Лекция 3

Толкование 20.
Не существует абсолютной классификации нехороших изделий, однако в различных источниках можно найти, что классифицировать их можно по таким критериям, как:
По характеру вредоносного воздействия, по способу реализации, по способу проникновения, по способности к саморазмножению.

Толкование 21.
По характеру вредоносного воздействия могут быть выделены следующие поражения систем тем, что называется “нехорошим изделием”
а) уничтожения, или искажения данных и программных средств
б) вывод системы из строя
в) вредоносное инициирование функционала системы
То есть невовремя и не в том месте
г) создание препятствия к выполнению функций системы

Толкование 22.
По способу проникновения в систему, badware могут быть классифицированы следующим образом:
а) в процессе производства аппаратной, или программной компонент системы
б) неосознанное внесение изменений персоналом в процессе функционирования системы
в) злонамеренные атаки
г) в процессе ремонта, или обновления оборудования, или ПО

Толкование 23.
В общем случае, угрозы безопасности информационной системы так же могут быть разделены на внутренние и внешние.

Программно-технические угрозы безопасности подробно рассмотрены на страницах 87-125. Из этих страниц важным является то, что на основании этих страниц, готовились билеты, на которые мы должны будем делать бомбы.

Тем, чем ближе к аппаратному уровню уровень системы защиты, при прочих равных условиях, тем выше уровень безопасности данной системы. Далее, мы будем говорить о шпиономании (вероятнее всего, начнём с неё). Но тк сегодняшняя лекция больше связана с Боровым, то придется записать еще несколько толкований.

Толкование 24. Классификация вредоносных программ.
Вредоносные нехорошие изделия можно разбить на группы. Вредоносных программ меньше, чем нехороших изделий.
Под вирусом будем понимать программу, то есть некоторую совокупность команд, или инструкций, которая сидит в оперативной памяти компьютера

и которая характеризуется двумя основными особенностями:

1. Без ведома пользователя компьютера осуществляет несанкционированные действия, направленные либо на создание, изменение, искажение, удаление, несанкционированную передачу данных, либо на изменение (разрушение) принципов функционирования систем обработки данных (на создание новых, или изменение существующих программ обработки данных)
2. Без ведома пользователя компьютера, программа заражает файлы на внешних устройствах посредством изменения или полной замены функционирующих программ, либо исполнимых файлов (заменить функционирующую программу очень сложно, поэтому в основном, заражение касается файлов, расположенных на внешних устройствах)

Существуют различные варианты классификации вирусов, как всегда, они могут быть поделены на группы, в зависимости от выбранного критерия классификации. В частности, вирусы можно разделить по типу объектов, которые они заражают, по методам заражения, по выбираемым жертвам, по среде обитания. Например, классифицируя вирусы по среде обитания, выделяют 2 типа вирусов, BootSector вирусы, либо вирусы-паразиты (их еще называют файловые вирусы)
Файловые вирусы - это программы, которые поражают файлы компьютера. После загрузки исполнимого модуля соответствующего вируса, т.е. Программы, которая будет посажена в оперативную память, эти вирусы в большинстве случаев, сделав какую-либо гадость с данными, хранящимися в компьютере, либо с исполнимыми модулями, обеспечивающими функционирование системы обработки данных, заражают эти файлы, либо отдельные элементы DLL.
При последующих загрузках уже зараженных исполнимых файлов, либо каких-либо других файлов, в оперативную память, они делают свои нехорошие дела и заражают другие данные (в других папках, или на других дисках)
2я группа вирусов - загрузочные вирусы (bootsector). Любая ОС (совокупность аппаратных и программных средств, предназначенных для управления устройствами компьютера и предоставлению сервисов сторонним программам по управлению этими устройствами). Так вот эта любая ОС организована таким образом, что после включения компьютера, сначала отрабатывает аппаратная часть ОС, включая организацию и осуществление процесса, под названием “Загрузка ОС”. Дальше будем говорить не загрузка ОС, а “загрузка программной части ОС”. Для хранения информации и ПО необходимых для реализация этой загрузки программной части используются так называемый загрузочный сектор (bootsъctor). В том случае, когда в этом загрузочном секторе появляется вредоносная программа (именно программа), замаскированная таким образом, что в какой-то момент времени, она получает управление в соответствие с правилами загрузки программной части ОС. Она делает свое дело в виде порчи программ или исполнимых модулей и сопровождает эту деятельность порчей или заражением других

исполнимых файлов, такую программу называют загрузочным вирусом.

Как было сказано ранее, существует так называемые нехорошие изделия. Их тоже можно классифицировать по месту их нахождения. В частности, бывают сетевые нехорошие изделия. Суть этих нехороших изделий заключается в том, что они обитают и передаются по сети, либо вирусами-паразитами, либо вирусами, под названием bootsector вирусами, они становятся только при каких-то условиях в оперативную память.
По месту обитания можно выделить и так называемые макро нехорошие изделия, эти изделия, или их суть, заключается в том, что они поражают так называемые макросы. Известно, что большинство программных средств, будь то Excel, 1С предприятие, будто Word, или еще какие-то программные средства, имеют свой, встроенный язык, который позволяет формировать макросы. Очень часто в этих макросах могут скрываться вот эти самые нехорошие изделия. В том случае, когда в какой-то момент времени, этот макрос инициализируются и ему передаётся управление, когда он находится в ОС, появляется вирус, чаще всего паразитический.
На ряду с указанными нехорошими изделиями по месту обитания чаще всего к нехорошим изделиям так же относят нехорошие изделия под названием “черви”. Это программное изделие, которое попадает в оперативную память, не заражает, в отличие от вируса, другие файлы и данные, а осуществляют действия, направленные на поиск уязвимостей в сетевых связях с другими компьютерами, чаще всего, эти черви существуют в виде сохранённых на жёстком диске файлов, а некоторые, поселяются в оперативной памяти компьютера.
Также выделяют нехорошие изделия под названием “Троян”, которое, попадая в оперативную память, не становится вирусом, оно становится программой, которая тоже не заражает данные, находящиеся на внешнем устройстве. Она заставляет компьютер исполнить незадокументированный функционал.

Нехорошее изделие “Руткит”, которое становится программой, попадая в оперативную память, предполагает, или осуществляет сокрытие вредоносной активности путём модификации программных средств, операционных систем таким образом, чтобы информация о функционировании как самой программы rootkit, или других программ, полученных в качестве нехороших изделий, была недоступна, или скрыта, от программных средств защиты, характерных для тех, или иных, операционных оболочек.