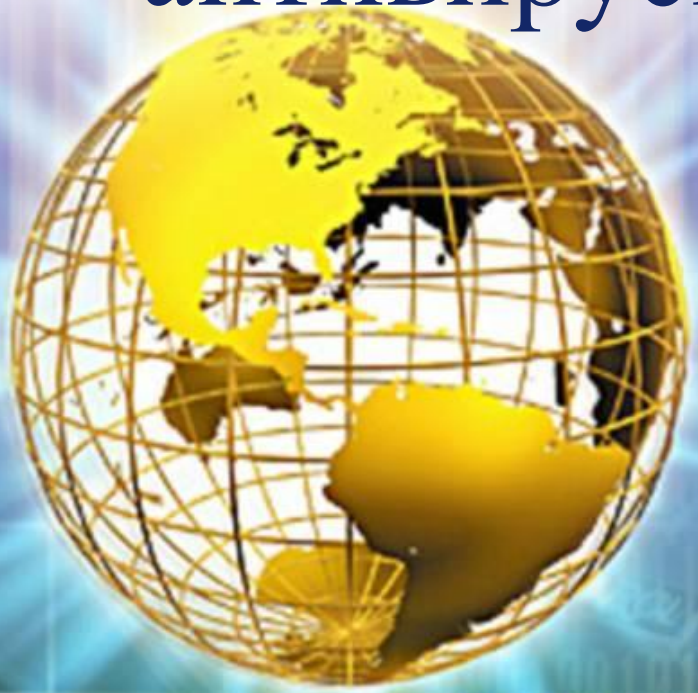
Кодирование и шифрование информации
Компьютерные вирусы и антивирусные программы



Лекция №6

План

1. Кодирование и шифрование
2. Компьютерные вирусы, антивирусные программы

Кто владеет информацией – владеет миром.

Информационная безопасность

Информационная безопасность информационной системы – защищенность информации, обрабатываемой компьютерной системой, от внутренних (внутрисистемных) или внешних угроз, то есть состояние защищенности информационных ресурсов системы, обеспечивающее устойчивое функционирование, целостность и эволюцию системы.

Что нужно защищать?

- электронные документы и спецификации
- программное обеспечение
- структуры и базы данных
- информация личного характера
- информация финансового характера
- военная информация
- и др.

Кодирование и шифрование

Как вы считаете, понятия «кодирование» и «шифрование» являются синонимами?

Кодирование и шифрование

Преобразование информации

Кодирование

Изменяет форму, но оставляет прежним содержание
Для прочтения нужно знать алгоритм и таблицу кодирования

Шифрование

Может оставлять прежней форму, но изменяет, маскирует содержание
Для прочтения недостаточно знать только алгоритм, нужно знать ключ

Кодирование

Код – правило соответствия набора знаков одного множества X знакам другого множества Y.

Кодирование – процесс преобразования букв (слов) алфавита X в буквы (слова) алфавита Y.

Кодирование

Если каждому символу X при кодировании соответствует отдельный знак Y, то это кодирование.

Если для каждого символа из Y однозначно отыщется по некоторому правилу его прообраз в X, то это правило называется декодированием.

Кодирование

Пример:

Если каждый цвет кодировать:

2 битами, то можно закодировать не более $2^2 = 4$ цветов,

3 битами – $2^3 = 8$ цветов,

8 битами (байтом) – 256 цветов.

Шифрование

Открытый текст – это сообщение, текст которого необходимо сделать непонятным для посторонних.

Шифр - совокупность обратимых преобразований множества возможных открытых данных во множество возможных шифртекстов, осуществляемых по определенным правилам с применением ключей.

Шифрование

Шифрование – процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре.

Шифрование

Исходное сообщение: «A»

Зашифрованное: «B»

Правило шифрования: «f»

Схема шифрования: f(A)=B

Правило шифрования f не может быть произвольным. Оно должно быть таким, чтобы по зашифрованному тексту B с помощью правила g можно было однозначно восстановить отрытое сообщение.

Шифрование

Дешифрование – процесс, обратный шифрованию, т.е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Правило дешифрования: «g»

Схема дешифрования: g(B)=A

Шифрование

Ключ – конкретное секретное состояние некоторого параметра (параметров), обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования.

Это сменный элемент шифра.

Шифрование

Если k – ключ, то **f(k(A)) = B**

Для каждого ключа k, преобразование f(k) должно быть обратимым, то есть

g(k(B)) = A

Отличие кодирования от шифрования

При кодировании секретного ключа нет, так как кодирование ставит **целью** лишь более **сжатое**, **компактное** представление сообщения.

Криптология – область секретной связи

Криптология
«cryptos» - тайна
«logos» - слово

Криптография

Наука о создании шифров

Криптоанализ

Наука о вскрытии шифров

Классификация криптоалгоритмов

Основная схема классификации:

Тайнопись и Криптография с ключом

По характеру ключа:

Симметричные и Асимметричные

По характеру воздействий на данные:

Перестановочные и Подстановочные

В зависимости от размера блока информации:

Потоковые и Блочные

Симметричная криптография

Если в процессе обмена информацией для шифрования и дешифрования информации пользуются одним и тем же ключом, то такой криптографический процесс является **симметричным**.

Недостатки симметричного шифрования

Необходимость наличия защищенного канала связи для передачи ключа.

Пример:

Если рассмотреть оплату клиентом товара или услуги с помощью кредитной карты, то получается, что торговая фирма должна создать по одному ключу для каждого своего клиента и каким-то образом передать им эти ключи. Это крайне неудобно.

Асимметричная криптография

Используется два ключа: открытый и секретный

На самом деле это как бы две «половинки» одного целого ключа, связанные друг с другом.

Асимметричная криптография

- Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было закодировано).

- Создав пару ключей, компания широко распространяет открытый ключ и надежно сохраняет секретный ключ.

Асимметричная криптография

1. Публичный и закрытый ключи представляют собой некую последовательность.

2. Публичный ключ может быть опубликован на сервере, откуда каждый желающий может его получить. Если клиент хочет сделать фирме заказ, он возьмет ее публичный ключ и с его помощью зашифрует свое сообщение о заказе и данные о своей кредитной карте.

3. После шифрования это сообщение может прочесть только владелец закрытого ключа. Никто из участников цепочки, по которой пересылается информация, не в состоянии это сделать.

4. Даже сам отправитель не может прочитать собственное сообщение. Лишь получатель сможет прочесть сообщение, поскольку только у него есть секретный ключ, дополняющий использованный открытый ключ.

Асимметричная криптография

Пример:

Если фирме надо будет отправить клиенту квитанцию о том, что заказ принят к исполнению, она зашифрует ее своим секретным ключом.

Клиент сможет прочитать квитанцию, воспользовавшись имеющимся у него открытым ключом данной фирмы.

Он может быть уверен, что квитанцию ему отправила именно эта фирма, поскольку никто иной доступа к закрытому ключу фирмы не имеет.

Принцип достаточности защиты

Алгоритмы шифрования с открытым ключом нет смысла скрывать. Обычно к ним есть доступ, а часто они просто широко публикуются.

Тонкость заключается в том, что **знание алгоритма еще не означает возможности провести реконструкцию ключа, в разумно приемлемые сроки.**

Принцип достаточности защиты

- **Защиту информации** принято считать **достаточной**, если затраты на ее преодоление превышают ожидаемую ценность самой информации.
- Защита не абсолютна и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие нецелесообразным.
- При появлении иных средств, позволяющих получить зашифрованную информацию в разумные сроки, изменяют принцип работы алгоритма, и проблема повторяется на более высоком уровне.

Криптоанализ

Не всегда поиск секретного ключа производят методами простого перебора комбинаций. Для этого существуют специальные методы, основанные на исследовании особенностей взаимодействия открытого ключа с определенными структурами данных.

Область науки, посвященная этим исследованиям, называется **криптоанализом**.

Криптоанализ

Средняя продолжительность времени, необходимого для реконструкции закрытого ключа по его опубликованному открытому ключу, называется **криптостойкостью алгоритма шифрования**.

Криптоанализ

В России к использованию в государственных и коммерческих организациях разрешены только те программные средства шифрования данных, которые прошли **государственную сертификацию** в административных органах, в частности, в Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Понятие об электронной подписи

Клиент может общаться и с банком, отдавая ему распоряжения о перечислении своих средств на счета других лиц и организаций. Однако здесь возникает проблема: как банк узнает, что распоряжение поступило именно от данного лица, а не от злоумышленника, выдающего себя за него?

Эта проблема решается с помощью **электронной подписи**.

Понятие об электронной подписи

При создании электронной подписи создаются два ключа: секретный и открытый.

Открытый ключ передается банку. Если теперь надо отправить поручение банку на операцию с расчетным счетом, оно шифруется открытым ключом банка, а своя подпись под ним - собственным секретным ключом. Банк поступает наоборот.

Если подпись читаема – это 100% подтверждение авторства отправителя.

Принцип Кирхгоффа

- Все современные криптосистемы построены по **принципу Кирхгоффа**: секретность зашифрованных сообщений определяется секретностью ключа.

- Если даже алгоритм шифрования будет известен криптоаналитику, тот тем не менее не в состоянии будет расшифровать закрытое сообщение, если не располагает соответствующим ключом.

Принцип Кирхгоффа

- Все классические шифры соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полный перебор по всему ключевому пространству, то есть перебор всех возможных значений ключа.
- Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Компьютерный вирус

Основными типами средств воздействия на компьютерные сети и системы являются **компьютерные вирусы**.

Компьютерным вирусом называется программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной копии, причем последняя сохраняет способность к дальнейшему размножению.

Компьютерный вирус

Помимо заражения, вирус подобно любой другой программе, может выполнять и другие несанкционированные действия, от вполне безобидных до крайне разрушительных.

Признаки заражения компьютерным вирусом

- замедление работы компьютера;
- невозможность загрузки операционной системы;
- частые «зависания» и сбои в работе компьютера;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- увеличение количества файлов на диске;
- изменение размеров файлов;
- периодическое появление на экране монитора неуместных системных сообщений;
- уменьшение объема свободной оперативной памяти;
- заметное возрастание времени доступа к жесткому диску;
- изменение даты и времени создания файлов;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);
- загорание сигнальной лампочки дисковода, когда к нему нет обращения.

Источники распространения компьютерных вирусов

- Интернет
- Интранет
- Электронная почта
- Съемные носители информации

Интернет

Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, «маскируют» их под полезное и бесплатное программное обеспечение. Кроме того, скрипты, автоматически запускаемые при открытии веб-страницы, могут выполнять вредоносные действия на вашем компьютере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и серверы компаний. Результатом таких атак может являться выведение ресурса из строя, получение полного доступа к ресурсу.

Интранет

Интранет - это внутренняя сеть, специально разработанная для управления информацией внутри компании или, например, частной домашней сети. Интранет является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети.

Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются огромному риску заражения. Во избежание возникновения таких ситуаций необходимо защищать не только периметр сети, но и каждый отдельный компьютер.

Электронная почта

Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысяч своих абонентов.

Помимо угрозы проникновения вредоносных программ существуют проблема внешней нежелательной почты рекламного характера (*спама*). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые серверы, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный финансовый урон.

Съемные носители информации

Съемные носители - дискеты, CD/DVD-диски, флеш-карты - широко используются для хранения и передачи информации.

При запуске файла, содержащего вредоносный код, со съемного носителя вы можете повредить данные, хранящиеся на вашем компьютере, а также распространить вирус на другие диски компьютера или компьютерные сети.

Классификация компьютерных вирусов

Среда обитания

- **Сетевые вирусы** распространяются по различным компьютерным сетям.
- **Файловые вирусы** внедряются главным образом в исполняемые модули, в файлы COM и EXE. Могут внедряться и в другие, но, записанные в таких файлах, они никогда не получают управление и теряют способность к размножению.
- **Загрузочные вирусы** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- **Файлово-загрузочные вирусы** заражают как файлы, так и загрузочные сектора дисков.

Способ заражения

- **Резидентный вирус** оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
- **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

Степень воздействия

- **Неопасные (безвредные)**, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, проявляются в каких-либо графических или звуковых эффектах.
- **Опасные**, которые могут привести к различным нарушениям в работе компьютера
- **Очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Особенности алгоритма

- «**Черви**» - распостраняются в компьютерных сетях, проникают в память ПК из компьютерной сети, вычисляют адреса других ПК и пересылают на эти адреса свои копии. Иногда оставляют временные файлы на ПК, но некоторые могут и не затрагивать ресурсы компьютера за исключением ОЗУи CPU.
- **Спутники** - поражают EXE-файлы путем создания COM-файла двойника, и по этому при запуске программы запустится сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения "инфицированная" программа не изменяется.
- "**Паразитические**" - модифицируют содержимое файлов или секторов на диске.

Особенности алгоритма

- "**Полиморфные**" (самошифрующиеся или вирусы-призраки, polymorphic) - достаточно труднообнаруживаемые, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

- "**Макро-вирусы**" - используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы, заражающие текстовые документы редактора Microsoft Word.

Особенности алгоритма

- "**Стелс-вирусы**" (вирусы-невидимки, stealth) - представляющие собой весьма совершенные программы, которые перехватывают обращения к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие "обманывать" резидентные антивирусные мониторы.

- **Троянские программы** не способны к самораспространению, очень опасны (разрушают загрузочный сектор и файловую систему дисков), распространяются под видом полезного ПО.

Программы-шпионы (Spyware)

ПО, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться.

Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании HDD; чаще всего сканируются некоторые каталоги и системный реестр с целью составления списка ПО, установленного на ПК;
- сбор информации о качестве связи, способе подключения,
- скорости модема и т.д.

Программы-рекламы (Adware)

Программный код, без ведома пользователя включенный в ПО с целью демонстрации рекламных объявлений.

Программы-рекламы встроены в ПО, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шутки (Jokes)

ПО, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Программы-маскировщики (Rootkit)

Утилиты, используемые для сокрытия вредоносной активности.

Маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Программы-маскировщики модифицируют ОС на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Антивирусные программы

- **Программы-детекторы** позволяют обнаружить файлы, зараженные одним из нескольких известных вирусов.

- **Программы-доктора**, или **фаги**, «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.

Антивирусные программы

- **Программы-ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.

- **Доктора-ревизоры** – это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Антивирусные программы

- **Программы-фильтры** располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю.

Антивирусные программы

- **Программы-вакцины,** или **иммунизаторы**, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Профилактика заражения компьютерным вирусом

Копирование информации и разграничение доступа:

- Необходимо иметь архивные или эталонные копии используемых пакетов программ и данных и периодически архивировать те файлы, которые вы создавали или изменяли. Перед архивацией файлов целесообразно проверить их на отсутствие вирусов с помощью программы-детектора (например, Dr.Web). Важно, чтобы информация копировалась не слишком редко – тогда потери информации при её случайном уничтожении будут не так велики.
- Целесообразно также скопировать на дискеты сектор с таблицей разделения жесткого диска, разгрузочные сектора всех логических дисков и содержимое CMOS (энергонезависимой памяти компьютера).
- Следует устанавливать защиту от записи на дискетах с файлами, которые не надо изменять. На жестком диске целесообразно создать логический диск, защищенный от записи, и разместить на нём программы и данные, которые не надо изменять.
- Не следует переписывать программное обеспечение с других компьютеров (особенно тех, к которым могут иметь доступ различные безответственные лица), т.к. оно может быть заражено вирусом. Однако следует заметить, что распространяемые производителями «фирменные» дискеты с программами, как правило, не содержат вирусов.

Профилактика заражения компьютерным вирусом

Проверка поступающих извне данных:

- Все принесенные извне дискеты перед использованием следует проверить на наличие вируса с помощью программ- детекторов. Это полезно делать даже в тех случаях, когда нужно использовать на этих дискетах только файлы с данными – чем раньше будет обнаружен вирус, тем лучше.
- Если принесённые программы записаны на дискеты в заархивированном виде, следует извлечь файлы из архива и проверить их сразу после этого.
- Если программы из архивов можно извлечь только программой установки пакета программ, то надо выполнить установку этого пакета и сразу после этого проверить записанные на диск файлы, как это описано выше. Желательно выполнять установку при включенной резидентной программе-фильтре для защиты от вирусов.

Действия при заражении компьютерным вирусом

1. **Не надо торопиться** и принимать опрометчивых решений – непродуманные действия могут привести не только к потере части файлов которые можно было бы и восстановить, но и к повторному заражению компьютера.
2. **Немедленно выключить компьютер**, чтобы вирус не продолжал своих разрушительных действий.
3. **Все действия по обнаружению вида заражения и лечению компьютера следует выполнять только при загрузке компьютера с защищённой от записи «эталонной» дискеты с операционной системой.** При этом следует использовать только программы (исполнимые файлы), хранящиеся на защищённых от записи дискетах. Несоблюдение этого правила может привести к очень тяжелым последствиям, поскольку при загрузке компьютера или запуске программы с зараженного диска в компьютере может быть активирован вирус, а при работающем вирусе лечение компьютера будет бессмысленным, т.к. оно будет сопровождаться дальнейшим заражением дисков и программ.
4. Если используется резидентная программа-фильтр для защиты от вируса, то наличие вируса в какой-либо программе можно обнаружить на самом раннем этапе, когда вирус не успел ещё заразить другие программы и испортить какие-либо файлы. В этом случае следует перезагрузить компьютер с дискеты и удалить зараженную программу, а затем переписать эту программу с эталонной дискеты или восстановить её из архива. Для того чтобы выяснить, не испортил ли вирус каких-то других файлов, следует запустить программу-ревизор для проверки изменений в файлах, желательно с широким списком проверяемых файлов. Чтобы в процессе проверки не продолжать заражение компьютера, следует запускать исполнимый файл программы-ревизора, находящийся на дискете.

История компьютерной вирусологии

1945 год.

Рождение термина. Вице-адмирал ВМФ США Грейс Мюррей Хоппер, руководивший информационным отделом военно-морского штаба, столкнулся с тем, что электронно-счетные машины (прототипы современных компьютеров) начали давать сбои. Причиной стал мотылек, залетевший внутрь одного из реле. Адмирал назвал эту проблему «**жуком**» - bug, используя термин, применявшийся физиками США и Великобритании с конца 19 века (он обозначал любого рода неполадку в электрических устройствах). Адмирал также впервые использовал термин «**избавление от жука**» - **debugging**, который ныне применяется для описания действий, ставящих своей целью устранение неполадок в компьютере.

История компьютерной вирусологии

- **1949 год.** Американский ученый венгерского происхождения **Джон фон Нейман** разработал математическую теорию создания самовоспроизводящихся программ. Это была первая теория создания компьютерных вирусов, вызвавшая весьма ограниченный интерес у научного сообщества.

История компьютерной вирусологии

- **Конец 1960-х годов.** Появление первых вирусов. В ряде случаев это были ошибки в программах, приводивших к тому, что программы копировали сами себя, засоряя жесткий диск компьютеров, что снижало их продуктивность, однако считается, что в большинстве случаев вирусы сознательно создавались для разрушения. Вероятно, первой жертвой настоящего вируса, написанного программистом для развлечения, стал компьютер Univax 1108. Вирус назывался Pervading Animal и заразил только один компьютер - на котором и был создан.

История компьютерной вирусологии

- **1975 год.** Через Telenet (коммерческая компьютерная сеть) распространяется первый в истории сетевой вирус The Creeper. Для противодействия вирусу впервые в истории написана особая антивирусная программа The Reeper.
- **1979 год.** Инженеры из исследовательского центра компании Xerox создали первого компьютерного "червя"\worm.
- **1981 год.** Вирус Elk Cloner поражает компьютеры Apple. Вирус распространялся через "пиратские" компьютерные игры.

История компьютерной вирусологии

- **1983 год.** Ученый Фред Кохен из Университета Северной Каролины *вводит термин "компьютерный вирус".*
- **1986 год.** Впервые создан вирус для IBM PC - The Brain. Два брата-программиста из Пакистана *написали программу, которая должна была "наказать" местных "пиратов",* ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Успех вируса был обеспечен тем, что компьютерное сообщество было абсолютно не готово к подобному развитию событий.

История компьютерной вирусологии

- **1988 год.** 23-летний американский программист создал "червя", поразившего ARPANET. Впервые заражение было массовым - пострадали 6 тыс. компьютеров. Впервые суд осудил автора компьютерного вируса: он был приговорен к $10 тыс. штрафа и трем годам испытательного срока. После этого инцидента о проблеме компьютерных вирусов стали писать серьезные некомпьютерные издания.

История компьютерной вирусологии

- **1989 год.** ARPANET официально переименован в Интернет. Создано первое антивирусное программное обеспечение для IBM PC. В том же году появился первый "троянский конь" AIDS. Вирус делал недоступными всю информацию на жестком диске и высвечивал на экране лишь одну надпись: "Пришлите чек на $189 на такой-то адрес". Автор программы был арестован в момент обналичивания денег и осужден за вымогательство.

История компьютерной вирусологии

- **1993 год.** Вирус SatanBug поражает сотни компьютеров в столице США, Вашингтоне. Страдают даже компьютеры Белого Дома. ФБР арестовала автора - им оказался 12-летний подросток.
- **1999 год.** Впервые компьютерный вирус вызвал эпидемию в мировом масштабе. Вирус Melissa поразил десятки тысяч компьютеров и нанес ущерб в $80 млн. После этого инцидента в мире начался обвальный спрос на антивирусные программы.
- **2000 год.** Рекорд Melissa побил вирус I Love You!, поразивший миллионы компьютеров в течение нескольких часов.

История компьютерной вирусологии

- **2003 год.** Рекорды быстроты распространения побил "червь" Slammer, заразивший 75. тыс. компьютеров в течение 10 минут. Вирус поразил компьютеры Госдепартамента США\State Department, где повредил базу данных. Консульства США по всему миру вынуждены были на 9 часов прервать процесс выдачи виз.

История компьютерной вирусологии

- В **2004 году** было зафиксировано 46 крупных вирусных эпидемий. Это число превосходит результаты прошлого года (35 эпидемий), причем многие из них были вызваны одновременным (в течение одних суток) появлением нескольких вариантов одного и того же вируса. Среди разновидностей вредоносных программ пальму первенства уже давно и прочно держат черви - как сетевые, так и почтовые, что неудивительно, ведь электронная почта - самая популярная среда распространения компьютерной инфекции и скорость распространения в такой среде самая высокая.

История компьютерной вирусологии

- **2005 год** ознаменован появлением несколькими почтовыми червями (Mytob.LX, Sober-Z) и троянскими программами (Ryknos.G, Downloader.GPH).
- Червь Mytob.LX рассылается в электронных сообщениях, сообщающих пользователям, что для продления пользования услугами определенной компании безопасности они должны посетить некую веб-страницу (якобы для подтверждения своего электронного адреса). Однако если пользователь посещает этот сайт, на его компьютер скачивается файл Confirmation_Sheet.pif, который является копией червя Mytob.LX.
- После установки, червь ищет на компьютере электронные адреса (во временных файлах интернета, адресной книге и файлах с определенными расширениями), содержащие определенные текстовые строки. Затем он отсылает себя на найденные адреса.

Вирусные тенденции на 2010 год

- Антивируса самого по себе будет недостаточно
- Социальная инженерия – главный вектор развития вредоносных атак
- Жульничество связанное с продажами антивирусов
- Целью атак станут сторонние приложения в социальных сетях
- Больше вирусов для Windows 7
- Скрытие зараженных сайтов за прокси-серверами
- Сокращение ссылок
- Количество вирусов для Mac и смартфонов будет увеличиваться
- Больше спама
- Активность спамеров будет колебаться
- Увеличение количества специализированного вредоносного ПО
- Технология CAPTCHA будет улучшаться
- Спам в сетях обмена сообщениями будет расти