Методы и средства защиты компьютерной информации

Лекция 1.

Введение в дисциплину

Основные разделы

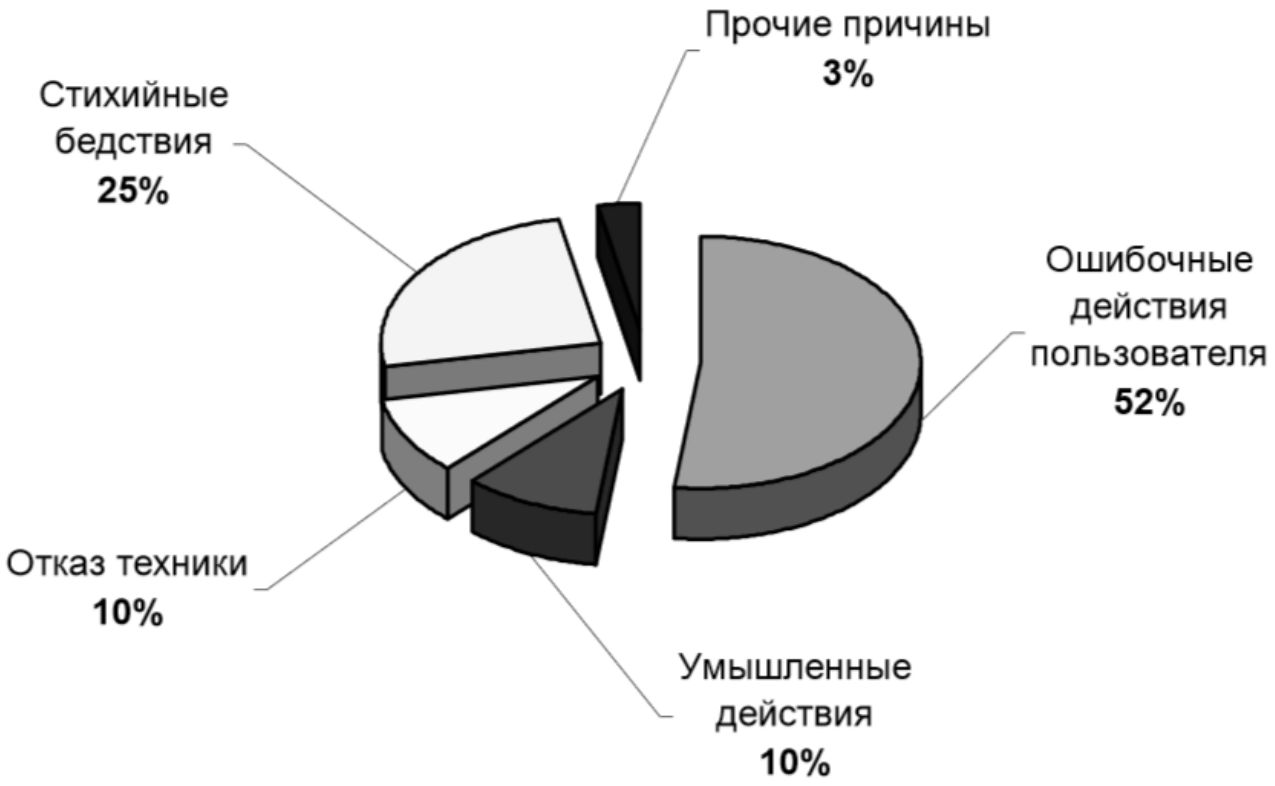
История криптографии

Основные понятия

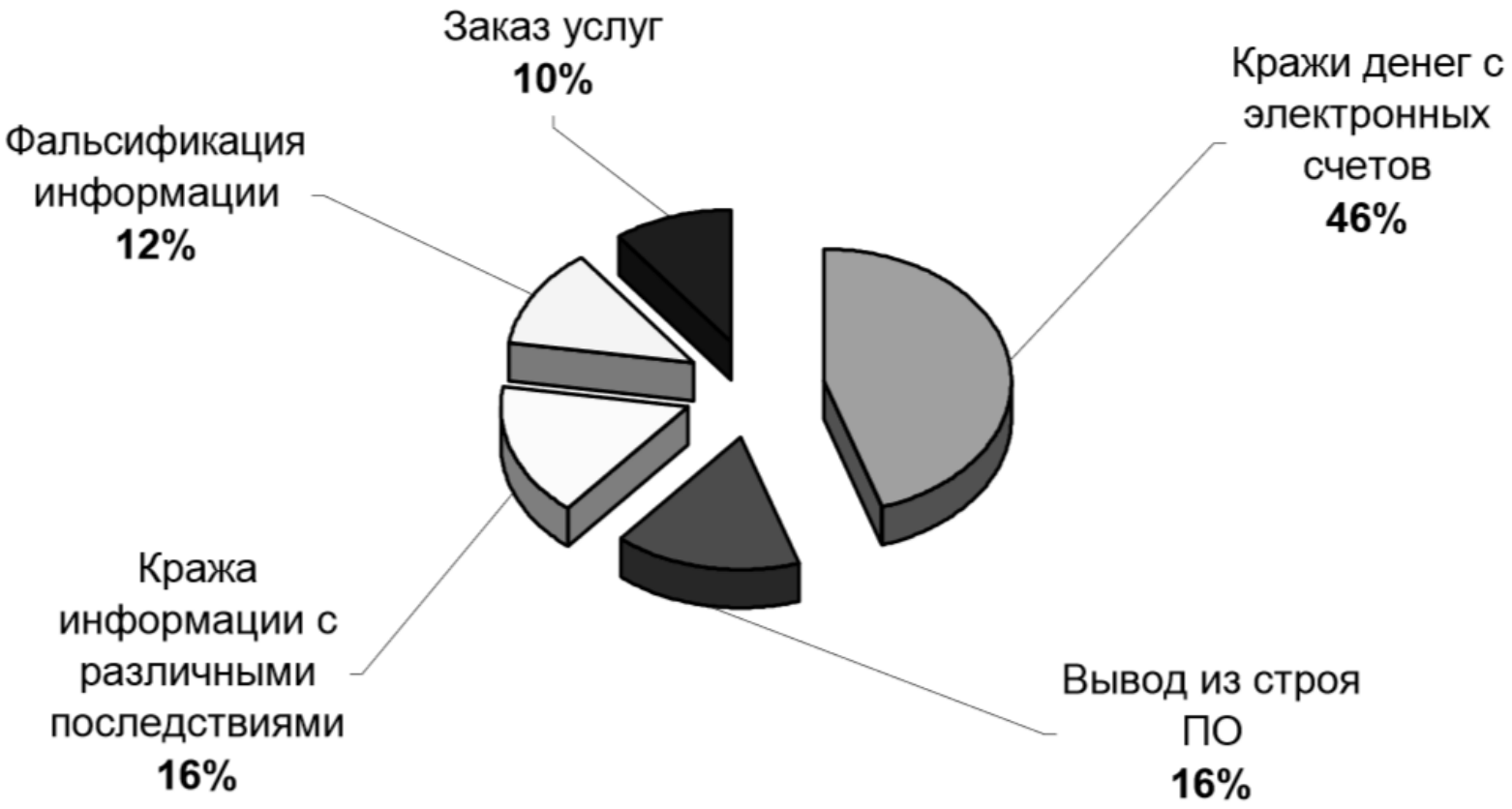
- **Защита информации** – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах

- **Информационная угроза** – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации

Причины повреждения электронной информации



Действия злоумышленников



Принципы проектирования систем защиты информации

- Простота механизма защиты
- В механизме защиты при работе в нормальных условиях доступ должен разрешаться, а не запрещаться
- Все возможные каналы утечки информации должны быть перекрыты, то есть предполагается проверка полномочий любого обращения к любому объекту
- Сам механизм защиты можно не засекречивать, засекречивается только какая-то его часть, например списки паролей
- Установление для любого пользователя только тех полномочий, которые ему необходимы, то есть круг полномочий должен быть минимальным
- Обособленность или сведение к минимуму числа общих для нескольких пользователей параметров и характеристик защиты.
- Психологическая привлекательность и простота использования системы

Основные разделы дисциплины

- Криптографическая защита информации
  - Симметричные системы
  - Ассиметричные системы
  - Электронная цифровая подпись
- Компьютерные вирусы и антивирусология
  - Определение понятия «Компьютерный вирус»
  - Классификация вирусов
  - Антивирусное программное обеспечение
- Системная защита информации
  - Защита от копирования
  - Защита информации в информационных системах
- Основы сетевой безопасности
  - Безопасность в компьютерных сетях
  - Протоколы защиты информации

Список литературы

- Е. Баранова, А. Бабаш "Информационная безопасность и защита информации" 3-е изд. (2016) / Учебное пособие
- В. Бондарев "Введение в информационную безопасность автоматизированных систем" (2016)
- С. Нестеров "Основы информационной безопасности" (2016)
- А. Бирюков "Информационная безопасность: защита и нападение" 2-е изд. (2017)
- Мартынов А.И. Методы и задачи криптографической защиты информации : учебное пособие для студентов специальности «Вычислительные машины, комплексы, системы и сети»/ А. И. Мартынов. – Ульяновск : УлГТУ, 2007. – 92 с.

Шифр Скитала (V век до Н.Э.)

Квадрат Полибия (II век до НЭ)

РИМ > 352331

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ж	З	И	Й	К	Л
3	М	Н	О	П	Р	С
4	Т	У	Ф	Х	Ц	Ч
5	Ш	Щ	Ъ	Ы	Ь	Э
6	Ю	Я	.	,	-	

34

Ключ:

- Язык сообщения
- Порядок следования букв
- Размер квадрата

Шифр Цезаря (I век до НЭ)

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ш Щ Ы Ь Ъ Э Ю Я

Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ш Щ Ы Ь Ъ Э Ю Я А Б В

РИМ > УЛП

Ключ:

- Язык сообщения
- Порядок следования букв
- Величина сдвига строки алфавита

Магический квадрат (Средневековье)

Шифруемое сообщение - «*ПРИЕЗЖАЮ СЕГОДНЯ*»

16У	**3**И	**2**Р	**13**Д
5З	**10**Е	**11**Г	**8**Ю
9С	**6**Ж	**7**А	**12**О
4Е	**15**Я	**14**Н	**1**П

Зашифрованное сообщение - «*УИРДЗЕГЮСЖАОЕЯНП*»

Книжный шифр

n – номер страницы

m – номер строки

t – номер буквы

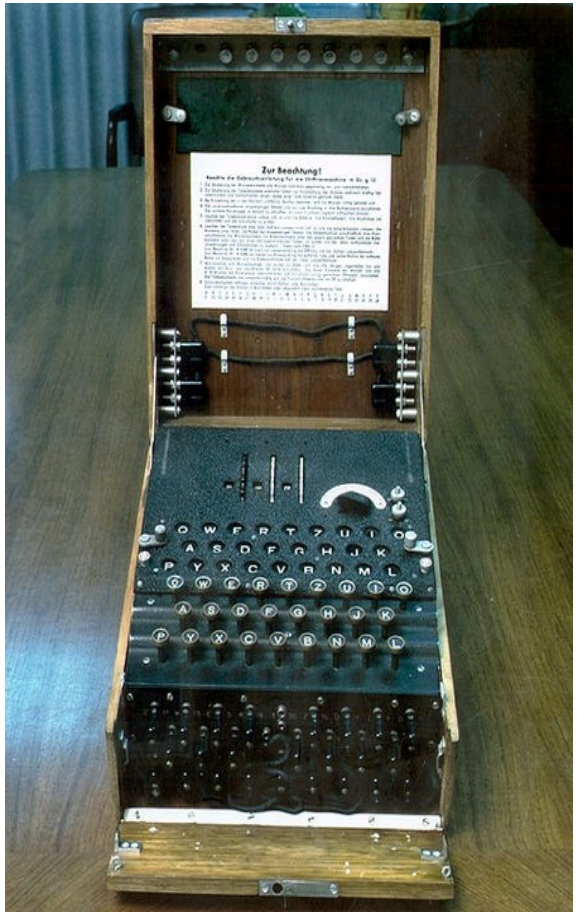
Шифратор Томаса Джефферсона

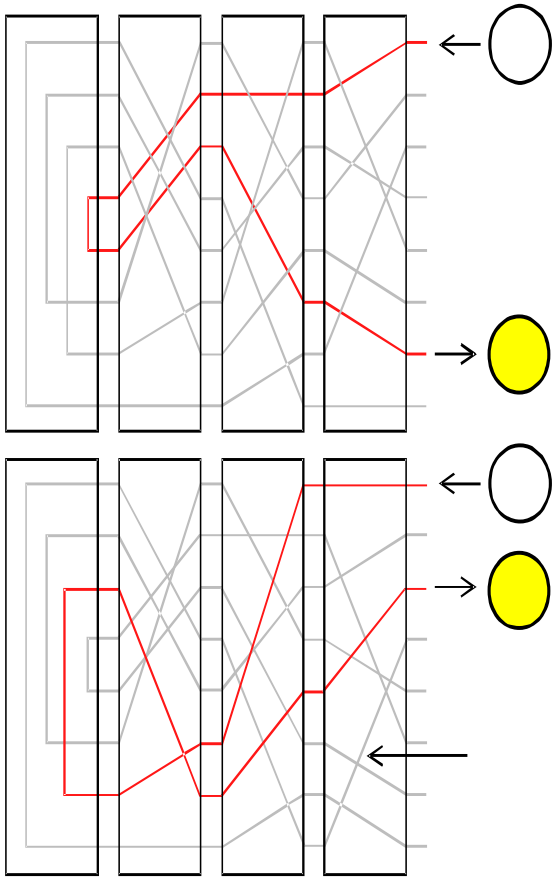
Ключ:

- порядок расположения букв на каждом диске
- порядок расположения этих дисков на общей оси

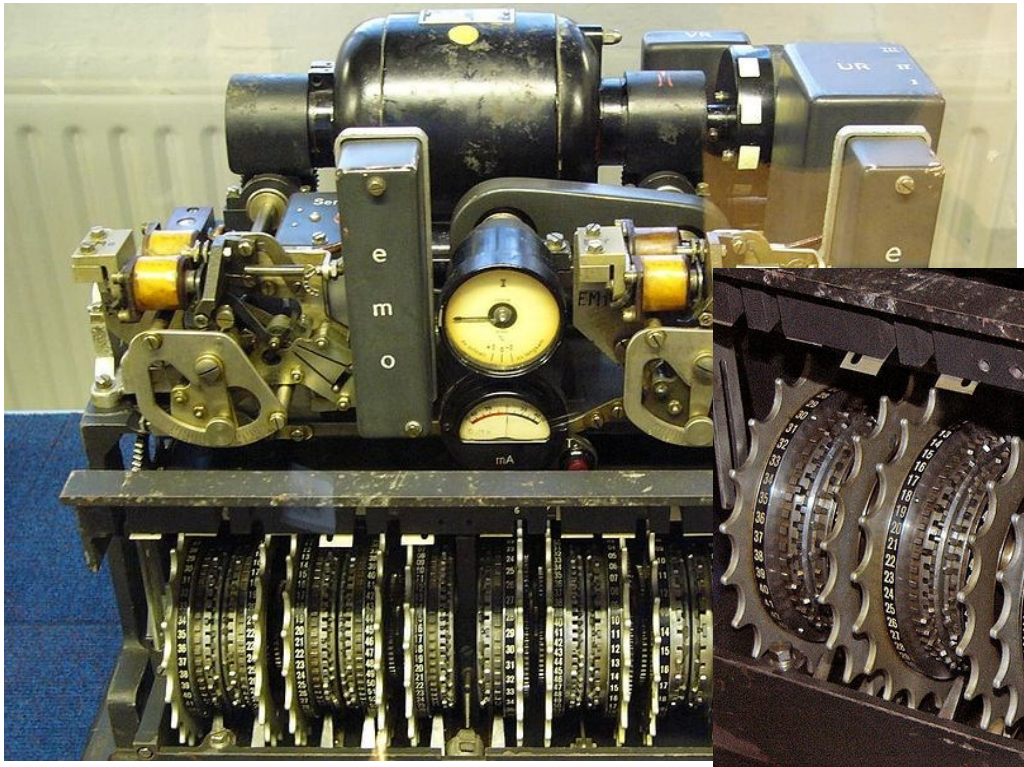
Это изобретение стало предвестником появления так называемых дисковых шифраторов, нашедших широкое распространение в XX веке.

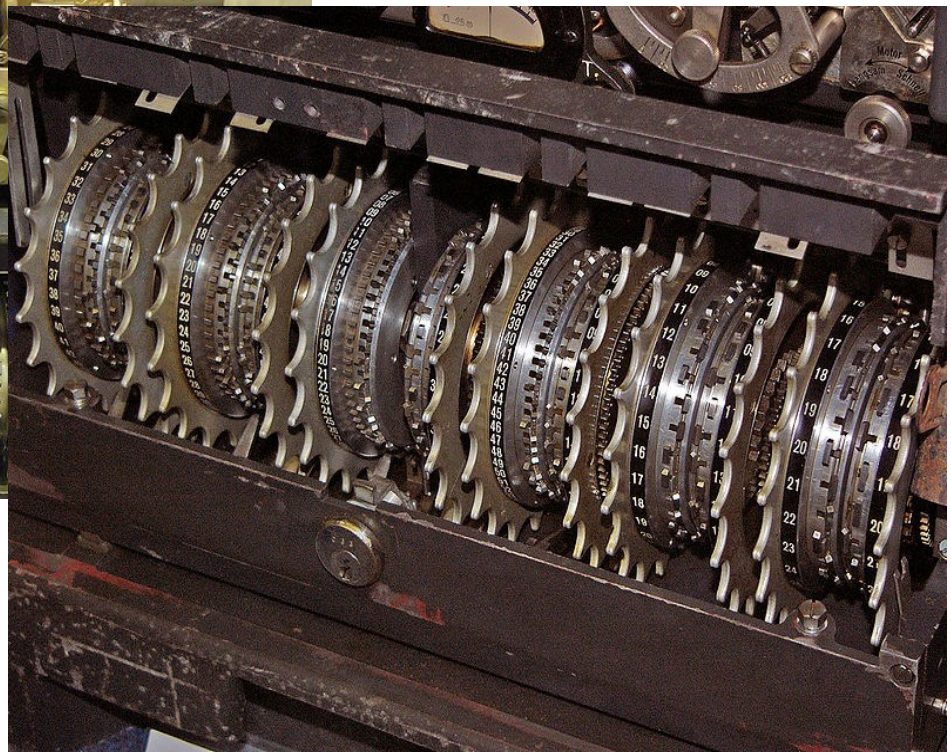
Шифровальная машина «Энигма» (Германия, 1920 г)





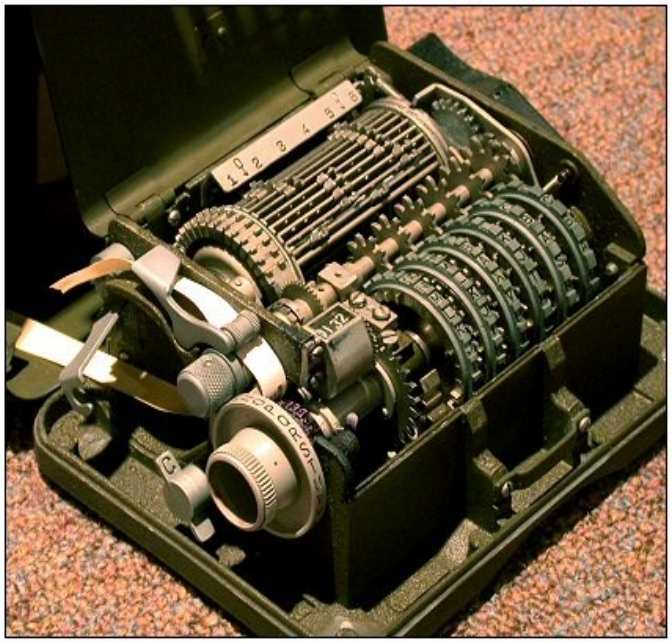
Шифровальная машина Лоренца (Германия, 1930-1942)





Шифровальная машина «М-209» (США, 1930 г.)

HAGELIN M-209 CIPHER MACHINE (GVG / PD)



Огюст Керкгоффс

В 80-х годах XIX века издал книгу *"Военная криптография"* объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии.

Керкгоффс сформулировал общие требования к шифрам:

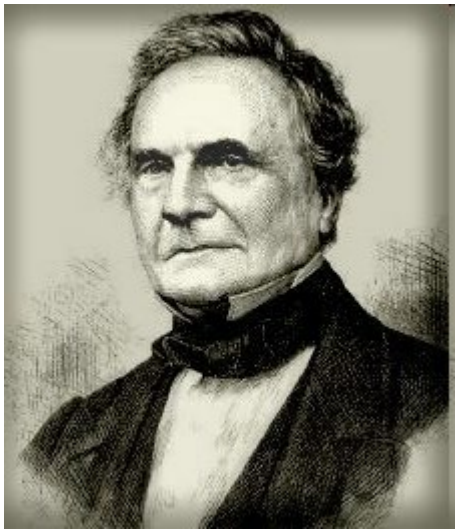
- простота практического использования
- надежность
- операции шифрования и расшифрования не должны требовать значительных затрат времени

Чарльз Бэббидж

Бэббидж одним из первых математиков начал применять алгебру в области криптографии.

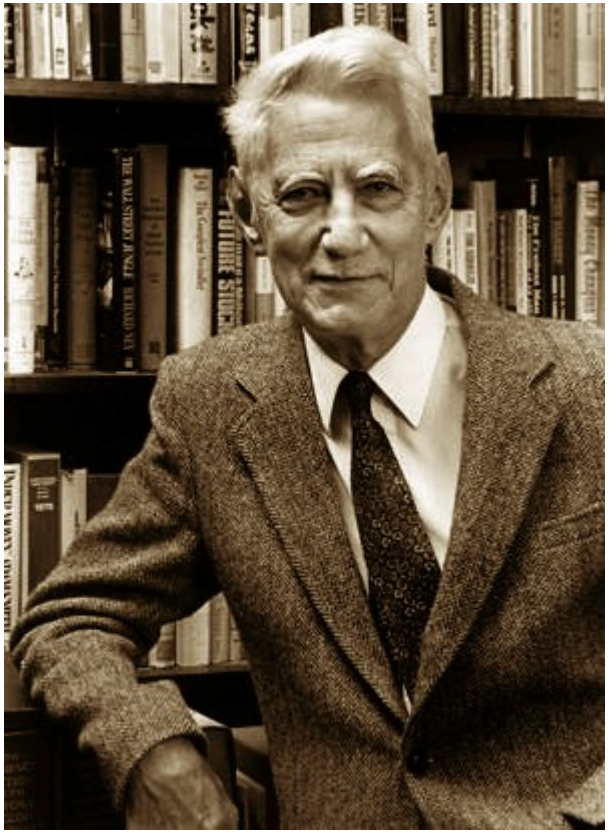
Алгебраическое моделирование шифров и их алгебраический анализ помогли ему проникнуть во внутренний смысл шифров.

Однако содержание его математических замыслов в области их криптографического применения, к сожалению, в значительной степени утрачено.



Клод Шеннон

Работа Шеннона «Теория связи в секретных системах» (1945) с грифом «секретно», которую рассекретили и опубликовали только лишь в 1949 году, послужила началом обширных исследований в теории кодирования и передачи информации, и, по всеобщему мнению, придала криптографии статус науки. Именно Клод Шеннон впервые начал изучать криптографию, применяя научный подход.



XX век

В 70-х годах XX века в США был принят первый гражданский стандарт на криптографическую защиту информации (DES, Data Encryption Standard)

В 1976 г. Уитфрид Диффи (Diffie) и Мартин Хеллман (Hellman) предложили революционную концепцию криптографии с открытым ключом

Изобретение Диффи и Хеллмана открыло новую страницу в современной криптографии – Ассиметричную криптографию с открытыми ключами

Что такое криптография?

Криптография — наука о защите информации от прочтения ее посторонними лицами. Защита достигается путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной информации

Криптография позволяет хранить важную информацию или передавать её по ненадёжным каналам связи (таким как Интернет) так, что она не может быть прочитана никем, кроме легитимного получателя.

Основные понятия криптографии

- **Шифр** – это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования
- **Ключ** – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающий выбор одного варианта из совокупности возможных для данного алгоритма
- **Алгоритм** (функция, уравнение) шифрования – соотношение, описывающее процесс образования зашифрованных данных из открытых
- **Криптостойкость** – это характеристика шифра, определяющая ее стойкость к дешифрованию

Классификация алгоритмов