Тема 3-4

1) Для того чтобы вирус мог выполнить какие либо действия, он должен оказаться в памяти в виде программного кода и получить доступ к управлению компьютером.

Исполняемые программы(.exe)

Загрузочные секторы дисков(MBR=Master Boot Record)

Драйверы(.sys)

Библиотеки динамической загрузки(.dll)

Документы с макросами(не заражает файлы с данными(тексты, рисунки, звук, видео))

Веб-страницы(внедрение программы-скрипта)

2) Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Такие вирусы называются невидимыми, или stealth (стелс) вирусами. Разумеется, эффект "невидимости" наблюдается толькона зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

3)Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать. Стелс-вирусы (невидимки) перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

4) Методы борьбы с компьютерными вирусами: Резервное копирование всех программ, файлов и системных областей дисков на накопители, чтобы можно было восстановить данные в случае вирусной атаки. Создание системного и аварийного накопителя. Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков. Включение антивирусного протектора от загрузочных вирусов в CMOS Setup машины.

5) Специализированные программы защиты от компьютерных вирусов применяются в случаях когда пользователь сам не в состоянии очистить компьютер от вирусов, а также для предостережения заражения компьютера вирусом.

6) Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов: Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Программы-доктора, или фаги, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.

7) **Программы**-**детекторы**. **Программы**-**детекторы** осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

8) Сигнатура вируса - это **уникальная** **последовательность** **байтов**, принадлежащая вирусу и не встречающаяся в других программах.

9) Программы- детекторы практически не вызывают ложные тревоги. Если программа сообщила о заражении, то можно быть уверенным, что это действительно так. (Ранние версии иногда ошибались, например, объявляли зараженными файлы других антивирусных программ, находя в них сигнатуры вирусов.). Но если детектор не обнаружил вирусы в системе, это означает только то, что в системе нет вирусов, на которые он рассчитан.

10)Принцип работы ревизоров основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

Программы-фильтры или "сторожа" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

Вакцины используют в том случае, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация может быть использована только от известных вирусов. Суть данного метода в том, что вакцина видоизменяет программу или диск таким образом, чтобы это не выражалось в их работе, а вирус будет считать их зараженными, и, следовательно, не внедрится.

11) Многоуровневая защита от вирусов представлена в виде модулей:

1. Эвристический модуль-для выявления неизвестных вирусов.

2. Монитор-программа которая постоянно находится в памяти ПК.

3. Устройство управления-осуществляет запуск антивирусных программ и обновление вирусной базы данных и компонентов.

4. Программа сканер-проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков.

5. Сетевой экран-защита от хакерских атак.

12) Защита от компьютерных вирусов. Основными мерами защитыот вирусов считаются: резервирование (копирование, ежедневное ведение архивов измененных файлов); профилактика (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ).

13) Технология антивирусной защиты реализуется при помощи специализированного программного обеспечения, называемого антивирусными программами. Существует четыре основных типа антивирусных программ: сканеры, программы контроля целостности данных, мониторы и гибридные антивирусные средства. Алгоритм работы антивирусного сканера заключается в обнаружении вирусов на базе сигнатур, хранящихся в БД сканера.

Тема Симметричные криптосистемы

1) Криптология - наука, объединяющая криптографию и криптоанализ.

2) Криптография решает следующие задачи: шифрование данных с целью защиты от несанкционированного доступа; проверка подлинности сообщений; проверка целостности передаваемых данных; обеспечение невозможности отказа.

3) Криптографический алгоритм — набор правил, который используется для шифрования информации, чтобы ее могли прочитать только авторизованные стороны.

4) Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования: - зашифрованные сообщения должны поддаваться чтению только при наличии ключа; - число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей.

5) Шифр замены - заменяет каждый знак входного алфавита на некоторый знак из того же алфавита.

6) При многоалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй - символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты.

7) Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

8) Гаммирование— метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

9) При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов.

10) Важнейшим показателем надежности криптографического закрытия информации является его стойкость -- тот минимальный объем зашифрованного текста, который можно вскрыть статистическим анализом. Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

11) Трудоемкость метода шифрования определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста

12) маршрутная перестановка, основанна на некоторой геометрической фигуре. Отрезок открытого текста записывается в такую фигуру по некоторой траектории. Шифрованным текстом является последовательность, полученная при выписывании текста по другой траектории.

13) Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера клеток. В трафарете вырезано тк клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

15) Шифры сложной замены – шифры сложной замены отличаются от шифров простой замены тем, что в них при шифровании используется много алфавитов.