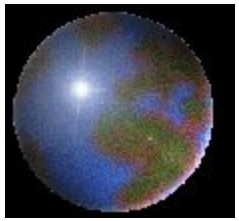
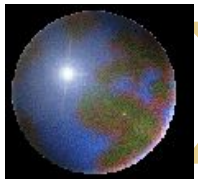


Лекция №3

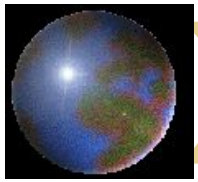
Системное программное обеспечение: антивирусные программы

Лекцію підготував: ст. викладач Денисова Л.В.



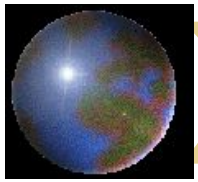
План

- Свойства компьютерного вируса
- **Классификация компьютерных вирусов**
- **Основные симптомы вирусного поражения**
- **Антивирусные программы**



Обязательным свойством компьютерного вируса

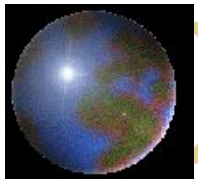
является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.



Классификация компьютерных вирусов

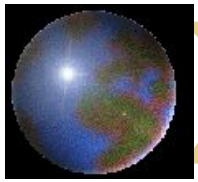
В настоящее время известно более 70 000 программных вирусов, их можно классифицировать по следующим признакам:

- *по среде обитания;*
- *по способу заражения среды обитания;*
- *по воздействию (деструктивным возможностям);*
- *по особенностям алгоритма.*



По среде обитания вирусы можно разделить на:

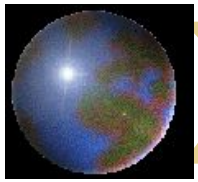
- ***файловые*** - либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы);
- ***загрузочные*** - записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор;
- ***макро вирусы*** - заражают файлы-документы и электронные таблицы нескольких популярных редакторов;
- ***сетевые*** - используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.



По способу заражения среды обитания вирусы делят на:

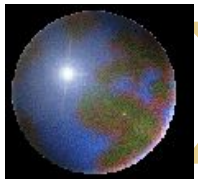
- ***Резидентные вирусы*** - при инфицировании компьютера оставляющие в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

- ***Нерезидентные вирусы*** - не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.



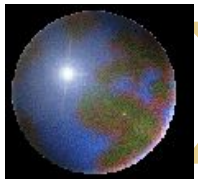
По деструктивным возможностям вирусы можно разделить на:

- ***безвредные,*** т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результа-те своего распространения);
- ***неопасные,*** влияние которых ограничивается уменьшением свободной памяти на диске и, как правило, сопровождаю-щиеся графическими, звуковыми и пр. эффектами;
- ***опасные*** вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- ***очень опасные,*** в алгоритм работы которых заведомо зало-жены процедуры, ведущие к потере программ, уничтожению данных, стиранию необходимой для работы компьютера информации, записанной в системных областях памяти.



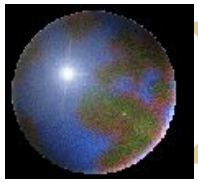
По особенностям алгоритма вирусы делят на классы по показателям:

- ***Использование стелс-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись заражен-ных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. («Frodo», «Brain»).
- ***Самошифрование и полиморфичность*** используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы (polymorphic) - это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.
- ***Использование различных нестандартных приемов*** в вирусах позволяет как можно глубже спрятать себя в ядре ОС («ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.



Основные симптомы вирусного поражения:

- Прекращение работы или неправильная работа ранее успешно функционировавших программ.
- Невозможность загрузки операционной системы.
- Замедление работы компьютера.
- Исчезновение файлов и каталогов или искажение их содержимого.
- Увеличение размеров файлов (особенно выполняемых).
- Изменение даты и времени модификации файлов.
- Неожиданное значительное увеличение количества файлов на диске.
- Существенное уменьшение размера свободной оперативной памяти.
- Появление не существовавших ранее “странных” файлов.
- Вывод на экран непредусмотренных сообщений или изображений.
- Подача непредусмотренных звуковых сигналов.



Антивирусные программы делятся на:

Специализированные антивирусные программы *(AidsTest)* способны находить и ликвидировать только определенные типы уже известных вирусов. С неизвестными (новыми) вирусами эти программы бороться не могут.

Универсальные антивирусные программы *(DrWeb)*, в свою очередь, делятся на *резидентные* программы и *программы-ревизоры(Adinf)*.

Резидентные постоянно находятся во внутренней памяти компьютера и периодически осуществляют проверку на наличие вирусов.

Антивирусы-ревизоры способны только установить, поддавался ли файл каким-либо изменениям (в том числе и вирусным) после последнего его редактирования.