1. Внутренние и внешние угрозы, классификация вредоносного программного обеспечения: вирусы, логические бомбы, «шпионские программы», «трояны» - определение и исследование

Ответ:

Под угрозой понимают возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательными воздействия на информацию:

А) нарушение физической целостности

Б) несанкционированная модификация

В) несанкционированное получение

Г) несанкционированное размножение информации.

В общем случае угрозы безопасности информационной системы могут быть разделены на внутренние (хакер владеет offline доступ ) и внешние (хакер имеет удалённый доступ).

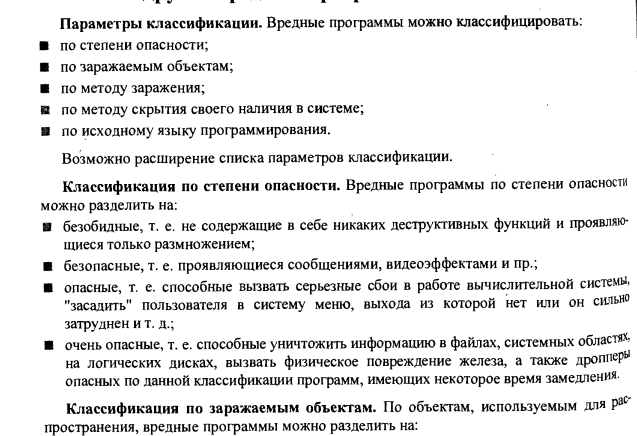
Вирус. Это программа, которая характеризуется двумя основными особенностями:

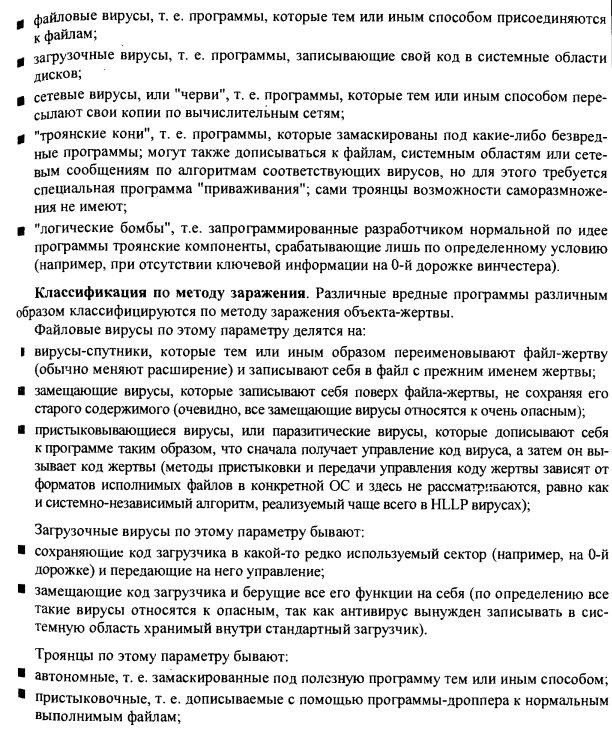
1. Без ведома пользователя компьютера осуществляет несанкционированные действия, направленные либо

а) на создание, изменение, искажение, удаление, несанкционированную передачу данных, либо

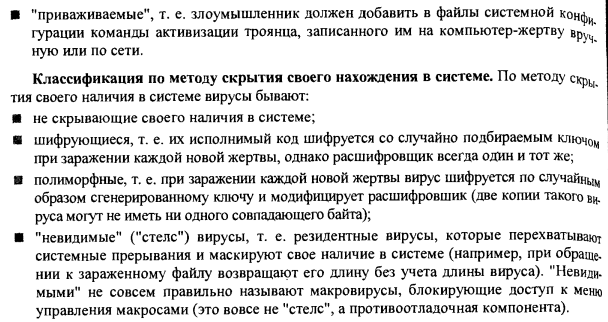
б) на изменение (разрушение) принципов функционирования систем обработки данных (на создание новых, изменение существующих программ обработки данных).

2. Без ведома пользователя компьютера размножается (заражает файлы) посредством изменения или полной замены функционирующих программ либо исполнимых файлов.





После лекции 3 мы решили, что не будем говорить, что существуют сетевые вирусы и макро-вирус это вирус.В итоге есть две большие классификации Файловые и Загрузочные ( во время Загрузки В ОПЕРАТИВНУЮ ПАМЯТЬ ПРОГРАММНЫХ СРЕДСТВ, являющихся составной частью ОС)



**Общий алгоритм обнаружения вируса**

При анализе алгоритма вируса необходимо выяснить:

· способ(ы) размножения вируса;

· характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;

· метод лечения оперативной памяти и зараженных файлов (секторов).

**При анализе файлового вируса** необходимо выяснить, какие файлы (COM, EXE, SYS) поражаются вирусом, в какое место (места) в файле записывается код вируса - в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

**При анализе загрузочного вируса** основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор.

**Для резидентного вируса** требуется также выделить участок кода, создающий резидентную копию вируса. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии.

**Для анализа макровирусов** необходимо получить текст их макросов. Для нешифрованных ("не-стелс") вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует "стелс"-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов. Такие специализированные утилиты есть практически у каждой фирмы-производителя антивирусов, однако, они являются утилитами "внутреннего пользования" и не распространяются за пределы фирм.