**Министерство Образования Азербайджанской Республики**

**Академия Государственного Управления при**

**Президенте Азербайджанской Республики**



Факультет: Административное управление

Специализация: Компьютерные науки

Группа: K-162

Студент: Рустамова Нурана Азер

Тема: ВИДЫ ВИРУСОВ И АНТИВИРУСОВ

План:

* Вирус
  + - Что такое вирус?
    - Классификация вирусов
* Антивирусные программы
  + - Что такое антивирусная программа?
    - Некоторые её параметры
    - Виды антивирусных программ
* Вопросы по изученному материалу
  + - Блок контроля
    - Блок самоконтроля

Вообще, что такое вирус???

* Прежде всего, вирус – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.
* Активизация компьютерного вируса может вызвать уничтожение программ и данных, и даже уничтожение составляющих компьютера (системного блока).

Признаки появления вирусов:

* Неправильная работа нормально работающих программ
* Частые зависания и сбои в работе ПК
* Медленная работа ПК
* Изменение размеров файлов
* Исчезновение файлов и каталогов
* Неожиданное увеличение количество файлов на диске
* Уменьшение размеров свободной оперативной памяти
* Вывод на экран неожиданных сообщений и изображений
* Подача непредусмотренных звуковых сигналов
* Невозможность загрузки Операционной Системы

Классификация вирусов

* Загрузочные вирусы
* Файловые вирусы
* Макро-вирусы
* Сетевые вирусы

Загрузочные вирусы

* заражают загрузочный сектор гибкого диска или винчестера.
* При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.

Файловые вирусы

* при своем размножении тем или иным способом используют файловую систему операционной системы.
* Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).

Макро-вирусы

* являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).
* Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Сетевые вирусы

* для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.
* Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

Вирусы делятся также на резидентные и нерезидентные

Первые, в отличие от нерезидентных, при получении управления загружаются в память и могут действовать не только во время работы зараженного файла.

Дополнительные типы вирусов

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые распространяются вирусы и другие вредоносные программы.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

* утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
* программные библиотеки, разработанные для создания вредоносного ПО;
* хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
* «злые шутки», затрудняющие работу с компьютером;
* программы, сообщающие пользователю заведомо ложную

информацию о своих действиях в системе;

* прочие программы, тем или иным способом намеренно

наносящие прямой или косвенный ущерб данному или

удалённым компьютерам.

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 источник заражения для компьютеров.
* 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.
* 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.
* Веб-страницы . Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

Антивирусные программы

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

* Антивирусные блокировщики
* Ревизоры
* Полифаги
* Полифаги-мониторы

Краткий обзор антивирусных программ

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту

ее обновления,

наличие

дополнительных

функций.

Наиболее известные из антивирусных программ

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Однако только 200-300 вирусов из них можно встретить, а опасность представляют лишь несколько десятков из них.

Norton AntiVirus

Один из известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы. В интерфейсе программы Norton AntiVirus имеется функция LiveUpdate, позволяющая щелчком на одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов.