Защита информации в компьютерных сетях.

Электронная подпись.

Информационная безопасность

Защита информации – это деятельность по предотвращению:

- утечки защищаемой информации;
- несанкционированных или непреднамеренных воздействий на защищаемую информацию.

Понятие **компьютерной (информационной) безопасности** включает следующие аспекты: конфиденциальность информации, аутентификацию и целостность, т.е. сохранность и защиту информации от несанкционированных изменений, сохранение тайны переписки в электронной связи, а также надежность работы компьютера.

Под **угрозой информационной безопасности** понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов.

Информационные угрозы

Методы защиты информации

- **Методы защиты от преднамеренных угроз:**

1. Ограничение доступа к информации – использование паролей, биометрических систем идентификации.

2. Шифрование (**криптография**) информации.

3. Контроль доступа к аппаратуре – вся аппаратура закрыта, а в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры.

4. Законодательные меры.

Средства защиты информации

- **Законодательные средства защиты информации:**

1. Международные договоры РФ;

2. Конституция РФ;

3. Законы федерального уровня (включая федеральные конституционные законы, кодексы);

4. Указы Президента РФ;

5. Постановления правительства РФ;

6. Нормативные правовые акты федеральных министерств и ведомств;

7. Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Средства защиты информации

Законодательные средства защиты информации:

Законодательные средства защиты определяются законодательными актами страны. Эти акты регламентируют правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Наиболее общим законом Российской Федерации является ***Конституция***. Главы 41, 42 и статьи 23, 29 Конституции затрагивают вопросы информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных разговоров, почтовых и иных сообщений.

Статья 29 Конституции гарантирует право свободно искать, получать, передавать и распространять информацию любым законным способом.

Главы 41 и 42 гарантируют право на знание фактов, создающих угрозу жизни и здоровью людей, право на знание достоверной информации о состоянии окружающей среды.

Уголовный кодекс (УК) Российской Федерации предусматривает наказания за преступления, связанные с нарушением конфиденциальности информации. ***Глава 28 УК*** (статьи 272-274) посвящены преступлениям, связанным с неправомерным доступом к компьютерной информации, созданием и распространением вредоносных программ.

Средства защиты информации

❑ Законодательные средства защиты информации:

Интересы государства в плане обеспечения конфиденциальности информации представлены в Законе «О государственной тайне».

Государственная тайна – это защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб Российской Федерации.

Для защиты сведений, составляющих государственную тайну, Закон определяет средства защиты: технические (аппаратные), криптографические, программные и другие средства. Система органов обеспечения информационной безопасности РФ включает министерство обороны и министерство юстиции.

Статья 273 УК РФ Создание, использование и распространение вредоносных программ для ЭВМ. ***До 4-х лет лишения свободы***

Статья 274 УК РФ Незаконное изменение программ, а также их копирование с корыстными целями. ***Штраф до 500 тыс. руб.***

Статья 275 УК РФ Государственная измена (т.е. шпионаж, выдача гос.тайны). ***Лишение свободы от 12 до 20 лет***

Средства защиты информации

- **Организационные средства защиты информации:**

Гарантом информационной безопасности является

Президент РФ, при котором существует служба ФСТЭК (Федеральная служба по техническому и экспортному контролю).

1. Средства контроля доступа в помещения.

2. Средства предотвращения взлома компьютеров и краж оборудования.

Средства защиты информации

- **Технические и программные средства защиты информации:**

  1. Системы мониторинга сетей.

  2. Антивирусные средства.
  3. Межсетевые экраны.
  4. Криптографические средства.
  5. Системы резервного копирования.
  6. Системы бесперебойного питания.
  7. Системы аутентификации (подтверждение подлинности **идентификаторов** субъекта).

Компьютерные вирусы

Компьютерный вирус – это программа, предназначенная для несанкционированного доступа к данным с целью их изменения или уничтожения.

Классификация вирусов

- по среде обитания:

  - сетевые (распространяются по сетям);

  - файловые (внедряются в исполняемые файлы; пр.: .exe, .com);

  - загрузочные (внедряются в главную загрузочную область диска)

Компьютерные вирусы

- по способу заражения:

  - резидентные (после исполнения зараженной программы остаются в оперативной памяти и продолжают деструктивные действия);

  - нерезидентные (не заражают оперативную память и проявляют свою активность лишь однократно – при запуске зараженной программы).

- по степени воздействия:

  - неопасные (например, выводят на экран сообщения);

  - опасные (уничтожают часть файлов на диске);

  - очень опасные (самостоятельно форматируют жесткий диск).

Компьютерные вирусы

- по алгоритму функционирования:

  - невидимки (**стелс**) – вирусы, способные скрываться при попытках их обнаружения;

  - «троянские кони» (**«логические бомбы»**) - вирусы, маскирующиеся под полезные программы, нарушающие работу системы или собирающие информацию о ней;

  - мутанты (**призраки**) - вирусы, изменяющие свой программный код;

  - репликаторы (**черви**) – вирусы, распространяемые в сети, могут размножаться без внедрения в другие программы;

  - макровирусы - заражают текстовые файлы и файлы электронных таблиц.

Антивирусные программы

Антивирус – программное средство, предназначенное для борьбы с вирусами.

- Программы-детекторы (**сканеры**)

  Назначение: обнаружение конкретных вирусов. Основаны на сравнении специфической последовательности байтов (сигнатур), содержащихся в теле вируса, и байтов проверяемых программ. Эти программы нужно регулярно обновлять, т.к. они быстро устаревают и не могут выявлять новые виды вирусов.

- Программы-доктора (**фаги**)

  Это программы, которые способны не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных программ и восстановить их работоспособность (если возможно).

Антивирусные программы

- Программы-ревизоры

  Назначение: запоминают исходное состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора.

- Программы-фильтры (**сторожа**)

  Это резидентная программа, постоянно находящаяся в памяти компьютера, контролирующая операции компьютера, связанные с изменением информации на дисках, и предупреждающая пользователя о них.

- Программы-иммунизаторы (**вакцины**)

  Антивирусные программы, ведущие себя подобно вирусам, но не наносящие вреда. Вакцины предохраняют файлы от изменений и способны не только обнаружить факт заражения, но и «вылечить» пораженные вирусами файлы. -- устарели

Криптография

Криптология – это наука о тайных записях.

Криптология включает:

- ***Криптографию*** (наука о составлении шифров);
- ***Криптоанализ*** (наука о доказательстве сложностей, о попытках взлома шифров).

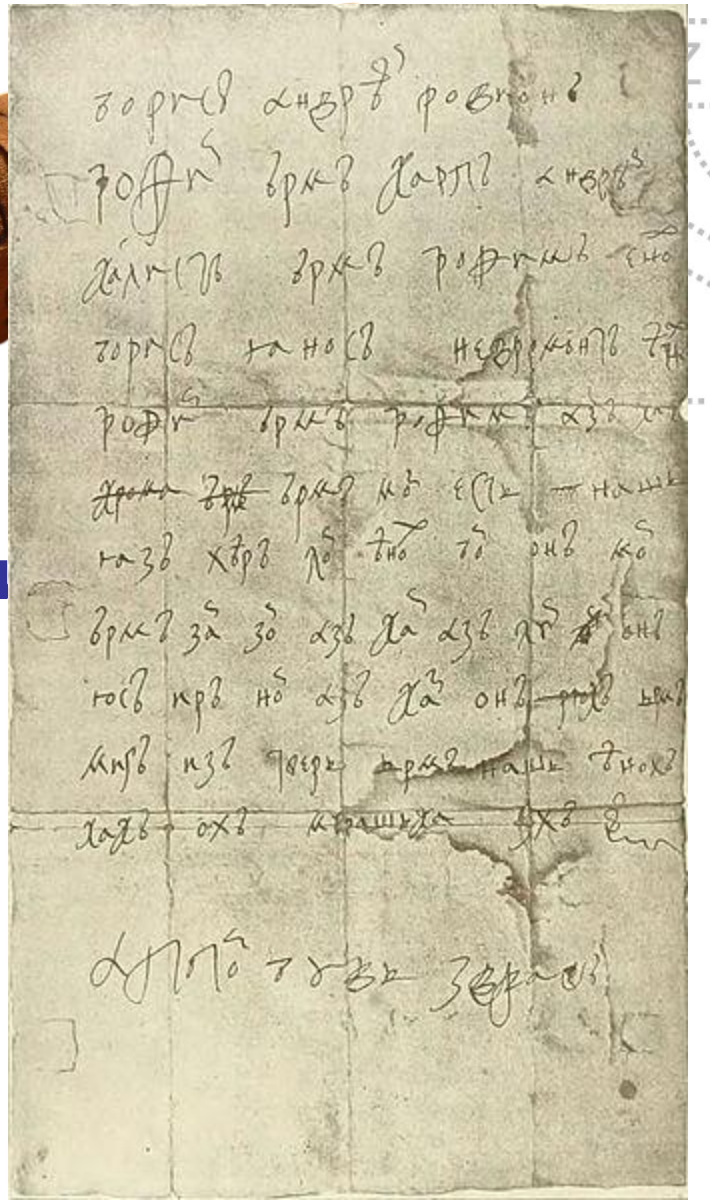
Криптостойкость – минимальный объем информации, который можно вскрыть в результате анализа.

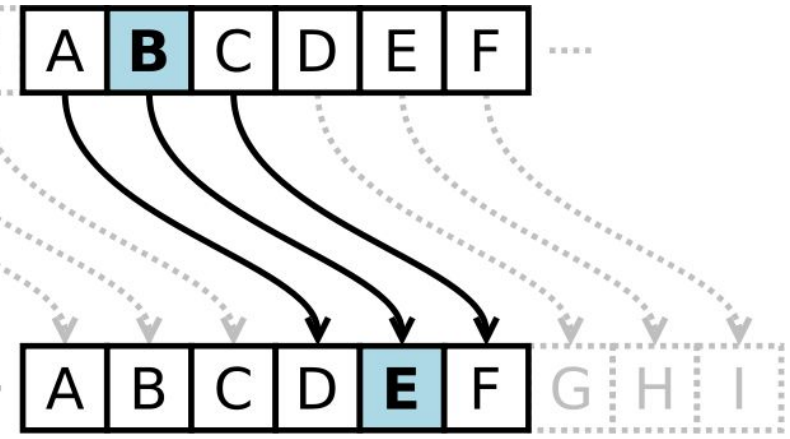
Достаточность защиты - затраты на вскрытие информации должны превышать ее ценность.

Криптографический ключ – секретная последовательность символов или битов.

История криптографии

Ски





шифр Цезаря

Письмо царя Алексея Михайловича, писанное тайнописью (тарабарщиной)

История криптографии

Эра

«черных кабинетов»

Практическое применение криптографии

Военная немецкая шифровальная машина «Энигма»

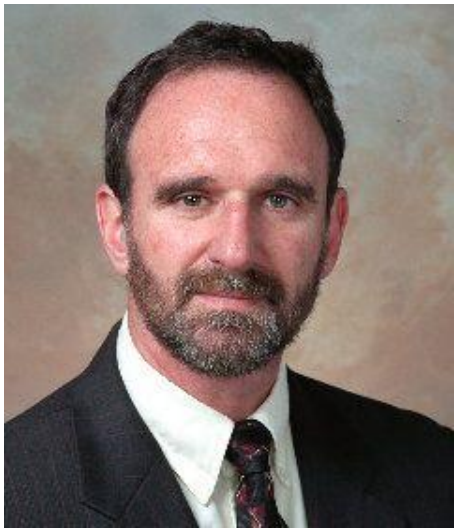
Математическая криптография

Симметричные криптографические шифры - подстановочные.

Асимметричные криптографические системы - основаны на использовании двух ключей: **открытого** (public) и **закрытого** (private). Открытый и закрытый ключи создаются одновременно и являются половинками одного ключа.

У. Диффи

Работа **У. Диффи** и **М. Хеллмана** **«Новые направления в криптографии»** (опубликована в 1976 г.) открыла новую область в криптографии, известную как **криптография с открытым ключом**.



М. Хеллман

Методы шифрования

❖ Симметричные криптосистемы:

- моноалфавитные подстановки;

- многоалфавитные подстановки;
- перестановки;
- гаммирование;
- блочное шифрование;
- DES (Data Encrypting Standard);
- FEAL (Fast data Encipherment ALgorithm);
- IDEA (International Data Encryption Algorithm).

Методы шифрования

❖ Асимметричные криптосистемы:

- криптосистема RSA;

(названа по имени авторов — R. Rivest, A. Shamir и L. Adleman)

Интересно!

Авторы пообещали премию в сто долларов тому, кто первым расшифрует RSA-шифрованную фразу:

«96861375462206147714092225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4»

Единственное, что требовалось для этого, — разложить на два сомножителя 129-значное число, приведенное в той же статье.

Расшифровано только через **17 лет**. Для того чтобы расшифровать фразу **The magic words are squeamish ossifrage**, команде из **600** человек потребовалось **220** дней работы и **1600** компьютеров, связанных через интернет.

Методы шифрования

Асимметричные криптосистемы:

- криптосистема Эль-Гамаля (*El Gamal*);
- криптосистема DSS (Digital Signature Standard);
- российский стандарт цифровой подписи;
- электронная подпись.

Электронная подпись

Электронная цифровая подпись (ЭЦП) используется для аутентификации данных (установления подлинности данных и источника их получения).

Назначение ЭЦП – сделать невозможным:

- отказ отправителя от посланного им сообщения;
- изменение отправленного сообщения получателем;
- изменение сообщения (с целью искажения) или повтор третьим лицом.

ЭЦП служит той же цели, что и собственноручная подпись на бумажном носителе. Однако ручную подпись очень легко подделать. ЭЦП же подделать **практически невозможно**, кроме того, она делает еще и то, чего «бумажная» подпись не умеет, — **подтверждает целостность информации** и **личность подписавшего**.

Электронная подпись применяется сегодня гораздо чаще, чем чистое шифрование.

Криптография сегодня

Место криптографии сегодня — не только в офисе или банке, в государственном учреждении или войсковой части. Ее место — везде, где используются электронные средства коммуникаций.

В самих алгоритмах стали использовать более сложные математические конструкции. Принципы выбора алгоритмов постепенно усложняются.

Предлагаются всё новые механизмы, в том числе организационные и законодательные.

Развиваются принципиально новые направления. На стыке квантовой физики и математики развиваются квантовые вычисления развиваются квантовые вычисления и квантовая криптография. Хотя квантовые компьютеры лишь дело будущего, уже сейчас предложены алгоритмы для взлома существующих «надежных» систем.

Используя квантовые эффекты, возможно построить и принципиально новые способы надежной передачи информации. В современном мире криптография находит множество различных применений. Для передачи информации, она используется в сотовой связиВ современном мире криптография находит множество различных применений. Для передачи информации, она используется в сотовой связи, платном цифровом телевидении при подключении к Wi-FiВ современном мире криптография находит

Стеганография

Стеганография (**«стеганос»** - тайный, **«графо»** - пишу; дословно – **«тайнопись»**) — это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи.

Этот термин ввел в **1499 г. Иоганн Тритемий** в своем трактате «Стеганография», зашифрованным под магическую книгу.

В отличие от **криптографии**, которая скрывает содержимое секретного сообщения, **стеганография** скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя ее.

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

История и классификация стеганографии

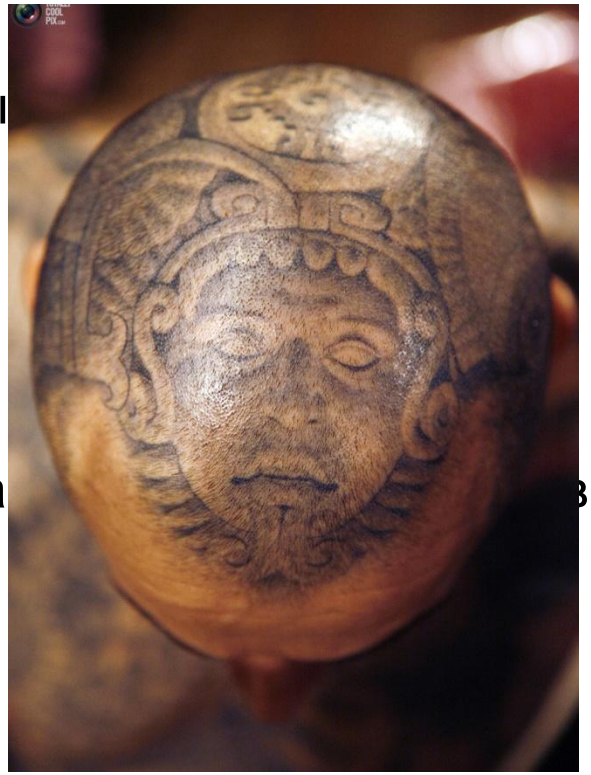
440 г. до н.э. - первая запись об использовании стеганографии встречается в трактате Геродота «История».

В конце 90-х годов выделилось несколько **направлений стеганографии**:

- **Классическая стеганография**
  - использование симпатических (невидимы
  - микроточки (Вторая мировая война);
  - «жаргонные шифры»

- **Компьютерная стеганография**
  - основана на особенностях компьютерной
  - скрытие данных в неиспользуемых обла в,
  подмена символов в названиях файлов

- **Цифровая стеганография**



Цифровая стеганография

Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Данные объекты являются мультимедиа-объектами (**изображения, видео, аудио, текстуры 3D-объектов**) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, **не приводит** к заметным **изменениям** этих объектов.

Изображение дерева со скрытым с помощью цифровой стеганографии в нем другим изображением.

Изображение спрятано с помощью удаления всех, кроме двух младших **битов** с каждого цветового компонента и последующей нормализации.

Изображение кота, извлеченное из изображения дерева.

Цифровая стеганография

Стегопрограммы: одна из самых распространенных утилит, умеющая прятать информацию в графических (форматы gif, bmp) и звуковых (формат wav) файлах является программа **S-Tools**. Программа позволяет не только скрыть сообщение, но и зашифровать его с помощью стойкого криптоалгоритма, что обеспечивает как высокую скрытность факта передачи сообщения, так и стойкость секретного сообщения.

В **графический файл** внедрен целый **куплет** одной песни вместе с припевом (формат MP3).

Визуально невозможно определить, что **рисунок** содержит в себе еще какую-то информацию.

Применение стеганографии

- **в современных принтерах**

  При печати на каждую страницу добавляются маленькие точки, содержащие информацию о времени и дате печати, а также серийный номер принтера.

- **предполагаемое использование террористами**

- **предполагаемое использование спецслужбами**

  В 2010 г. Федеральное бюро расследований выяснило, что Служба внешней разведки РФ использовала специальное программное обеспечение для скрытия информации в изображениях. Данный способ использовался для связи с агентами без дипломатического прикрытия за рубежом.