**ОСНОВНЫЕ ПОНЯТИЯ:**

**Простейшая ИС:**  
ИсС ----- канал (среда) передачи ----- ПС

*Инф. параметр (ИП)* – физ. величина, изменение которой обесп. отображение сообщение

**Сигналы:**  
\* непрерывные (аналог) : ИП м. приним любые мгнов.значения в опр. пределах  
\* дискретные : конечное число значений ИП

*Дискр. сообщ* сост из посл-сти диск.знаков (часто 0 и 1)

***Кодирование*** – построение сигнала по опр. правилам, обесп. соотв между сообщением и сигналом  
Кодирование – преобразование сообщения в сигнал  
Кодирование – предст. исх. символов в другом алфамите с меньшим числом знаков  
 -->повыш надежность + преобр. сигналы удобно перед по каналу

**ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПАРАМЕТРЫ ДВОИЧ СИСТЕМ:**

***Алфавит А*** – общее число символов {ai}, исп. для генерации или передачи сообщений  
N – мощность

Мин. число эл-тов Nmin = 2  
**A = {0,1}** – двоичный код  
один дискр знак – элементарное сообщ  
посл-сть знаков – сообщение

Набор эл-тов алфавита заранее известен ПС. ИсС в каждый дискр. момент выдает 1 символ алфавита. ПС заранее не известное, какой это эл-т

|  |
| --- |
| Е p(ai) = 1 |

- вероятность выбора каждого эл-та алфавита  
Эти вероятности нах. в рез анализа частотных св-в символов алф (если на входе принять док)

***Двоич. канал передачи*** строится на основе двоич алфавита A={0,1}.   
Канал в кот. p(0) = p(1), наз. ***двоич. симм каналом (ДСК)***

***p(1|0)*** *– “передан 0, принята 1”*  
***q*** – вер правильной передачи бита  
***p*** – вер передачи бита с ошибкой (p+q=1)

***Энтропия*** – инф. хар-ка алфавита, показ. какое кол-во инфы приходится в среднем на 1 символ алфавита (Шеннон):

|  |
| --- |
| Hs(A) = |

частный случай - ***Энтропия*** Хартли (все P(ai) одинаковы и постоянны):

|  |
| --- |
| Hch(A) = log2 N |

Сообщ Xk, сост. из k символов, характ опр. ***кол-вом инфы***:

|  |
| --- |
| I (Xk) = H(A) \* k |

Энтропия ***бинарного алфавита***:

|  |
| --- |
| H(A2) = –p(0) \* log2 (p(0)) – p(1) \* log2 (p(1)) |

***Моноалфавит*** – алфавит, сост. из 1 символа  
***Усл. энтропия*** – потеря инфы на 1 символ

***Энтропия*** – непредсказуемость появления символа  
***Кол-во инфы*** – сколько инфы сод. с нашем сообщ  
***Инфа*** – новые для получателя д-е (Шеннон)

Криптология = криптография (защита) + криптоанализ (взлом инфы)