Защита и резервирование информации

Под защитой информации понимается порядок и правила применения принципов и средств защиты информации.

Методы обеспечения информации.

- Правовые методы законодательно устанавливают правила использования данных ограниченного доступа и устанавливают меру ответственности за нарушение этих правил.

Основными международными стандартами в области защиты информации являются:

- Согласованные критерии оценки безопасности информационных технологий европейских стран
- Международный стандарт ISO/ IEC 17799:2000 «Управление информационной безопасностью - Информационные технологии.»
- Международный стандарт ISO/ IEC 15408 « Общие критерии безопасности информационных технологий», который на данный момент признаётся одним из наиболее функциональных стандартов в сфере информационной безопасности (ИБ).

Организационные и административные методы.

- Организационные и административные методы – это методы направленные в основном на работу с персоналом.

Инженерно-технические мероприятия.

- Инженерно-технические мероприятия направлены на защиту информации от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, разработку и реализацию программных и аппаратных комплексов безопасности и т.д.

Антивирусная защита

- Компьютерные вирусы – это вид вредоносного ПО, программы которого способны создавать и внедрять свои копии в ресурсы компьютерных систем, сетей и производить действия без ведома пользователя, приводящие к нежелательным последствиям.

Классификация вирусов

По среде обитания:

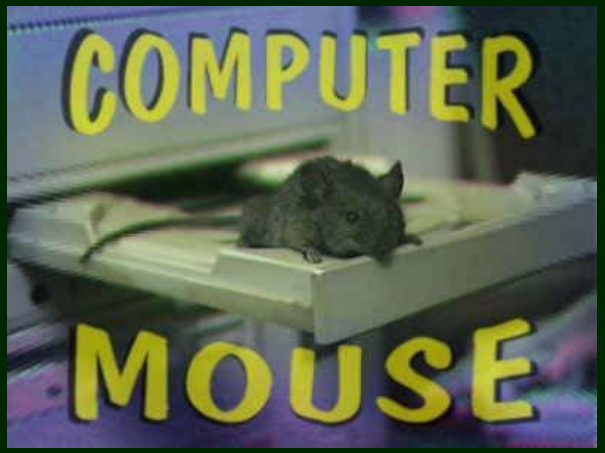
- Файловые
- Загрузочные
- Файлово - загрузочные
- Сетевые

По целостности:

- Монолитные
- распределённые

Разгрузочные вирусы

- Загрузочные вирусы - это разновидность вирусов, которые после запуска заражают, как дискеты, так и непосредственно сам жесткий диск, записываясь вместо главной загрузочной записи.

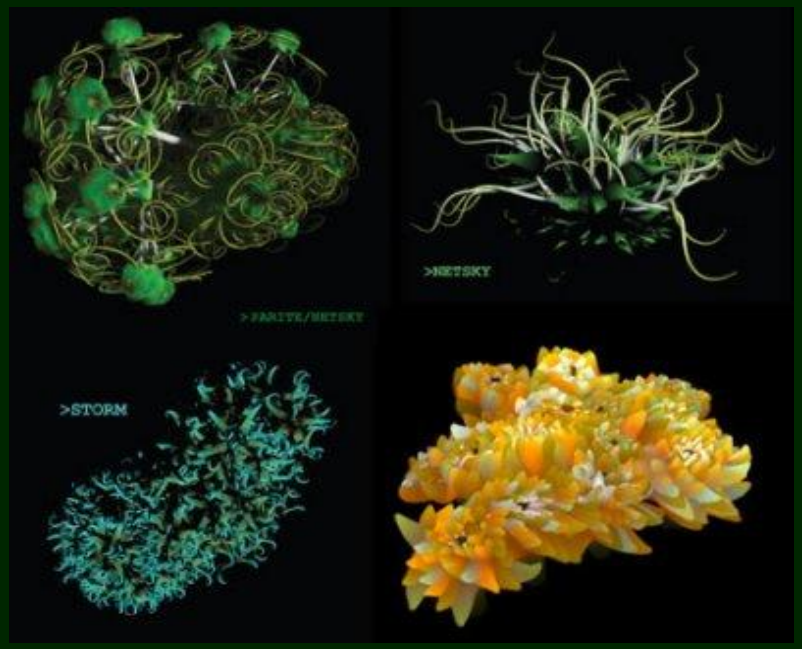


Файловые вирусы

- Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных - документы или электронные таблицы, - однако эти вирусы настолько специфичны, что вынесены в отдельную группу.

Резидентные вирусы

- Под термином "резидентность" (DOS'овский) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов).



Паразитические вирусы

- Компью́терные ви́русы — разновидность самовоспроизводящихся компьютерных программ, которые распространяются, внедряя себя в исполняемый код других программ или в документы специального формата, содержащие макрокоманды, такие, как MS Word и Excel. Многие вирусы вредят данным на заражённых компьютерах, хотя иногда их единственной целью является лишь заражение как можно большего количества компьютеров.
  В общем словоупотреблении к компьютерными вирусами причисляют все вредоносные программы, такие как сетевые и файловые черви, троянские кони, программы-шпионы.

Вирусы-невидимки

- **Stealth-вирусы (Стэлс) или вирусы-невидимки** являются разновидностью резидентных вирусов (постоянно находяться в оперативной памяти). Stealth-вирусы фальсифицируют информацию прочитанную из диска так, что программа, которой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах.