусы.** В их алгоритм работы заложены функции, вызывающие потерю программ, уничтожение данных, уничтожение необходимой для работы ПК информации из системных областей памяти.

**Практическая работа:**

**Ответьте на вопросы:**

* 1. Когда появился первый компьютерный вирус? Кто его создатель?
  2. Какие признаки заражения компьютера вирусом?
  3. Как защититься от вирусной атаки?
  4. Приведите примеры наиболее известных случаев заражения компьютеров вирусами.