ОБЩАЯ ТЕОРИЯ СВЯЗИ

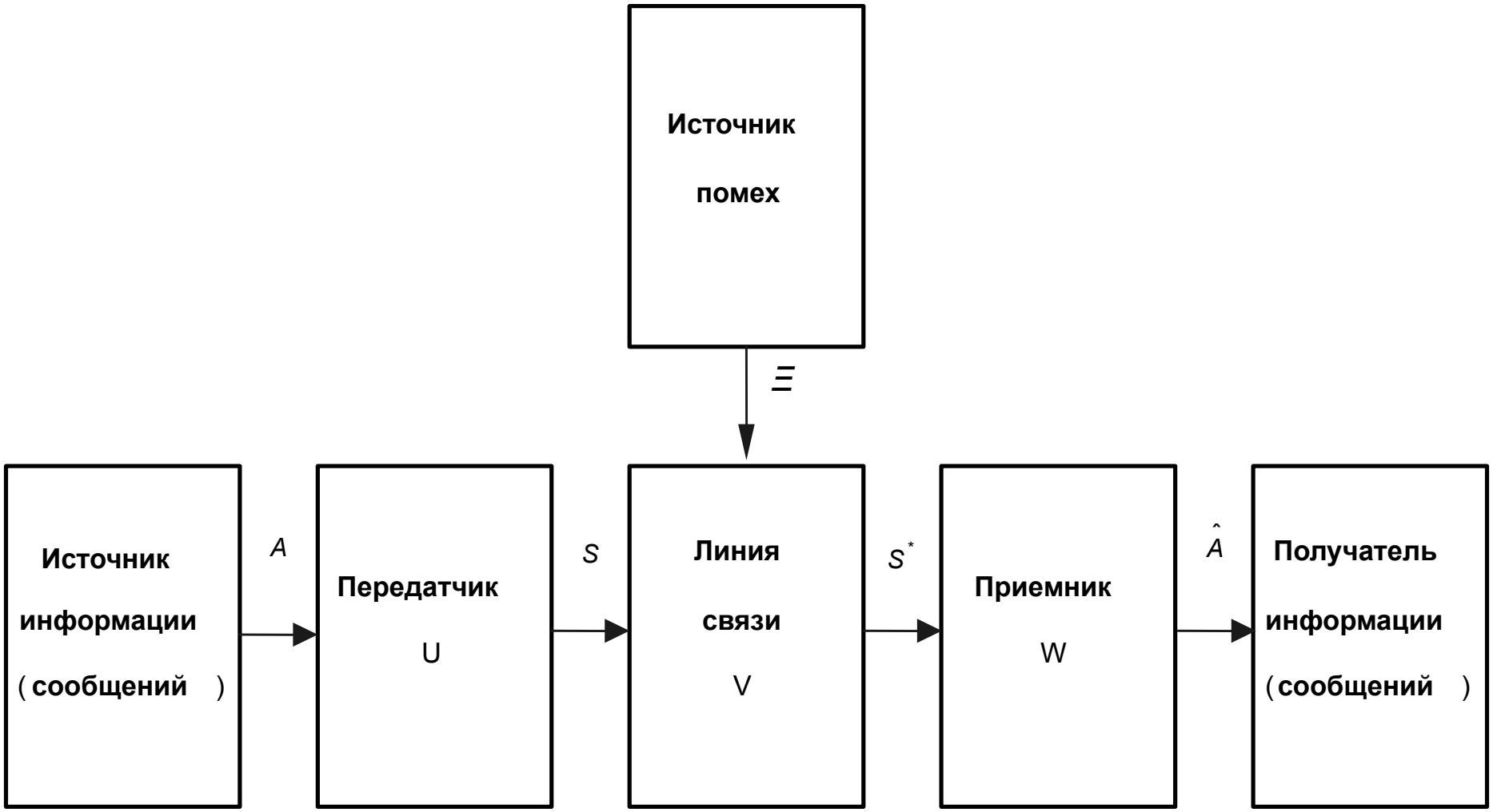
(часть 2)

Напоминание из ОБЩЕЙ ТЕОРИИ СВЯЗИ (часть 1)

1. Общие сведения о системах связи.
2. Детерминированные и случайные сигналы.
3. Каналы связи.
4. Методы формирования и преобразования сигналов в каналах связи.

- **ОБЩАЯ ТЕОРИЯ СВЯЗИ** – это теория о способах, законах и методах коммуницирования (общения) между людьми с помощью созданных ими устройств, а также способах взаимодействия между людьми и созданными ими объектами, например, компьютерами; способами и методами «общения» компьютеров между собой и различными устройствами, а так же о том, как осуществляется связь вообще, в том числе, в живой природе на самых разных уровнях, например, общение пчел, «общение» на клеточном уровне и т.д.

По Клоду Шеннону

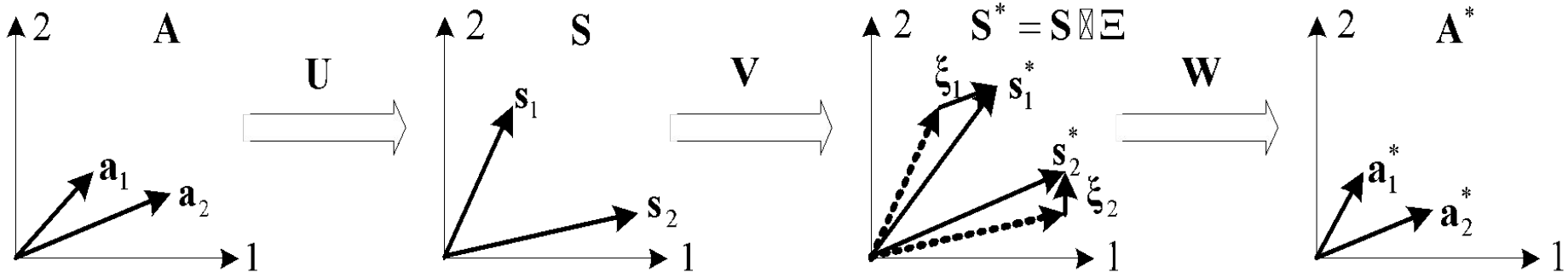


$$\hat{a} = \mathrm{W}\{\mathrm{V}[\mathrm{U}(a), \xi]\}$$

$$s^*(t) = s(t) + \xi(t)$$

$$s^*(t) = \mu(t)s(t)$$

$$s^*(t) = \mu(t)s(t) + \xi(t)$$



Геометрическое преобразование пространств сигналов

- *энергия* E_x, как средний квадрат сигнала на единичном сопротивлении

$$E_x = \int_{-\infty}^{\infty} x^2(t)dt;$$

- *длительность* T_x или интервал наблюдения сигнала; часто длительность сигнала T_x оценивается как такой интервал времени, в пределах которого сосредоточена определенная доля γ его энергии

$$\gamma E_x = \int_{-T_x/2}^{T_x/2} x^2(t)dt, \rightarrow T_x = \varphi[x;\gamma],$$

где T_x является функцией формы сигнала и величины γ;

- *средняя мощность* P_x

$$P_x = E_x / T_x,$$

- *динамический диапазон*, оцениваемый в децибелах (дБ)

$$D_x = 10\lg\left(P_{x,\max} / P_{x,\min}\right),$$

где $P_{x,\max}$ и $P_{x,\min}$ максимальная и минимальная мощности сигнала.

Помимо временного описания сигналов, рассматривается их описание в частотной области, используя преобразование Фурье.

- *спектральная плотность комплексных амплитуд* $S_x(j\omega)$ (СПКА), определяемая по форме сигнала на основе прямого преобразования Фурье

$$S_x(j\omega) = \int_{-\infty}^{\infty} x(t)\exp(-j\omega t)dt,$$

где $\omega = 2\pi f$ - круговая частота, $f = \omega / 2\pi$ - линейная частота, $\exp(-j\omega t)$ - комплексная экспонента, представляемая по формуле Эйлера

$$\exp(-j\omega t) = e^{-j\omega t} = \cos\omega t - j\sin\omega t;$$

- *энергия* E_x, которая на основе равенства Парсеваля определяется так

$$E_x = \frac{1}{2\pi}\int_{-\infty}^{\infty} S_x(j\omega)S_x(-j\omega)d\omega = \frac{1}{2\pi}\int_{-\infty}^{\infty} S_x^2(\omega)d\omega,$$

где $S_x(\omega) = |S_x(j\omega)|$ - модуль СПКА или амплитудный спектр сигнала $x(t)$;

- *ширина спектра* F_x; часто ширина спектра сигнала оценивается как такой интервал частот, в котором сосредоточена определенная доля β его энергии

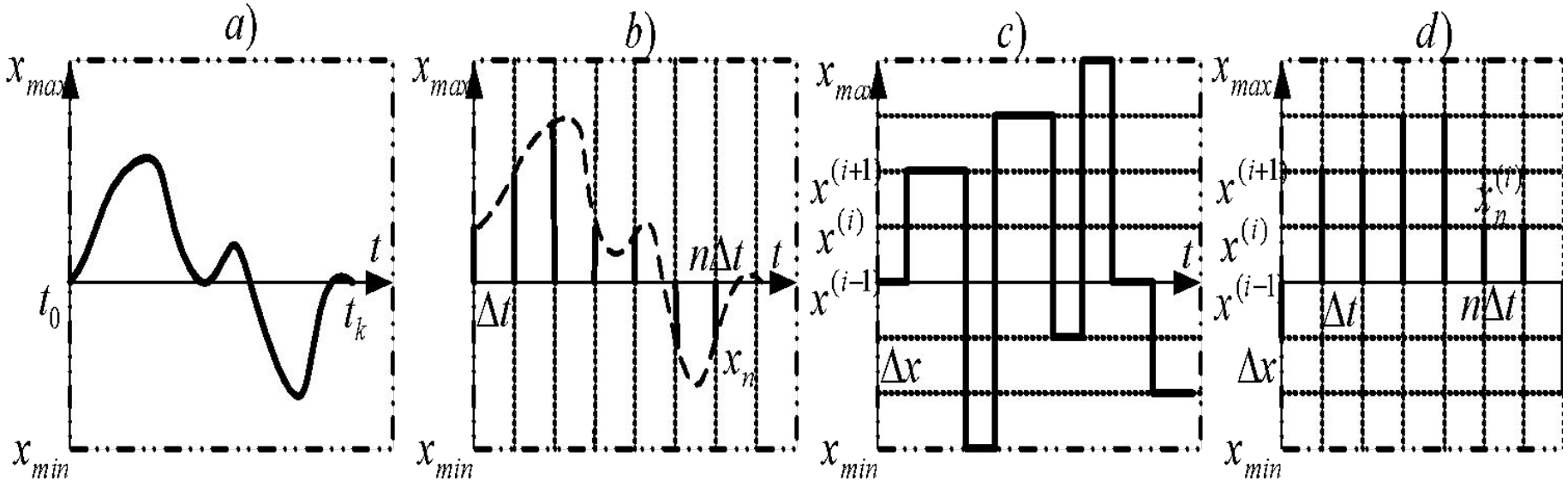
$$\beta E_x = \frac{1}{\pi}\int_{0}^{2\pi F_x} S_x^2(\omega)d\omega, \rightarrow F_x = \psi[S_x;\beta],$$

где F_x является функцией формы СПКА и величины β.

Что мы будем изучать в ОБЩЕЙ ТЕОРИИ СВЯЗИ (часть 2)

- **Методы цифрового представления и передачи сообщений.**
- **Основы теории передачи информации.**
- **Основы теории кодирования дискретных сообщений.**
- **Основы оптимального приема дискретных сообщений.**
- **Основы оптимального приема непрерывных сообщений.**
- **Методы многоканальной передачи и распределения информации.**

Методы цифрового представления и передачи сообщений.



- непрерывный (аналоговый), - дискретно-непрерывный, - непрерывно-дискретный, - дискретный (цифровой).

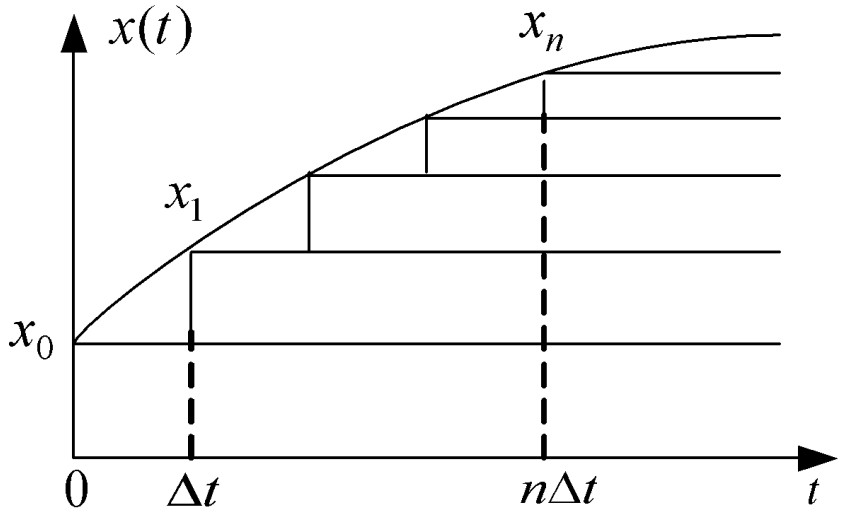

Источник сообщений
A
Аналого-Цифровой Преобразо-ватель
Модулятор
Передатчик
S
Источник помех
ξ
Линия связи
S*
Приёмник
Получатель сообщений
A*
Цифро-Аналоговый Преобразо-ватель
Детектор

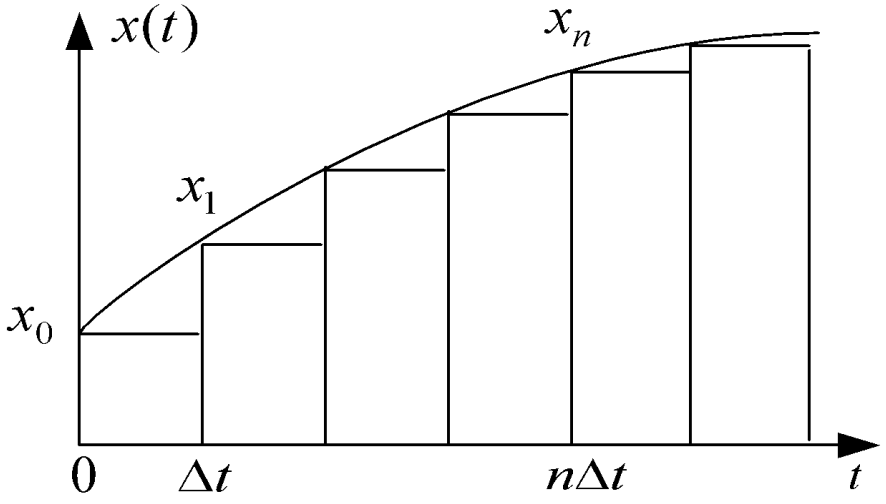
Временное представление аналоговых сигналов в виде суммы элементарных сигналов. Например:

$$x(t) = x_0\sigma(t) + \sum_{k=1}^{\infty}(x_k - x_{k-1})\sigma(t - k\Delta t),$$

или прямоугольных импульсов длительностью Δt, примыкающих друг к другу

$$x(t) = \sum_{k=-\infty}^{\infty}\frac{x_k}{\Delta t}[\sigma(t - t_k) - \sigma(t - t_k - \Delta t)]\Delta t\,.$$





Точность такого представления возрастает при $\Delta t \to 0$, а суммирование заменяется интегрированием по некоторой переменной τ, дифференциал $d\tau$ которой заменяет предел $\Delta t \to 0$. При таком предельном переходе формулы для сигнала преобразуются и принимают следующий вид

$$x(t) = \int_{-\infty}^{\infty} x(\tau)\delta(t-\tau)d\tau$$

$\sigma(t)$ – функция единичного скачка (Хевисайда) и $\delta(t)$ – дельта–функция (Дирака); они взаимосвязаны друг с другом и характеризуются соотношениями:

$$\sigma(t) = \int_{-\infty}^{t} \delta(\tau)d\tau = \begin{cases} 0, & t < 0, \\ 0.5, & t = 0, \\ 1, & t > 0. \end{cases}$$

$$\delta(t) = \frac{d\sigma(t)}{dt} = \begin{cases} 0, & t \neq 0, \\ \infty, & t = 0. \end{cases}$$

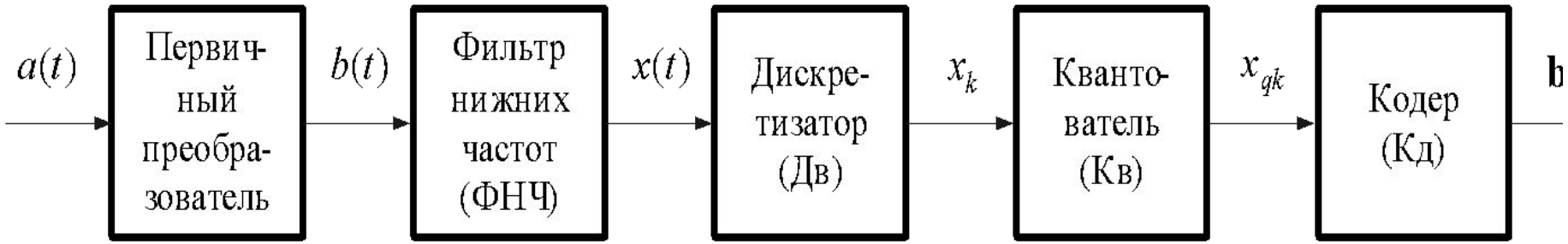
Для функции $\delta(t)$ справедливы: условие нормировки и фильтрующее свойство вида:

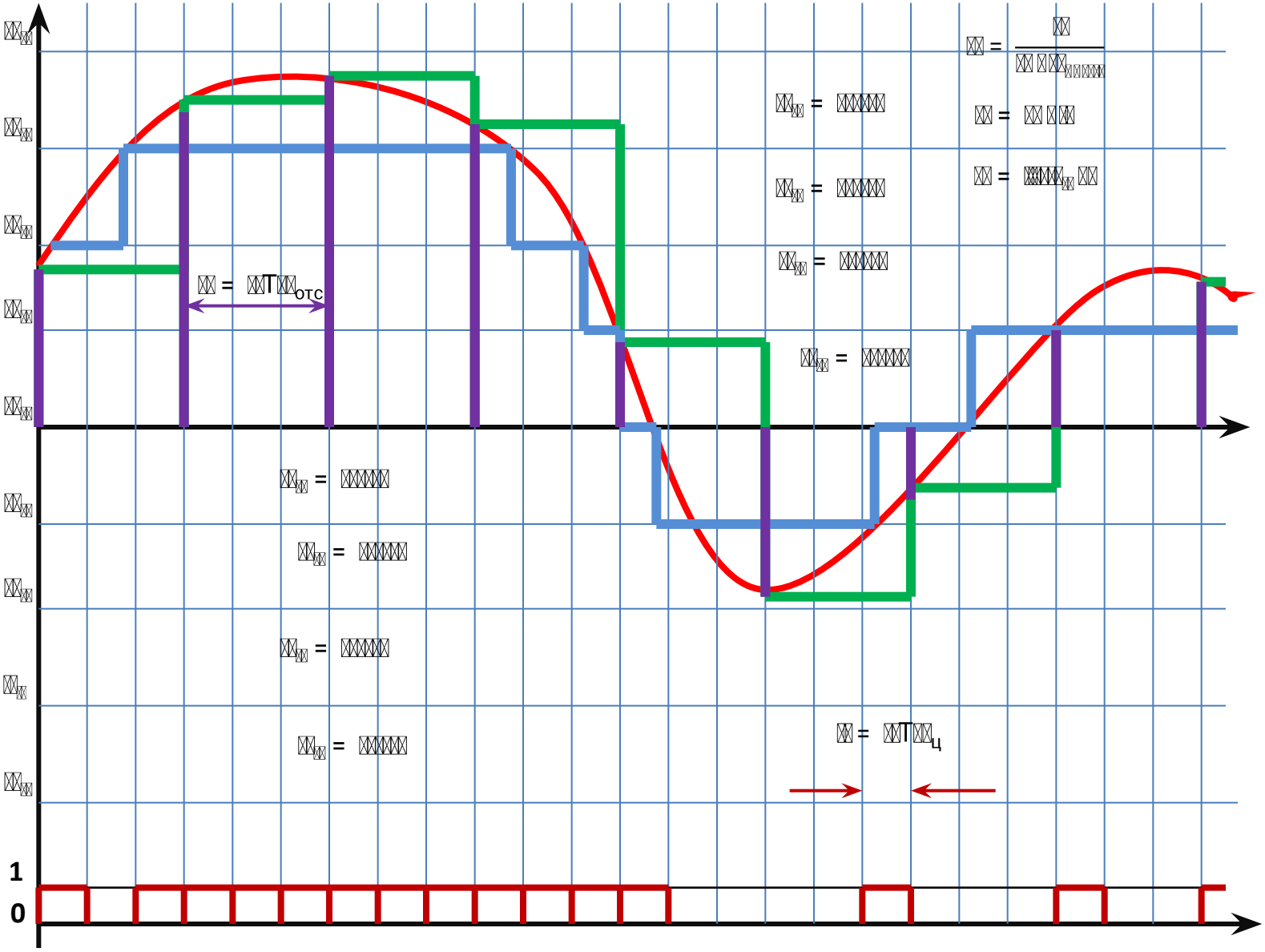
$$\int_{-\infty}^{\infty} \delta(t)dt = 1 \qquad \int_{-\infty}^{\infty} x(t)\delta(t-t_0)dt = x(t_0)$$

Оператор АЦП, осуществляющий преобразование непрерывного сообщения в цифровое, представляется в следующем виде

$$\mathbf{b}_k = \mathrm{Q}_{acp}[a(t)], \quad k = 1,2,3,...$$

где $\mathbf{b}_k = (b_0, b_1, ..., b_j, ..., b_{n-1})_k$ – вектор-строка кодовых символов, наблюдаемых на выходе АЦП в k – ый момент времени; это цифровой отклик АЦП на входное аналоговое сообщение. Иначе, $\{\mathbf{b}_k\}$ - есть *кодовый эквивалент сообщения* $a(t)$.




1
0

Теорема Котельникова

Любая непрерывная функция $x(t)$ с ограниченным (финитным) спектром может быть представлена своими отсчетами $x_n = x(n\Delta t)$, $n = 0, \pm 1, \pm 2, \ldots$, взятыми в моменты времени t_n, отстоящими друг от друга на интервал времени Δt (интервал дискретизации), где

$$\Delta t \le \frac{1}{2F_{max}} = \frac{\pi}{\omega_{max}}$$

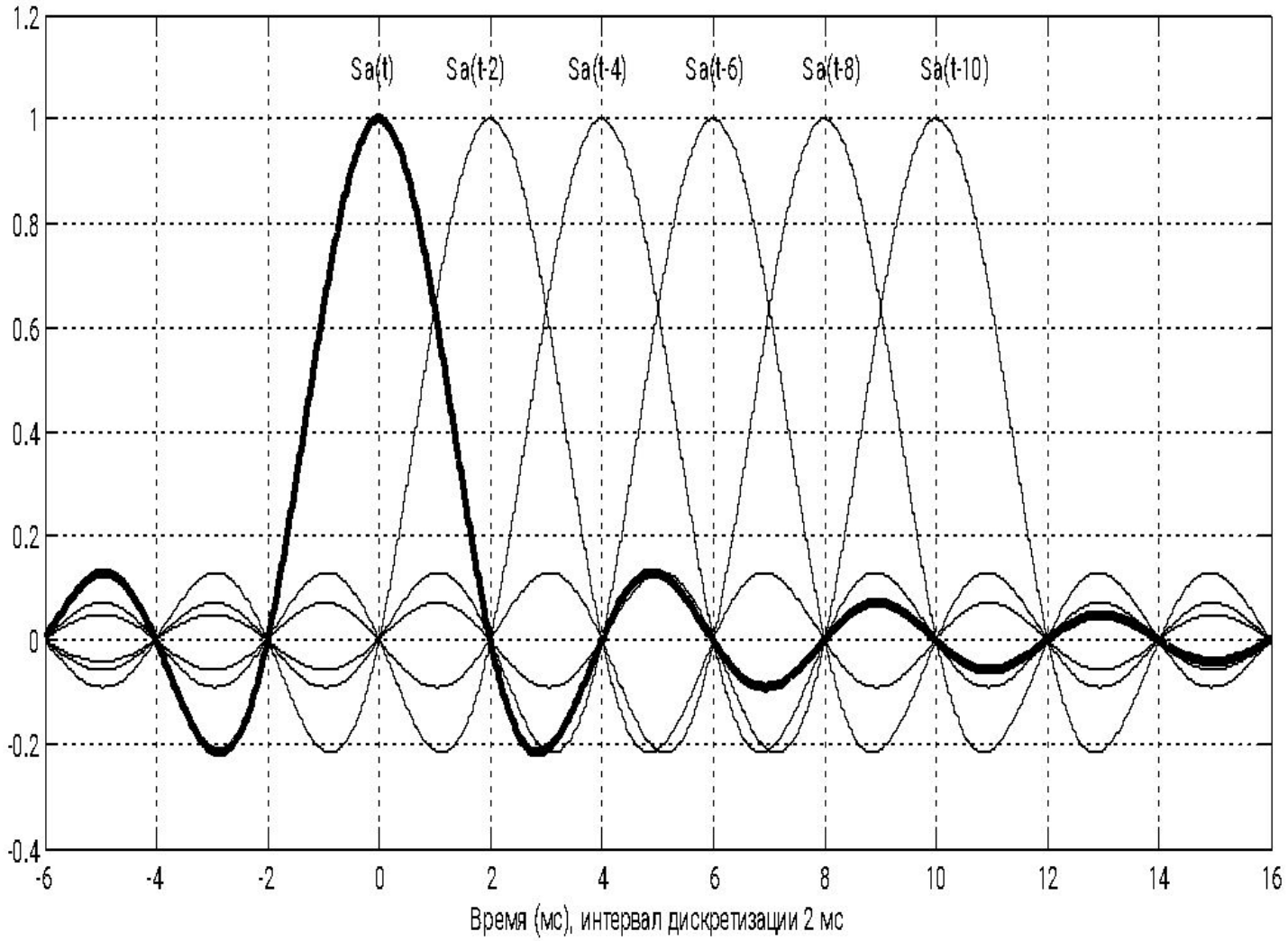
В итоге сигнал представляется в виде ортогонального ряда Котельникова

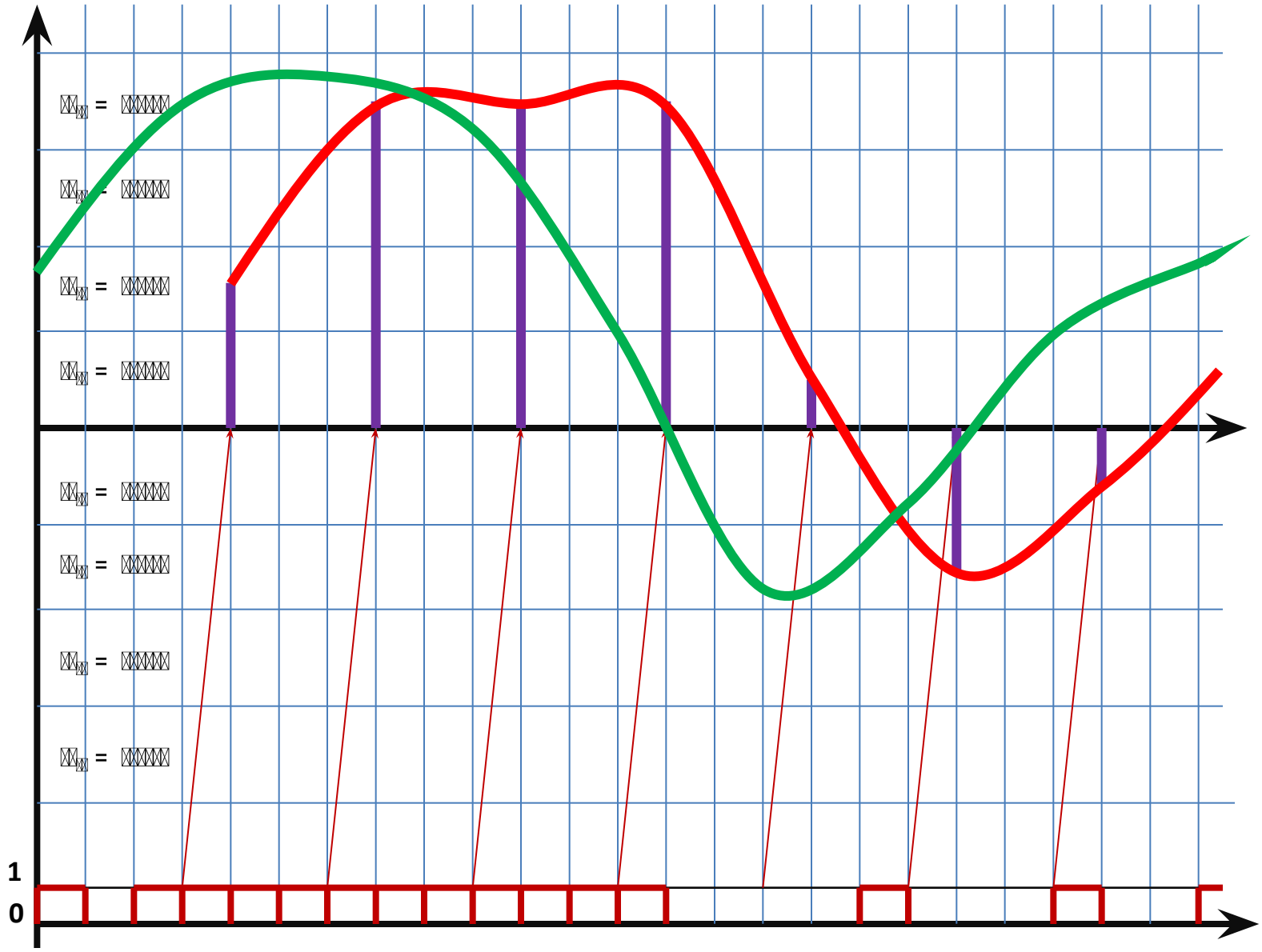
$$x(t) = \sum_{n=-\infty}^{n=\infty} x(n\Delta t) \cdot \frac{\sin \omega_{max}(t - n\Delta t)}{\omega_{max}(t - n\Delta t)},$$

что соответствует дискретной свертке во временной области последовательности отсчетов x_n с ортогональными функциями отсчетов $x_n(t) = \sin \omega_{max}(t - n\Delta t)$.

Это можно записать:

$$x(t) = \sum_{n=-\infty}^{n=\infty} x_n \cdot \sin \omega_{max}(t - n\Delta t)$$


Sa(t)
Sa(t-2)
Sa(t-4)
Sa(t-6)
Sa(t-8)
Sa(t-10)
1.2
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-6
-4
-2
0
2
4
6
8
10
12
14
16
Время (мс), интервал дискретизации 2 мс


1
0

В реальных условиях обработки аналоговых сигналов их полностью безошибочное восстановление по дискретным отсчетам не возможно по следующим причинам:

1. Сигналы с ограниченным спектром можно наблюдать только на бесконечном временном интервале. В реальных условиях этот интервал ограничен, что приводит к расширению спектра сигнала до бесконечности. Это следует из свойства преобразования Фурье для сигналов, ограниченных во времени.

2. На интервале наблюдения аналогового сигнала при конечном интервале дискретизации наблюдается конечное число отсчетов. Поэтому в реальном случае ряды содержат конечное число составляющих.

3. Реальное восстанавливающее устройство отлично от идеального фильтра нижних частот и имеет характеристики, отличные от идеальных.

4. Имеются погрешности в синхронизации, обеспечивающих стабильность частоты отсчетов.

5. Имеются погрешности из-за неточности квантования и проч.

Натур. Код (1)	000	001	010	011	100	101	110	111	Итого
3, 2, 1	4;2;1	4;2;1	4;2;1	4;2;1	4;2;1	4;2;1	4;2;1	4;2;1	4x8+ 2x8+ 1x8= 56
3-2, 2-1, 3-1	6;3;5	6;1;3	2;1;5	2;3;3	2;3;3	2;1;5	6;1;3	6;3;5	6x4+ 5x4+ 3x8+ 2x4+ 1x4= 80
321	7	5	3	1	1	3	5	7	7x2+ 5x2+ 3x2+ 1x2= 32

Код Грея (2)	000	001	011	010	110	111	101	100	Итого
3, 2, 1	7, 3, 1	5, 1, 1	3, 1, 1	1, 3, 1	1, 3, 1	3, 1, 1,	5, 1, 1,	7, 3, 1	7x2+ 5x2+ 3x6+ 1x14= 56
3-2, 2-1, 3-1	4, 2, 6	4, 2, 6	4, 2, 2	4, 2, 2	4, 2, 2	4, 2, 2,	4, 2, 6	4, 2, 6	6x4+ 4x8+ 2x12= 80
321	5	3	5	3	3	5	3	5	5x4+ 3x4= 32

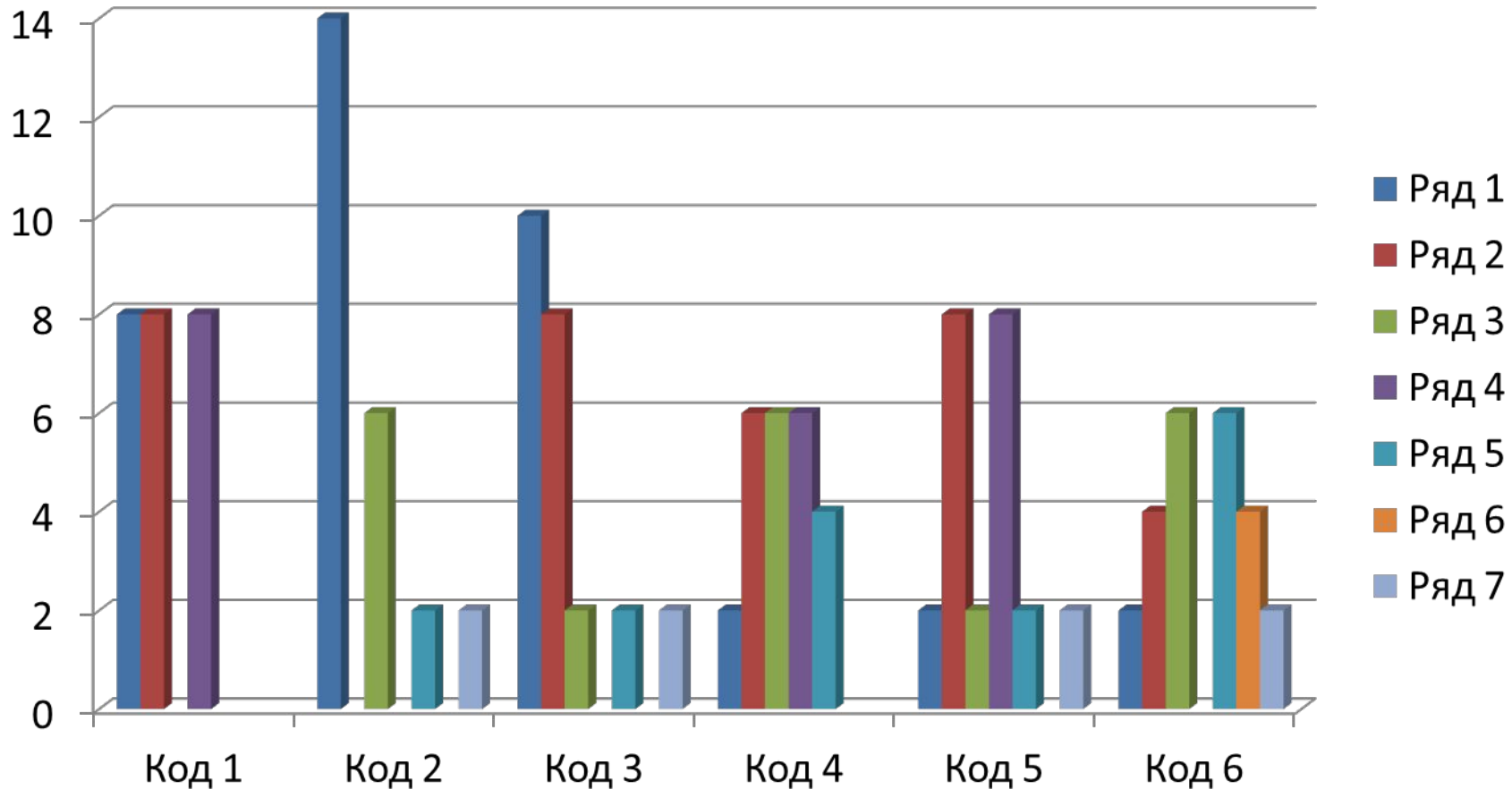
Код в ИКМ (3)	011	010	001	000	100	101	110	111	Итого
3, 2, 1	7, 2, 1	5, 2, 1	3, 2, 1	1, 2, 1	1, 2, 1	3, 2, 1	5, 2, 1	7, 2, 1	7x2+ 5x2+ 3x2+ 2x8+ 1x10= 56
3-2, 2-1, 3-1	5, 3, 6	3, 1, 6	5, 1, 2	3, 3, 2	3, 3, 2	5, 1, 2	3, 1, 6	5, 3, 6	6x4+ 5x4+ 3x8+ 2x4+ 1x4= 80
321	4	4	4	4	4	4	4	4	4x8= 32

Случ. код (4)	000	011	111	001	100	010	101	110	Итого
3, 2, 1	4, 5, 3	1, 2, 4	1, 4, 5	3, 2, 3	4, 3, 2	2, 5, 4	3, 4, 2	2, 3, 5	5x4+ 4x6+ 3x6+ 2x6+ 1x2= 76
3-2, 2-1, 3-1	7, 1, 6	5, 1, 6	1, 2, 3	1, 2, 1	1, 2, 1	1, 2, 3	5, 1, 6	7, 1, 6	7x2+ 6x4+ 5x2+ 3x2+ 2x4+ 1x10= 72
321	2	3	2	4	3	1	1	4	4x2+ 3x2+ 2x2+ 1x2= 20

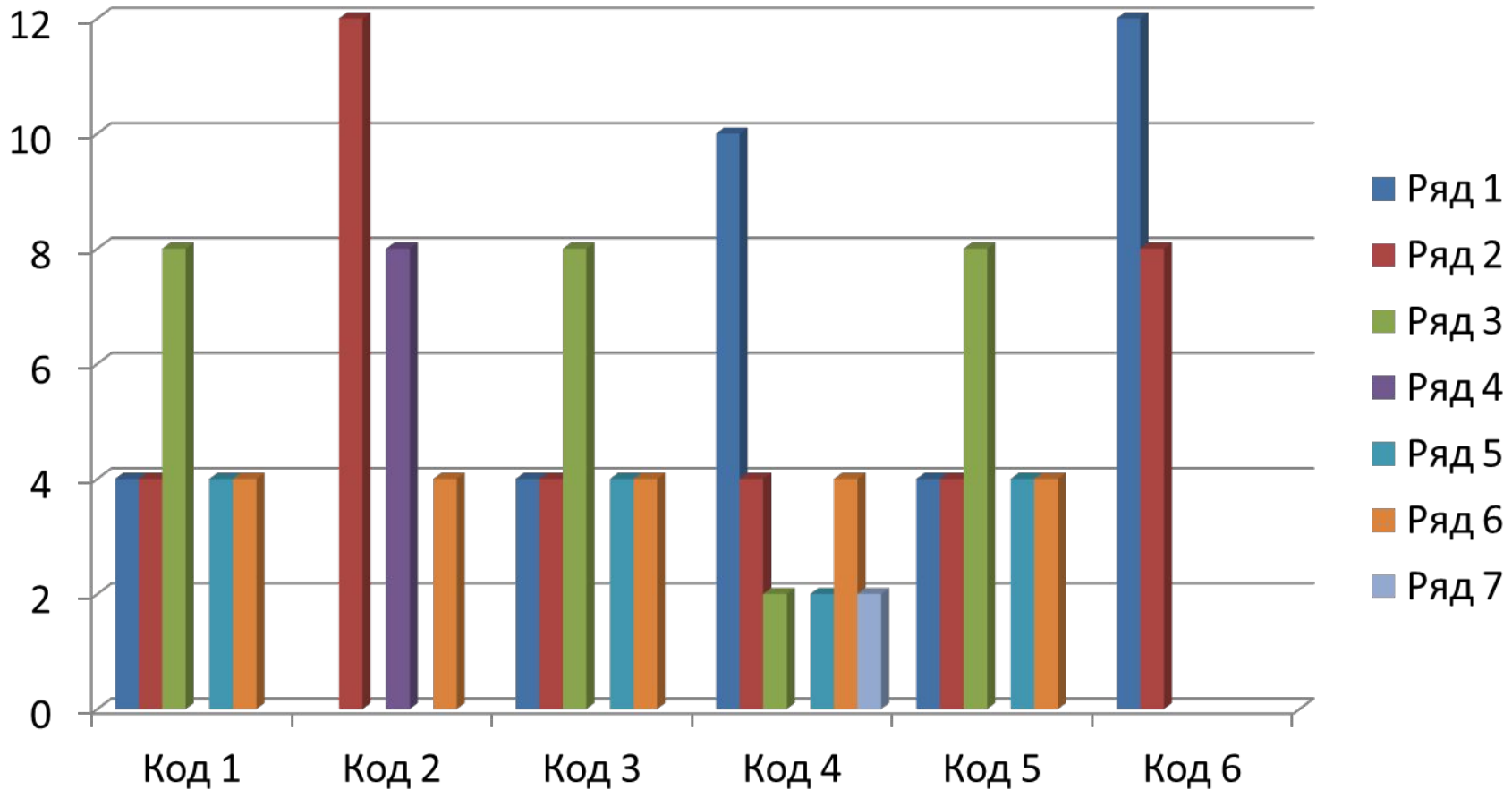
Код Ми 3 (5)	000	111	001	110	010	101	011	100	Итого
3, 2, 1	7, 4, 2	5, 4, 2	3, 4, 2	1, 4, 2	1, 4, 2	3, 4, 2	5, 4, 2	7, 4, 2	7x2+ 5x2+ 4x8+ 3x2+ 2x8+ 1x2= 80
3-2, 2-1, 3-1	3, 6, 5	1, 6, 3	1, 2, 5	3, 2, 3	3, 2, 3	1, 2, 5	1, 6, 3	3, 6, 5	6x4+ 5x4+ 3x8+ 2x4+ 1x4= 80
321	1	1	1	1	1	1	1	1	1x8= 8

Код Ми 2 (6)	000	110	011	101	111	001	100	010	
3, 2, 1	6, 7, 5	6, 5, 3	2, 3, 5	2, 1, 3	2, 1, 3	2, 3, 5	6, 5, 3	6, 7, 5	7x2+ 6x4+ 5x6+ 3x6+ 2x4+ 1x2= 96
3-2, 2-1, 3-1	1, 2, 3	1, 2, 1	1, 2, 1	1, 2, 3	1, 2, 3	1, 2, 1	1, 2, 1	1, 2, 3	3x4+ 2x8+ 1x12= 40
321	4	4	4	4	4	4	4	4	4x8= 32

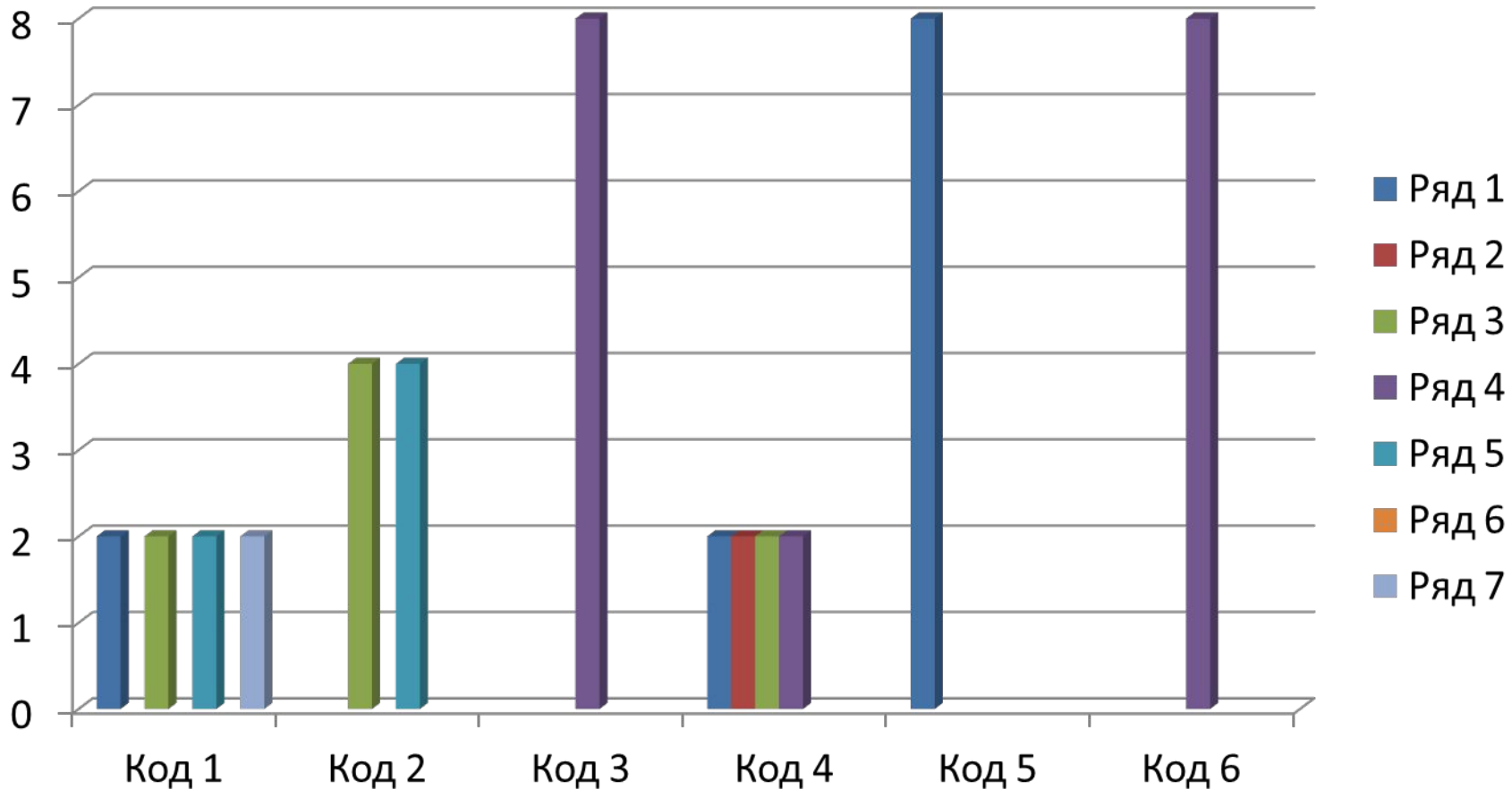
Код	1	2	3	4	5	6
Итого 1-кр	56	56	56	76	80	96



Код	1	2	3	4	5	6
Итого 2-кр	80	80	80	72	80	40



Код	1	2	3	4	5	6
Итого 3-кр	32	32	32	20	8	32



При неизменной общей сумме искажений равной 168 из-за 1-кратных, 2-кратных и 3-кратных ошибок и среди $M=(2^n)!=(2^3)!=40\ 320$ способов кодирования имеем:

Код	1	2	3	4	5	6
1-кр	56	56	56	76	80	96
2-кр	80	80	80	72	80	40
3-кр	32	32	32	20	8	32

Для натурального (взвешенного) кода следующие таблицы кодовых расстояний:

- При n=1 имеем комбинации 0 и 1. Для них: $D_1=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- При n=2 имеем комбинации 00; 01; 10 и 11.

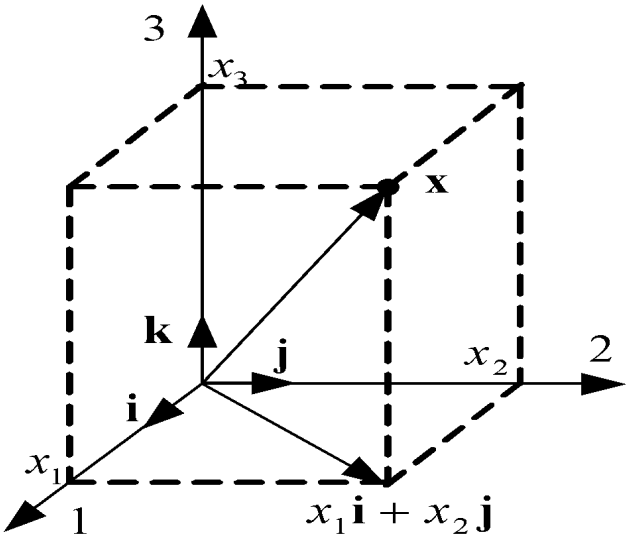
Для них: $D_2=\begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix}$

- В общем виде имеем: $D_n=\begin{pmatrix} D_{n-1} & D_{n-1}+E \\ D_{n-1}+E & D_{n-1} \end{pmatrix}$,

где $E=\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{pmatrix}$

- Матрица потерь $L_n = \begin{pmatrix} l_{11} & l_{12} & \dots & l_{1n} \\ l_{21} & l_{22} & \dots & l_{2n} \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{pmatrix}$

- Средние потери $\bar{L} = \sum_{j=1}^{n} \sum_{i=1}^{n} p_i \times l_{i;j} \times p\left(a_j^* / a_i\right)$



$$\mathbf{x} = x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$$

$$\mathbf{x} = \{x_1, x_2, x_3\}$$

Метрическое пространство. Пусть задано множество X произвольных элементов $\mathbf{x}$ – векторов сигнального пространства. Множество X называется *метрическим пространством*, если для каждых двух произвольных элементов $\mathbf{x}$, $\mathbf{y}$ этого множества введена неотрицательная функция $d(\mathbf{x},\mathbf{y})$, называемая *метрикой* или *расстоянием*, которая удовлетворяет следующим аксиомам:

а) $d(\mathbf{x},\mathbf{y}) > 0, d(\mathbf{x},\mathbf{y}) = 0$ только тогда, когда $\mathbf{x} = \mathbf{y}$;

б) $d(\mathbf{x},\mathbf{y}) = d(\mathbf{y},\mathbf{x})$ - аксиома симметрии;

в) $d(\mathbf{x},\mathbf{y}) \le d(\mathbf{x},\mathbf{z}) + d(\mathbf{z},\mathbf{y})$ - аксиома неравенства треугольника для расстояния.

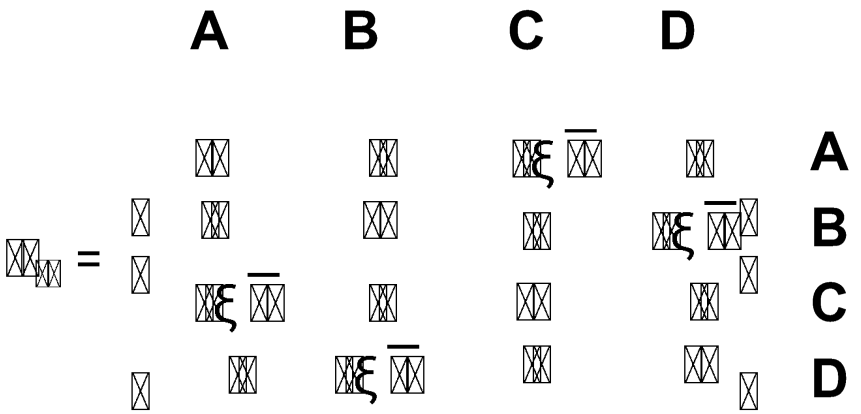
Матрица потерь:

$$L_n = \begin{pmatrix} l_{11} & l_{12} & \cdots & l_{1n} \\ l_{21} & l_{22} & \cdots & l_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ l_{n1} & l_{n2} & \cdots & l_{nn} \end{pmatrix}$$

A=(00) l **B=(01)**

l

D=(10) **C=(11)**



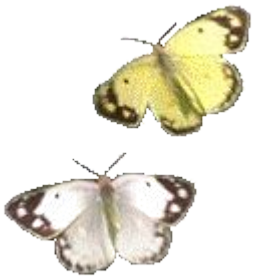
Пример расчета цифровой системы передачи

В телефонии для передачи речевого сообщения выделяется канал (тональной частоты) с полосой пропускания от 0,3 до 3,4 кГц. С учетом не идеальности фильтров выделяется дополнительная полоса частот на «расфильтровку». Итого получается 4 кГц. Тогда по теореме Котельникова скорость отсчетов равна $\square\square_{отсч} = \square\square\square\square_{\square\square\square\square} = \square\square$ кбитТс. Для необходимой точности передачи значений отсчетов выбрано $\square\square = \square\square\square\square\square$ уровней квантования, что доказано экспертными оценками. Тогда для кодирования каждого отсчета потребуется $\square\square = \square\square\square\square\square_{\square\square}\square\square = \square\square\square\square\square_{\square\square}\square\square\square\square\square = \square\square$ символов (элементов) цифрового сигнала. Следовательно, скорость цифрового сигнала $\square\square_{ц} = \square\square\square\square_{отсч} = \square\square\square\square = \square\square\square\square$ кбитТс.

В современных системах с тем же качеством речевой сигнал может передаваться со скоростью цифрового сигнала $\square\square_{ц} = \square\square$ кбитТс, что достигается за счет учета особенностей речи. А великая теорема Котельникова определяет лишь достаточные условия для передачи аналогового сигнала по цифровому тракту!

Основы теории передачи информации.












- ***Информация*** *- это объективно существующее неотъемлемое* ***свойство*** *объектов, процессов, явлений, отражающее их особенности и разнообразие в различных* ***метрических*** *или* ***топологических*** *пространствах.*
- ***Информация*** *отображается в форме (в виде)* ***сообщений****, имеющих ту или иную материальную основу.*
- ***Сообщения*** *преобразуются в* ***сигналы****, которые непосредственно передаются по системе связи.*
- ***Сигналы*** *могут многократно преобразовываться в другие* ***сигналы*** *с целью согласования со средой передачи.*
- ***Информация*** → ***Сообщение*** → ***Сигнал*** →…→ ***Сигнал*** → ***Сообщение*** →

- **Метри́ческим простра́нством** называется множество называется множество, в котором между любой парой элементов определено обладающее определенными свойствами расстояние, называемое *ме́трикой*.
- **Топологи́ческое простра́нство** — множество с дополнительной структурой определённого типа (так называемой топологией) или другими словами – это совокупность двух объектов: множества ***X***, состоящего из элементов произвольной природы, называемых точками данного пространства, и из введенной в это множество топологической структуры, или топологии.

- **Множество** - набор, совокупность, собрание каких-либо объектов, называемых его элементами, обладающих общим для всех их характерным свойством.
- **Расстоя́ние**, в широком смысле, степень удаленности или отличий объектов друг от друга.
- **Математи́ческая структу́ра** — название, объединяющее понятия, общей чертой которых является их применимость к множествам, природа которых не определена. Для определения самой структуры задают отношения, в которых находятся элементы этих множеств. Затем постулируют, что данные отношения удовлетворяют неким условиям, которые являются аксиомами рассматриваемой

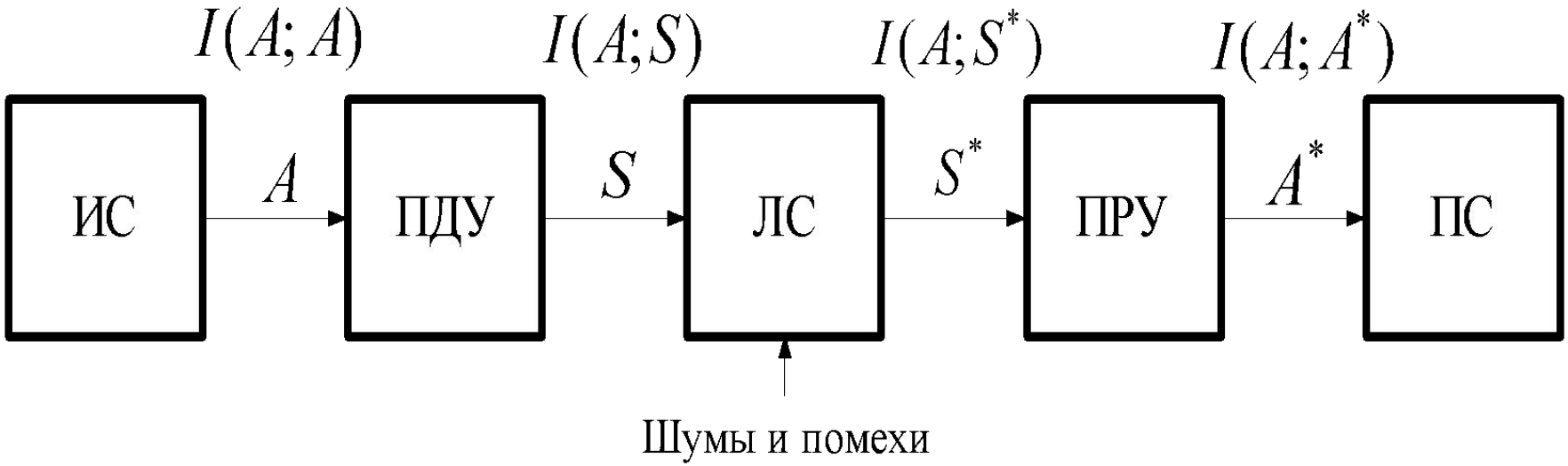
- **Отноше́ние** в теории множеств — математическая структура, которая формально определяет свойства различных объектов и их взаимосвязи. Распространёнными примерами отношений в математике являются равенство, делимость, подобие, параллельность и т.д. Наглядно теоретико-множественное отношение можно представить в виде таблицы, каждая строка которой содержит конкретные примеры объектов, связанных данным отношением. Например, телефонный справочник можно рассматривать как отношение, отражающее связь между следующими объектами: **Телефон** ↔ **ФИО абонента** ↔ **Почтовый адрес** ↔ **…** Отношения обычно классифицируются по количеству связываемых объектов и собственным свойствам (симметричность Отношения обычно

Отношение R симметрично, если

Отношение R транзитивно, если

, *при* Rb *и* bRc будет выполняться Rc.

Блок-схема системы передачи информации



В процессе передачи по СПИ сообщение подвергается многочисленным преобразованиям, существенно меняющим его электрическое представление и физические характеристики. Например, при передаче речевого сообщения по радиоканалу человек как источник информации с помощью голосового аппарата формирует звуки речи вначале на акустическом уровне. В микрофоне звуковое давление преобразуется в электрический ток. В модуляторе передатчика этот низкочастотный ток (первичный сигнал) преобразуется в высокочастотное напряжение (сигнал), которое затем на выходе антенной системы представляется в виде электромагнитной волны (поля), распространяющейся по радиолинии. Принятая радиоволна (поле) с помощью антенной системы преобразуется в высокочастотное напряжение (принятый сигнал), которое в приемнике преобразуется в низкочастотное напряжение (или ток) – принятое сообщение, и, наконец, с помощью телефона или громкоговорителя это сообщение преобразуется в акустические волны, воспринимаемые слуховой системой человека как получателя информации.

Надо иметь в виду, что в любой системе связи, используемой человеком, конечной целью передачи является не само сообщение, а та информация, которая в нем содержится. Эта информация определяется источником (человеком) и называется полезной информацией. Она не зависит (инвариантна) от физической формы представления сообщения, и, следовательно, сообщение, переданный и принятый сигналы, а также принятое сообщение в идеале должны содержать одно и то же количество информации, вырабатываемое источником. В реальных условиях количество передаваемой источником информации уменьшается из-за действия помех и искажений в различных блоках системы связи.

В теории информации это понятие носит более утилитарный характер. Под *информацией* понимают любые *сведения* о состоянии или поведении некоторого объекта или системы, либо о каких-то событиях, явлениях, предметах, подлежащие передаче от ИС к ПС. При таком определении источником информации уже может быть не только человек, но и компьютер, телеметрический датчик и т.д. При этом можно отметить, что если получатель априори (до передачи) достоверно знает, что будет передано от источника, то количество получаемой им информации нулевое и такая передача (связь) бессмысленна (нецелесообразна), ведь все заранее известно. Поэтому информация, воспринимаемая ПС, будет отличаться от нуля только в случае, если передаваемые сведения являются для него новыми, непредвиденными. Именно эта информация должна оставаться инвариантной при всех преобразованиях сообщений в СПИ; *сообщения и сигналы являются только физическими носителями информации*.

В СПИ сообщение $A \in \mathbf{A}$, выбираемое из множества $\mathbf{A}$, обладает информацией $I(A;A)$, называемой *собственной информацией*, содержащейся в сообщении A относительно исходного сообщения A. Отклик ПДУ $S \in \mathbf{S}$ переносит информацию $I(A;S)$, называемую *взаимной информацией*, содержащуюся в сигнале S относительно сообщения A. Аналогично $I(A;S^*)$ - взаимная информация, содержащаяся в сигнале $S^* \in \mathbf{S}^*$, наблюдаемого на приеме относительно сообщения A, а $I(A;A^*)$ - взаимная информация, содержащаяся в восстановленном сообщении $A^* \in \mathbf{A}^*$ относительно передаваемого сообщения A. Поскольку информация при преобразованиях сообщений и сигналов не может увеличиться, то в любой СПИ справедливы следующие неравенства

$$I(A;A) \geq I(A;S) \geq I(A;S^*) \geq I(A;A^*).$$

Равенства достигаются лишь в идеальном случае, когда в СПИ нет ни искажений, ни шумов, ни помех. В этом случае вся информация, вырабатываемая ИС поступает к ПС. В реальном случае в СПИ имеются потери информации. (Следует еще раз подчеркнуть, что в данном случае речь идет об информации, определенной в утилитарном смысле. При более общем определении процесс измерения количества информации приобретает более сложный вид).

В общей теории связи для количественной оценки предельных возможностей СПИ вводят ряд внешних и внутренних характеристик.

К *внешним характеристикам* относят верность, скорость и своевременность передачи информации (задержку). *Верность* передачи информации характеризуют мерой отличия принятого сообщения от переданного: $\rho = \mu(A^*, A)$. Примерами такой меры могут быть: вероятность отклонения принятого сообщения от переданного, их среднеквадратичное отклонение и т.д. *Скорость* передачи информации – это количество взаимной информации, передаваемой по системе (каналу) в единицу времени с заданной верностью: $R = I(S, S^*)/T$. *Своевременность* передачи информации или *задержка* зависят от времени, затрачиваемого при различных преобразованиях сигналов, времени его распространения к получателю относительно времени начала передачи.

К *внутренним характеристикам* относят информационную эффективность и помехоустойчивость СПИ. *Информационная эффективность* – это отношение скорости передачи информации к её предельно возможной (максимальной) величине: $\eta = R / R_{\max} = R / C$. Величину $C = R_{\max}$ определяют по всем возможным вероятностным распределениям источника и называют *пропускной способностью* канала. Эта величина зависит только от свойств используемых в канале преобразований сигналов, но не зависит от свойств источника сообщений. *Помехоустойчивость* – это способность системы противостоять вредному действию помех. Помехоустойчивость определяется выбранной мерой верности восстановления сообщения. Система, в которой достигается экстремум показателя верности, обладает *потенциальной* (предельно возможной) помехоустойчивостью, а её отдельные функциональные блоки (передатчик, приемник или их элементы), обеспечивающие экстремум выбранному показателю верности, называют *оптимальными*.

Информационная мера Хартли. Рассмотрим ИДС, работа которого осуществляется путем последовательной выборки символов из M равновероятных возможностей. При первом выборе возможны M различных символов, при двух последовательных выборах возможны M^2 различных перестановок или последовательностей символов. Очевидно, при n выборах возможны $M_0 = M^n$ различных последовательностей символов. Полагая, что на передаче осуществляется одна из M_0 возможностей, на приеме имеется априорная неопределенность прямо связанная с M_0 (т.е. чем больше M_0, тем больше неопределенность). Численной мерой неопределенности является *энтропия* H. Её связь с M_0 определяется некоторой неотрицательной, возрастающей функцией. Впервые логарифмическую меру информации ввел *Хартли*, поэтому величину

$$H = \log_b M_0 = \log_b \left(M^n\right) = n \cdot \log_b M \,,$$

называют *хартлиевским количеством информации*. Если основание логарифма равно $b = e$, то информация оценивается в *натах* (натуральных единицах): $H = \ln M$. Если $b = 2$, информация оценивается в *битах* (двоичных единицах): $H = \log_2 M = \mathrm{ld} M$. При $b = 10$, информация оценивается в *дитах* (десятичных единицах): $H = \log_{10} M = \lg M$. Из сопоставления данных единиц информации следует, что 1 нат крупнее 1 бита в $\log_2 e = 1/\ln 2 \approx 1{,}44$ раза, а 1 дит крупнее 1 бита в $\log_2 10 \approx 3{,}3$ раза. В инженерно-технических приложениях теории информации часто используется единица *бит* и её производные: *байт* ($8=2^3$ бит), *килобит* ($1024=2^{10}$ бит), *килобайт* ($8192=2^{13}$ бит), *мегабит* ($1048576=2^{20}$) и т.д.

Информационная мера Шеннона. Недостаток меры Хартли проявляется в том, что она не зависит от статистической структуры реального ИДС; она основана на равновероятных возможностях. Реальные ИДС вырабатывают символы с разной вероятностью, т.е. символы сообщения случайны, а вероятности различных возможностей не равны друг другу. Если, как и раньше, число возможностей равно M, можно рассматривать случайную величину A, принимающую одно из M значений. Тогда ИДС характеризуется одномерным законом распределения вероятностей. Причем вероятности $p(a_j) = p_j,\ j = \overline{0, M-1}$, этих значений неотрицательны и удовлетворяют условию нормировки:

$$\sum_{j=0}^{M-1} p(a_j) = \sum_{j=0}^{M-1} p_j = 1.$$

Рассматривая a_j как одно из M возможных состояний ИДС, Клод Шеннон определил меру её априорной неопределенности как логарифм величины, обратной вероятности её реализации:

$$H(a_j) = H_j = \log_b \frac{1}{p(a_j)} = -\log_b p_j,\ j = \overline{0, M-1}.$$

Тем самым приписывается определенное значение энтропии каждой реализации ДС A. Поскольку A - случайная величина, то эту энтропию можно рассматривать как случайную величину с тем же законом распределения вероятностей.

Апостериорная энтропия, имеющаяся после наблюдения реализации a_j в идеальной СПИ равна нулю. Поэтому *собственная информация*, получаемая при наблюдении реализации a_j, численно равна априорной (первоначальной) энтропии:

$$I_j = H_j = -\log_b p_j,\ j = \overline{0,M-1};$$

она, зависит от вида реализации a_j сообщения A и является случайной величиной. Очевидно, что информация и энтропия велики, когда априорная вероятность мала, и наоборот. Это вполне согласуется с интуитивными представлениями. Так достоверное событие с $p_j = 1$ не приносит информации: $I_j = 0$.

Энтропия источника независимых дискретных сообщений. В теории большую роль играет не случайная энтропия (соответственно, информация), но *средняя энтропия* $H(A)$, определяемая формулой

$$H(A) = \mathrm{M}\{H(a_j)\} = \overline{H_j} = \sum_{j=0}^{M-1} p_j \log_b \frac{1}{p_j} = -\sum_{j=0}^{M-1} p_j \log_b p_j,$$

где M – знак математического ожидания, её называют *шенноновской энтропией*.

Свойства энтропии

Энтропия неотрицательна: $H(A) \geq 0$**. Равенство нулю достигается тогда, когда одна из вероятностей равна единице:** $p_l = 1$**, а остальные равны нулю:** $p_i = 0, i \neq l$**.** Так, рассматривая компоненты $-p_j \log_b p_j$, имеем: при $p_l = 1$, $-1 \cdot \log_b(1) = 0$; при $p_l = 0$, величина $-0 \cdot \log_b(0) = 0 \cdot \log_b(\infty)$ представляет собой неопределенность типа $0 \cdot \infty$. Для раскрытия её воспользуемся правилом Лопиталя. В результате получаем

$$-\lim_{p \to 0} p \ln p = -\lim_{p \to 0} \frac{\ln p}{1/p} = -\lim_{p \to 0} \frac{\partial[\ln p]/\partial p}{\partial[[1/p]]/\partial p} = -\lim_{p \to 0} \frac{1/p}{-1/p^2} = \lim_{p \to 0} p = 0$$

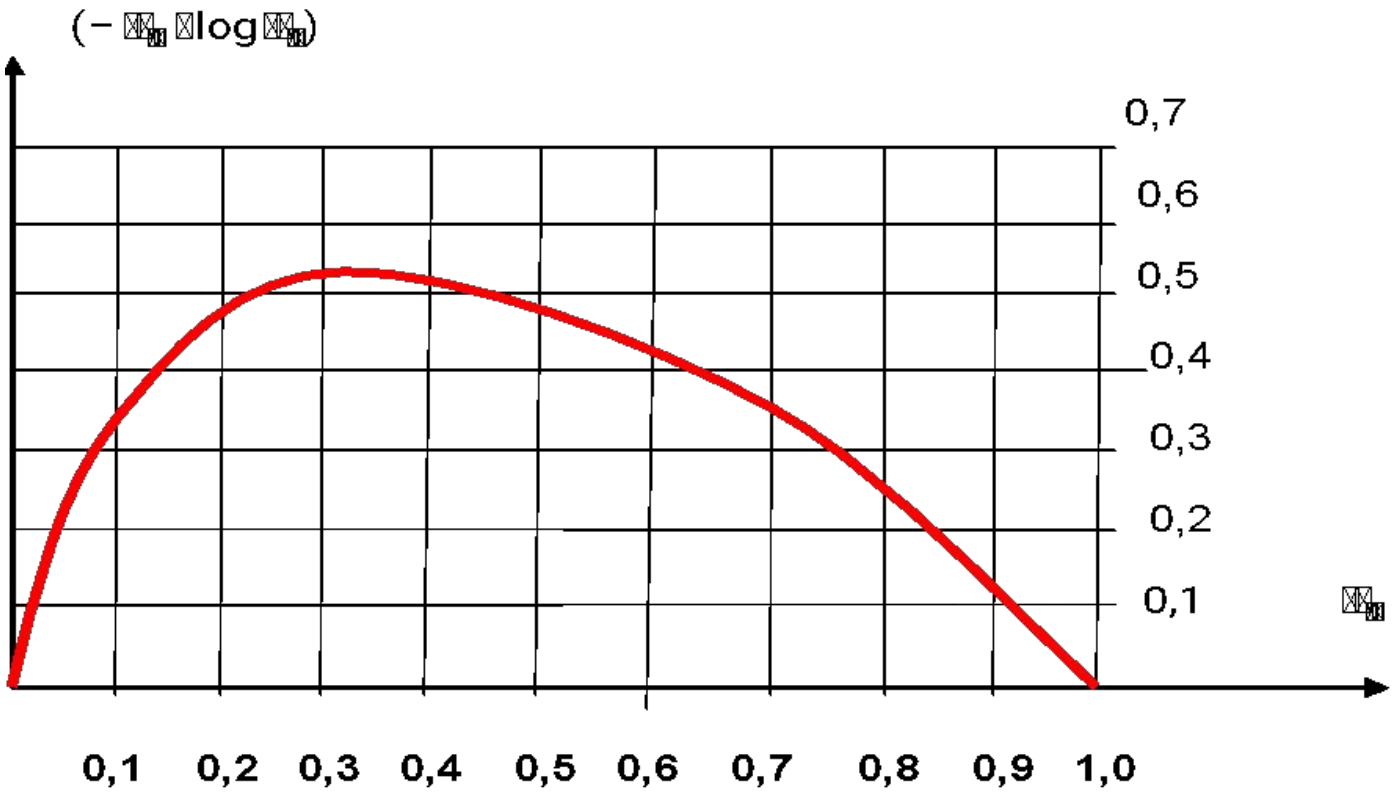
. Отсюда $0 \cdot \log_b(\infty) = 0$.

Величина $(-p_i \log p_i)$ **принимает максимальное значение при** $p_i = e^{-1}$. Докажем.

$$\frac{d}{dp_i}(-p_i \log p_i) = -\log p_i - \log e = -\log p_i - \log e = 0 .$$

Следовательно, $p_i \log e = 1$, а $p_i = e^{-1}$. Построим график зависимости $(-p_i \log p_i)$ от p_i. Максимум равен

$$(-p_i \log p_i) = p_i \log \frac{1}{p_i} = e \log \frac{1}{e} = 0{,}531$$



Энтропия максимальна и равна $H_{\max} = \log_b M$. Для доказательства этого воспользуемся методом неопределенных множителей Лагранжа. С учетом условия нормировки, при $b = e$, найдем экстремум функционала следующего вида

$$\psi(p_0, p_1, \ldots, p_{m-1}) = -\sum_{l=0}^{M-1} p_l \ln(p_l) + \lambda \sum_{l=0}^{M-1} p_l .$$

Дифференцируя по p_l, и приравнивая производные нулю, получаем

$$\frac{\partial}{\partial p_l}\psi(\cdot) = \frac{\partial}{\partial p_l}\left[-p_l \ln(p_l) + \lambda p_l\right] = \left[-\ln(p_l) - 1 + \lambda\right] = 0,\ p_l = \overline{0, M-1},$$

Отсюда следует, что $\ln(p_l) = (\lambda - 1) = const, \forall p_l$ или $p_l = p = 1/M$. Подставляя эту величину с учетом условия нормировки закона распределения вероятностей получаем максимум энтропии

$$H_{\max} = \log_b(1/p)\sum_{l=0}^{M-1} p_l = \log_b M .$$

$H(A) \le \log_b M$. Действительно, примем $b = e$ и рассмотрим разность:

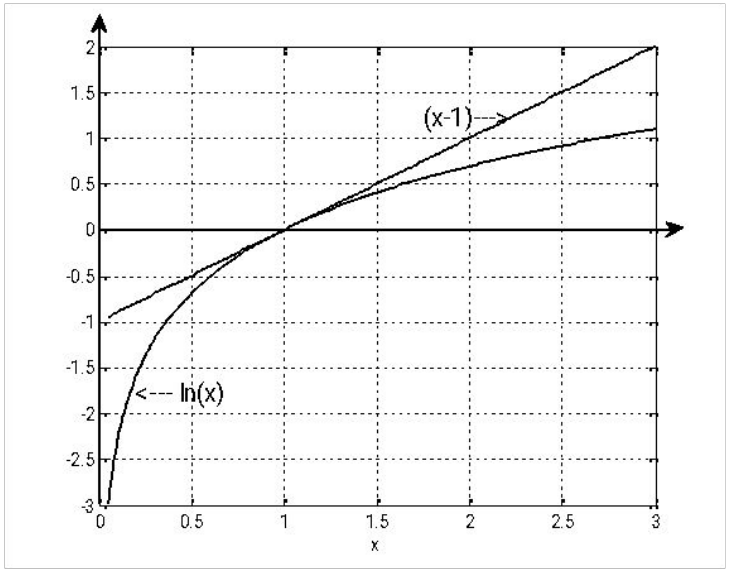


График логарифмической зависимости

$$H(A) - \ln M = \sum_j p_j \ln \frac{1}{p_j} - \sum_j p_j \ln M = \sum_j p_j \ln \frac{1}{p_j M}$$

.

Обозначив $x = 1/p_j M$, и используя неравенство $\ln x \le x - 1$, (см. рисунок), получаем

$$H(A) - \ln M \le \sum_j p_j \left(\frac{1}{p_j M} - 1 \right) = \left(\sum_j \frac{1}{M} - \sum_j p_j \right)$$

$$= (1 - 1) = 0.$$

Равенство имеет место только тогда, когда символы ансамбля $[A, P]$ равновероятны, т.е.

$p_l = 1/M$, $l = \overline{0, M-1}$.

Информационные меры Хартли и Шеннона совпадают тогда, когда ИДС бернулиевский с равномерным законом распределения вероятностей. Это следует из подстановки $A_k = A$, когда имеем

$$H_{\max}(A_1, A_2, \ldots, A_n) = \sum_{k=1}^{n} H_{\max}(A) = n \cdot \log_b M = \log_b M^n = \log_b M_0,$$

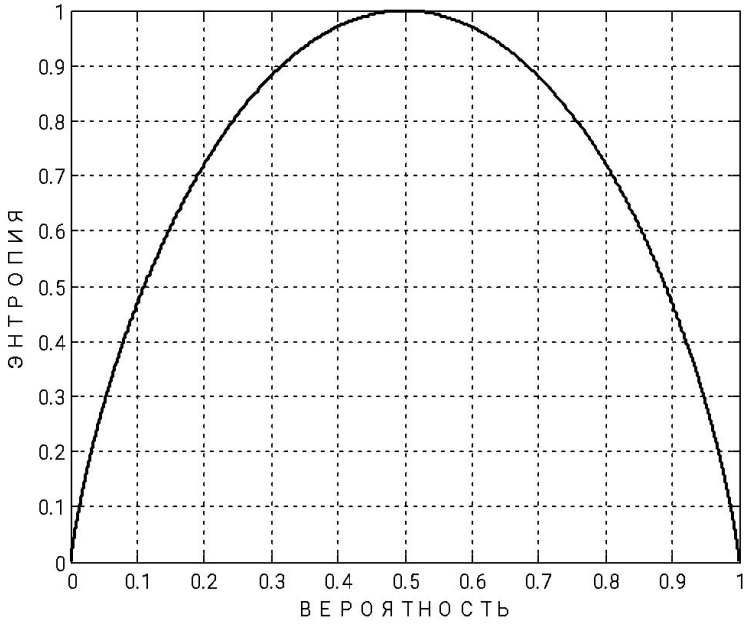
Аддитивное свойство энтропии. Если ансамбли $[A_k, P_k]$, $k = \overline{1,n}$, независимы, то энтропия $H(A_1, A_2, ..., A_n)$ совместного наступления n ДС распадается на сумму энтропий. Ввиду независимости ДС имеем: $P(A_1, A_2, ..., A_n) = \prod_{k=1}^{n} P(A_k)$. Поэтому получаем

$$H(A_1, A_2, ..., A_n) = -\mathrm{M}\left\{\log_b \prod_{k=1}^{n} P(A_k)\right\} = -\sum_{k=1}^{n} \mathrm{M}\{\log_b P(A_k)\} = \sum_{k=1}^{n} H(A_k).$$

Энтропия двоичного ансамбля. Пусть $m = 2$, $p_0 = p, p_1 = (1-p)$. Тогда

$$H(A) = -p\log_2 p - (1-p)\log_2(1-p).$$

На рисунке показана зависимость энтропии H от вероятности p двоичного ансамбля. Видно, что $H = 0$ при $p = 0$ и $p = 1$; $H_{\max} = \log_2 2 = 1$ достигается при $p = 1/2$. Размерность энтропии: [бит/символ].



На практике встречаются ИДС, представляющие собой последовательность n *взаимно зависимых* дискретных случайных величин $A_k, k=\overline{1,n}$. Если зависимость распространяется только *на каждую пару* случайных величин, то последовательность, называется *простой марковской*, а источник *марковским*. Энтропию марковского ИДС можно представить в виде:

$$H(AB) = H(A) + H(B \mid A) = H(B) + H(A \mid B).$$

В этом проявляется свойство аддитивности энтропии источника ДС. При этом условная энтропия не может превосходить безусловную, т.е.

$$H(B \mid A) \le H(B).$$

Равенство $H(B \mid A) = H(B)$ достигается тогда и только тогда, когда события A и B - *статистически независимы*.

Удельная энтропия. Рассмотрим n-последовательность M - символьных случайных величин, вырабатываемую ИДС: $A_1^n = A_1, A_2, ..., A_n$. Энтропия этой последовательности - есть совместная энтропия $H(A_1^n)$ n одномерных ансамблей A. Тогда *удельная энтропия* или энтропия на сообщение равна

$$H_n(A) = H(A_1^n)/n.$$

Производительность и избыточность источника. Количество собственной информации, вырабатываемое ИДС в единицу времени, называют *производительностью источника*:

$$I'(A) = \frac{I(A,A)}{T} = \frac{I(A)}{T} = \frac{H_{IDS}}{T}.$$

Если энтропия ИДС измеряется в битах, то размерность $I'(A)$ [бит/с]. Величину $I'(A)$ называют еще *скоростью ввода информации в канал связи*.

Отношение производительности ИДС к её максимальной величине называют *информационной насыщенностью*

$$I_{ns} = \frac{I'(A)}{I'_{\max}} = \frac{H_{IDS}}{\log_b M} \le 1.$$

Избыточность источника определяется так

$$r = 1 - I_{ns} = \frac{H_{\max} - H_{IDS}}{H_{\max}} \ge 0;$$

она характеризует степень использования информационной емкости ИДС.

Энтропия непрерывного ансамбля. Для аналогового или непрерывного сообщения (НС), как случайного процесса, использование приведенных выше определений информационных характеристик для ДС осложняется тем, что вероятность его конкретной реализаций бесконечно мала, а, следовательно, неопределенность или энтропия её бесконечно велика. В этом случае энтропия равна:

$$H(A) = \log_b \frac{1}{\Delta x \to 0} + \left\{ - \int_{-\infty}^{\infty} W_A(x) \cdot \log_b W_A(x) dx \right\} = \infty + h(A),$$

где $W_A(x) = dF_A(x)/dx$ - функция плотности вероятности, а $F_A(x) = p\{A \le x\}$ функция распределения вероятностей. Величина

$$h(A) = - \int_{-\infty}^{\infty} W_A(x) \log_b W_A(x) dx = \mathrm{M}\left\{ \log_b \frac{1}{W_A(x)} \right\};$$

называется *дифференциальной энтропией* и она является средним значением (математическим ожиданием) случайной величины

$$h(x) = -\log_b W_A(x) = \log_b \left[1/W_A(x) \right].$$

В отличие от информационной меры Шеннона для ДС величина $h(x)$ для НС не обладает многими свойствами, присущими информации. Она, например, может принимать отрицательные значения при $W_A(x) > 1$; зависит от масштаба x, а значит, от выбора единиц измерения.

Для непрерывного ансамбля выполняется условие нормировки ФПВ, а именно:

$$\int_{-\infty}^{\infty} W_{xx}(x)\,dx = 1$$

Рассмотрим два случая, когда дисперсия состояний элементов непрерывного сообщения величина заданная, т.е.:

$$\int_{-\infty}^{\infty} x^2 W_{xx}(x)\,dx = \sigma^2 = \text{const}$$

и когда дисперсия не ограниченна.

Можно показать, что сообщение обладает максимальной информативностью, если в первом случае ФПВ имеет нормальное центрированное распределение

$$W_{xx}(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}$$

а во втором энтропия максимальна, когда состояния элементов сообщения распределены по равномерному (равновероятному) закону:

$$W_{xx}(x) = \frac{1}{B - A}$$

где B и A определяют границы интервала, в котором существуют элементы сообщений.

Основы теории кодирования дискретных сообщений

Кодирование – это отображение элементов одного множества элементами другого. При этом правила такого отображения должны быть известны и для обратного преобразования.

В общей теории связи различают следующие виды кодирования: *примитивное*, *эффективное* (статистическое) и *корректирующее* (помехоустойчивое).

Примитивное кодирование (его еще называют *первичным кодированием*) связано с представлением сообщений в виде чисел в той или иной системе счисления. В современных цифровых СПИ часто применяют представление чисел в *двоичной* системе счисления. В рекуррентной форме:

$$N_q = \pm \sum_{i=-m}^{n-1} a_i q^i,$$

где N_q - представляемое число, q - основание системы счисления, a_i - разрядный коэффициент, изменяющийся от 0 до $q-1$. Величина i является номером разряда, n - число целых разрядов, m - число дробных разрядов.

В десятичной системе счисления, когда $q = 10$ данная формула может быть записана следующим образом:

$$N_{10} = \pm \sum_{i=-m}^{n-1} a_i \cdot 10^i,$$

где $a = 0, 1, 2, 3\ldots, 9$.

В двоичной системе счисления, когда $q = 2$, формула примет вид:

$$N_2 = \pm \sum_{i=-m}^{n-1} a_i \cdot 2^i$$

где a = 0, 1.

Достаточно широко при компьютерной обработке информации применяются восьмеричная и шестнадцатеричная системы счисления, которые используются, например, для обозначения адресов расположения данных в памяти компьютера и т. д. Для восьмеричной и шестнадцатеричной системы счисления $q = 8$ и $q = 16$ соответственно, Тогда имеем:

$$N_8 = \pm \sum_{i=-m}^{n-1} a_i \cdot 8^i$$

где a = 0, 1, 2, 3…, 7.

$$N_{16} = \pm \sum_{i=-m}^{n-1} a_i \cdot 16^i$$

где *a* = 0, 1, 2, 3…, 9, A, B, C, D, E, F.

Пример:

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Пусть [illegible] ансамбль сообщений, наблюдаемый на выходе источника ДС. Требуется подобрать такой *эффективный* код, который максимально устраняет избыточность ДС или приводит к минимально возможному объему цифрового представления ДС по сравнению с примитивным кодированием (*максимальному сжатию данных*). *Теоретической основой эффективного кодирования* является **первая теорема Шеннона** (**основная теорема кодирования для канала без шума**), согласно которой при любой статистике источника ДС существует код по основанию [illegible], позволяющий при отсутствии ограничений на задержку получить среднее число $\bar{n} = \mathrm{M}\{n_i\}$ кодовых символов на элемент сообщения, сколь угодно близкое к минимально возможному значению

$$[illegible] = \frac{[illegible]}{\log [illegible]}$$

или иначе, каким бы ни был источник ДС с энтропией $H(A) < \infty$, всегда существует такой способ кодирования сообщений, для которого выполняется условие:

$$\bar{n} = n_{\min} + \varepsilon,$$

где $\varepsilon > 0$ - сколь угодно малая величина, взятая "для перестраховки", потому что имеем дело со случайными последовательностями.

Метод укрупнения алфавита. Пусть 10-ичный источник создает последовательности цифр: ...3, 1, 5, 7, 9, 8, 0, 2, ... и пусть очередная цифра выбирается независимо от предыдущей с одинаковой вероятностью 1/10 (поскольку цифр всего 10). Если применять примитивное двоичное кодирование, то каждая десятичная цифра заменяется $\lceil \log_2 10 \rceil = 4$ символьной двоичной комбинацией. Для передачи N десятичных цифр придется израсходовать $4N$ двоичных символов. Однако энтропия источника ДС в данном случае $H(A) = \log_2 10 \approx 3.32$ и в соответствии с первой теоремой Шеннона должен существовать код с $\bar{n} \approx 3.32$. Найдем его, укрупняя алфавит. Для этого разобьем десятичную последовательность на пары цифр: ...31, 57, 38, 02, 10, 47,11, 25, и каждую пару будем примитивно кодировать как единый символ нового, большего по мощности, алфавита. Поскольку таких разных пар будет 100, то понадобятся $\lceil \log_2 100 \rceil = 7$ -ми символьные двоичные кодовые комбинации. При этом на одну десятичную цифру будет расходоваться уже 7/2=3.5 двоичных символов.

Этот процесс можно продолжить и попытаться кодировать тройки десятичных цифр: ...315, 798, 021, 047, 112, 5.... и т.д. Постепенно мы приблизимся к теоретически достижимому пределу. Однако при этом растет задержка и ухудшается помехоустойчивость.

Методы статистического кодирования. При статистическом двоичном кодировании элементов ДС используются кодовые комбинации разной длины. Причем более вероятным элементам ДС, приписываются более короткие кодовые комбинации. Наибольшее снижение избыточности достигается кодированием по методу *Фано-Шеннона* или *Хаффмана*. Рассмотрим пример построения неравномерного кода по методу Хаффмана, имеющего более общий алгоритм.

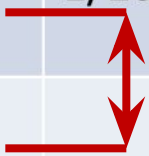
Поясним сказанное на примере двоичного кодирования (ансамбля $[A, P(A)]$, характеризуемого 8-ью сообщениями $\square_0, \square_1, \ldots \square_7$ и соответственно вероятностями их появления $\square(\square_0) = 1/2, \square(\square_1) = \square(\square_2) = 1/8, \square(\square_3) = \square(\square_4) = \square(\square_5) = 1/16, \square(\square_6) = \square(\square_7) = 1/32$.

- на 1-ом этапе объединяются два наименее вероятных события в одно составное (с суммарной вероятностью объединяемых событий), располагаемого также в порядке убывания вероятностей нового ансамбля с числом элементов на единицу меньшим;
- на 2-ом и последующих этапах процедура 1-го этапа повторяются до тех пор, пока суммарная вероятность составного события не достигнет единицы;
- на каждом этапе строится сигнальный граф, содержащий две ветви по числу объединяемых событий и узел, характеризующий составное событие;
- кодирование осуществляется, начиная с конечного узла, имеющего вероятность 1, и заканчивается в начале графа, с присваиванием кодового символа 1, если в каждом узле идти к верхней ветви и 0, если идти к нижней ветви. Подсчет единиц и нулей (в каждом промежуточном узле) при переходе от конца графа к L его начальным узлам определяют искомые кодовые комбинации кода Хаффмана.

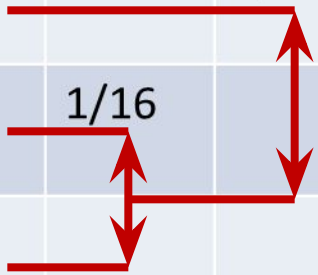
		A								
		a_0								
		a_1								
		a_2								
		a_3								
		a_4								
		a_5								
		a_6								
		a_7								

	p(A)	A								
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5								
	1/32	a_6								
	1/32	a_7								

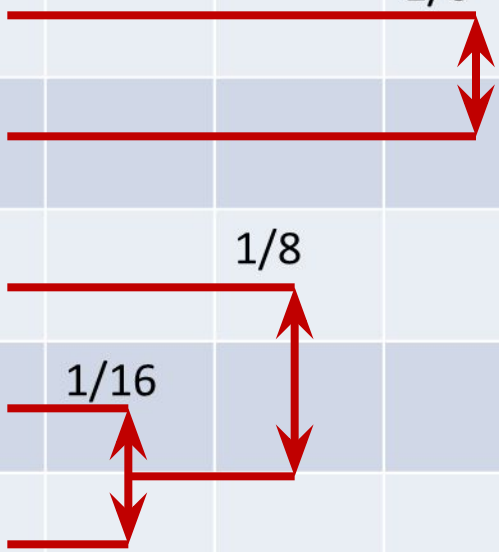
	p(A)	A	Шаг 1							
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5								
	1/32	a_6	1/16							
	1/32	a_7								



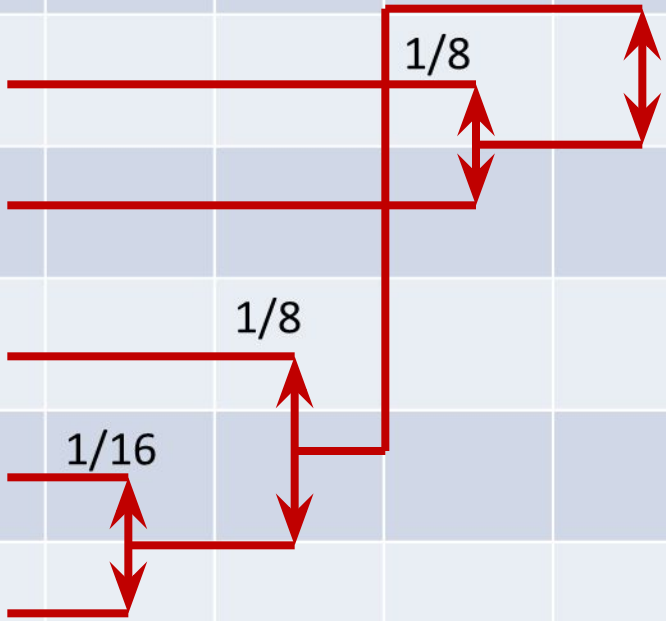
	p(A)	A	Шаг 1	Шаг 2						
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5		1/8						
	1/32	a_6	1/16							
	1/32	a_7								



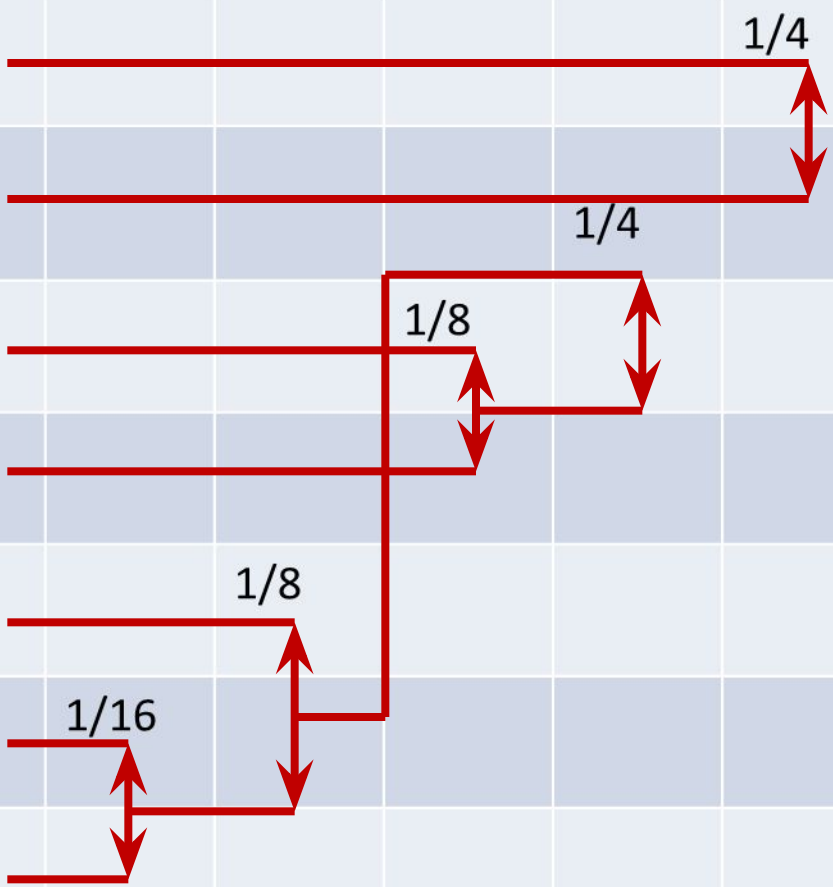
	p(A)	A	Шаг 1	Шаг 2	Шаг 3					
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3			1/8					
	1/16	a_4								
	1/16	a_5		1/8						
	1/32	a_6	1/16							
	1/32	a_7								



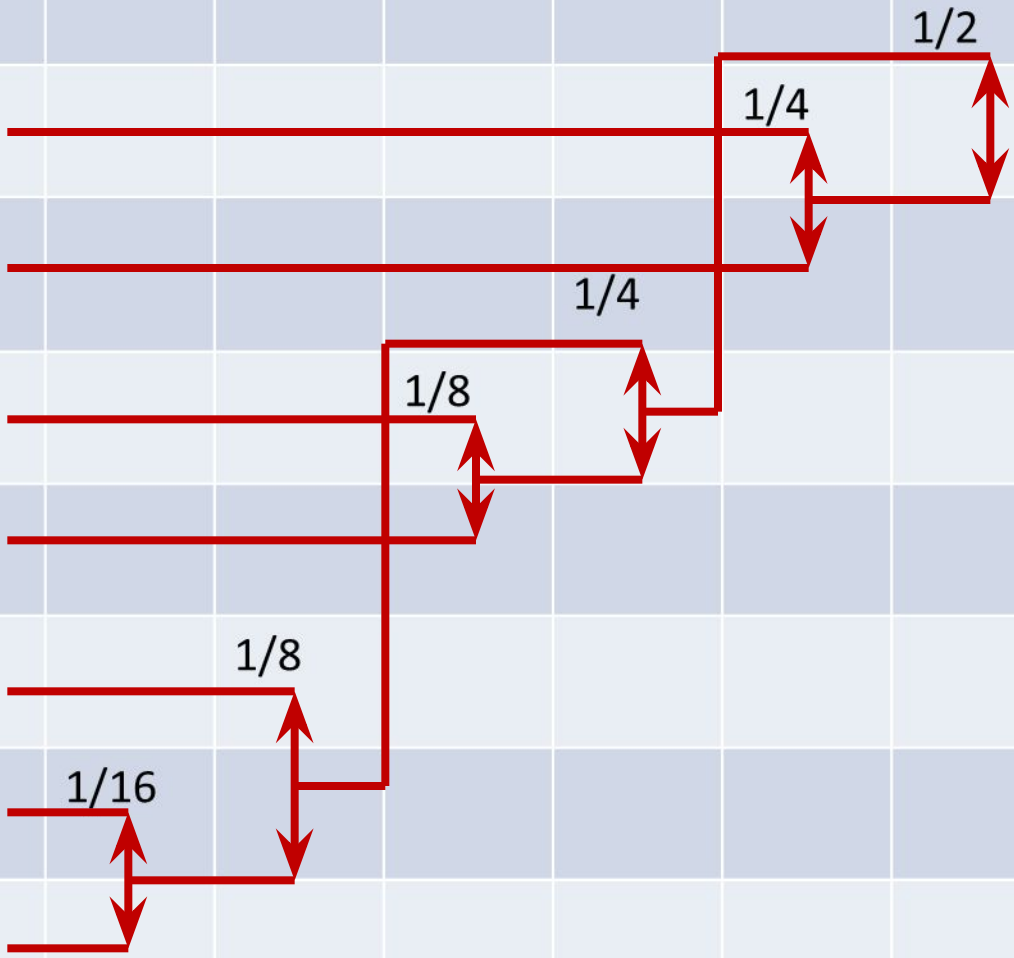
	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4				
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5								
	1/32	a_6								
	1/32	a_7								



	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4	Шаг 5			
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5								
	1/32	a_6								
	1/32	a_7								

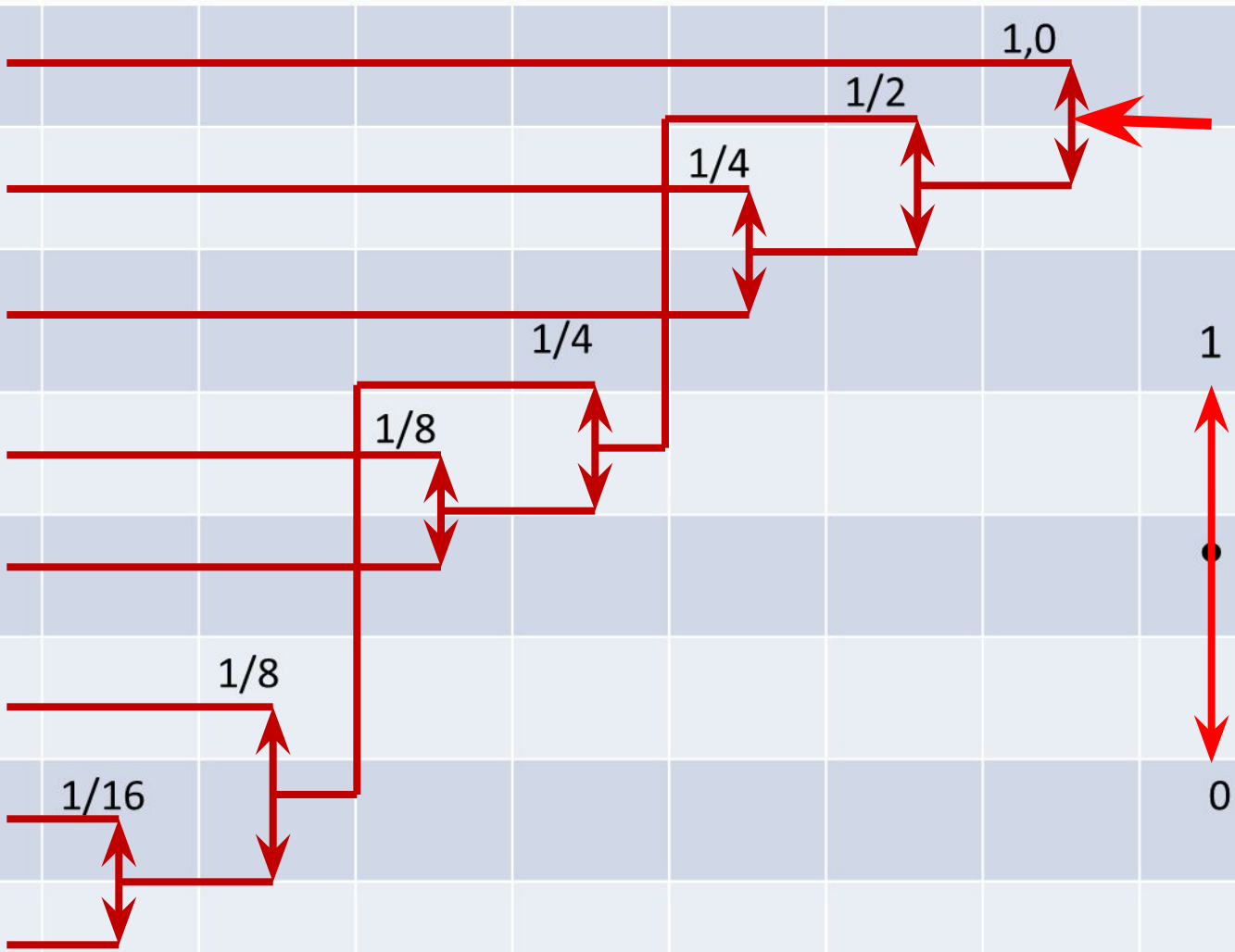


	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4	Шаг 5	Шаг 6		
	1/2	a_0								
	1/8	a_1								
	1/8	a_2								
	1/16	a_3								
	1/16	a_4								
	1/16	a_5								
	1/32	a_6								
	1/32	a_7								

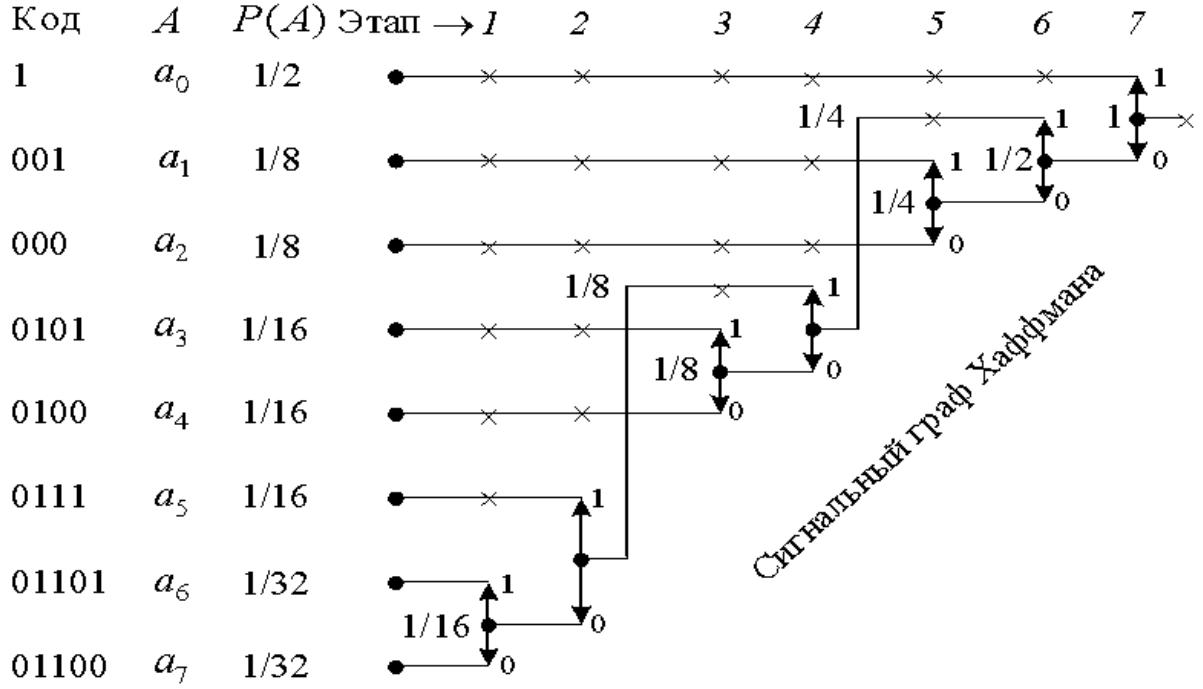


	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4	Шаг 5	Шаг 6	Шаг 7	
	1/2	a_0							1,0	
	1/8	a_1						1/2		
	1/8	a_2					1/4			
	1/16	a_3				1/4				
	1/16	a_4			1/8					
	1/16	a_5		1/8						
	1/32	a_6	1/16							
	1/32	a_7								

	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4	Шаг 5	Шаг 6	Шаг 7	Старт
	1/2	a_0							1,0	
	1/8	a_1						1/2		
	1/8	a_2					1/4			
	1/16	a_3				1/4				1
	1/16	a_4			1/8					
	1/16	a_5		1/8						
	1/32	a_6	1/16							0
	1/32	a_7								



Код	p(A)	A	Шаг 1	Шаг 2	Шаг 3	Шаг 4	Шаг 5	Шаг 6	Шаг 7	Старт
1	1/2	a_0							1,0	
001	1/8	a_1						1/2		
000	1/8	a_2					1/4			
0101	1/16	a_3				1/4				1
0100	1/16	a_4			1/8					•
0111	1/16	a_5		1/8						
01101	1/32	a_6	1/16							0
01100	1/32	a_7								



Сигнальный граф эффективного кодирования по Хаффману

Неравномерный код обладает высокой скоростью кодирования, но имеет худшую помехоустойчивость по сравнению с равномерным кодом, а так же более сложную реализацию. Следует так же отметить неравномерность задержки, что так же усложняет восстановление исходного сообщения.

Сообщ.	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
Хаффм	1	001	000	0101	0100	0111	01101	01100
Натур.	000	001	010	011	100	101	110	111

Декодируем последовательность:

…0100111100100101010101000111011011011001101000001001010 0…

По **Хаффману**:

$$\ldots x_2; x_3; x_0; x_0; x_1; x_1; x_2; x_0; x_2; x_0; \ldots$$

Натуральный (взвешенный) код:

- необходимо обеспечить обнаружение начало кодовых комбинаций и только потом декодирование:

$$\ldots x_2; x_3; x_6; x_2; x_2; x_5; x_2; x_4; x_3; x_5; \ldots$$

Неравенство **Крафта-Макмиллана** устанавливает, что при заданных кодируемом и кодирующем алфавитах, состоящих соответственно из n и d символов, а так же заданных желаемых длин кодовых слов: $\ell_1, \ell_2, \ldots, \ell_n$, необходимым и достаточным условием существования разделимого и префиксного кодов, обладающих заданным набором длин кодовых слов является выполнение неравенства:

$$\sum_{i=1}^{n} d^{-\ell_i} \leqslant 1.$$

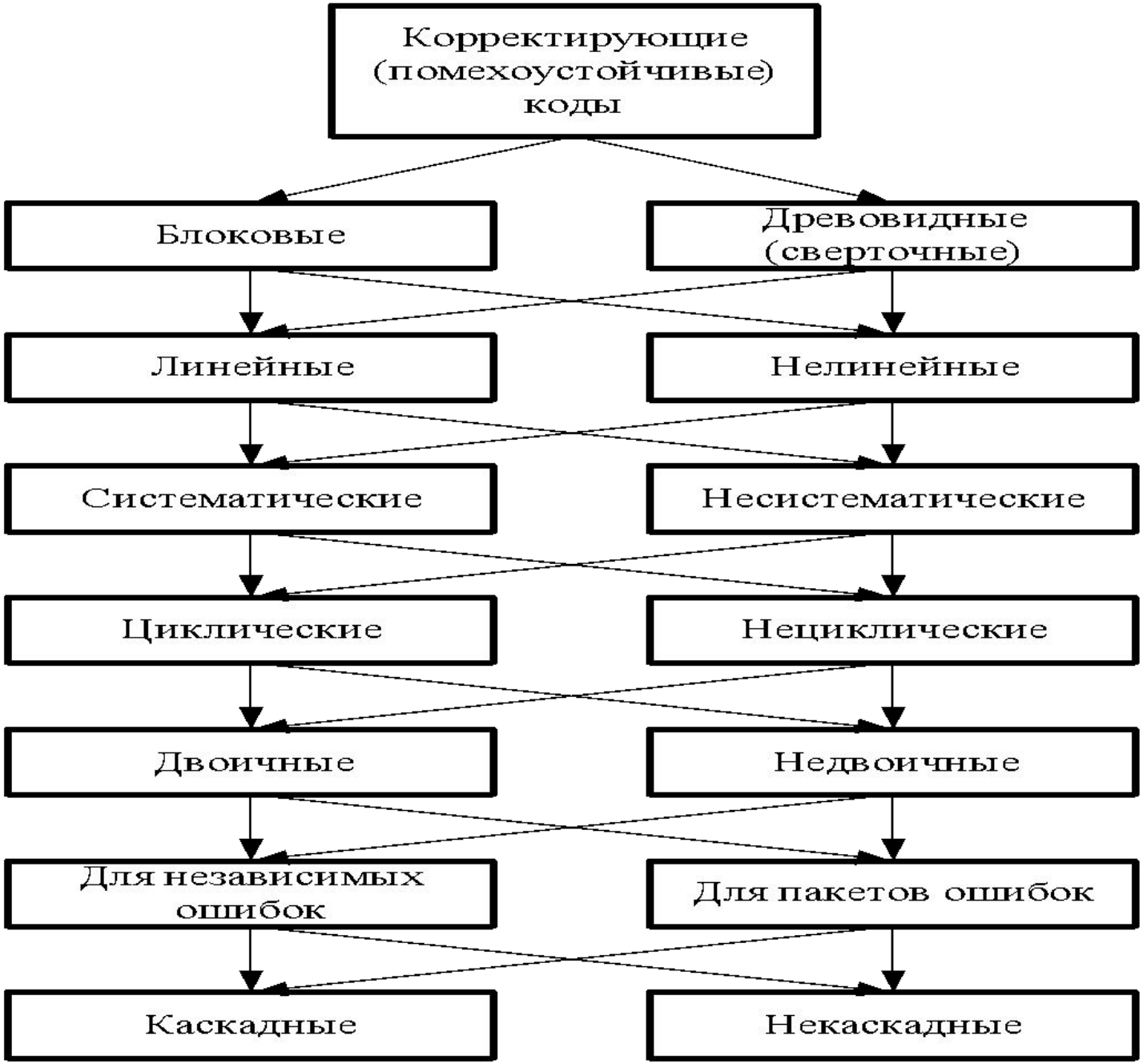
Генетический код

1-е положение		2-е положение U		2-е положение C		2-е положение A		2-е положение G		3-е положение
		UUU	Phe	UCU	Ser	UAU	Tyr	UGU	Cys	U
		UUC	Phe	UCC	Ser	UAC	Tyr	UGC	Cys	C
		UUA	Leu	UCA	Ser	UAA	ochre	UGA	opal	A
	U	UUG	Leu	UCG	Ser	UAG	amber	UGG	Try	G
		CUU	Leu	CCU	Pro	CAU	His	CGU	Arg	U
		CUC	Leu	CCC	Pro	CAC	His	CGC	Arg	C
		CUA	Leu	CCA	Pro	CAA	Gln	CGA	Arg	A
	C	CUG	Leu	CCG	Pro	CAG	Gln	CGG	Arg	G
		AUU	Ile	ACU	Thr	AAU	Asn	AGU	Ser	U
		AUC	Ile	ACC	Thr	AAC	Asn	AGC	Ser	C
		AUA	Ile	ACA	Thr	AAA	Lys	AGA	Arg	A
	A	AUG*	Met	ACG	Thr	AAG	Lys	AGG	Arg	G
		GUU	Val	GCU	Ala	GAU	Asp	GGU	Gly	U
		GUC	Val	GCC	Ala	GAC	Asp	GGC	Gly	C
		GUA	Val	GCA	Ala	GAA	Glu	GGA	Gly	A
	G	GUG*	Val	GCG	Ala	GAG	Glu	GGG	Gly	G

Триплетные комбинации азотистых оснований мРНК: тимин, цитозин, аденин, гуанин (U, C, A, G) определяют следующие аминокислоты: **Phe** – фениланин, **Leu** – лейцин, **Ile** – изолейцин, **Met** – метионин, **Val** – валин, **Ser** – серин, **Pro** – пролин, **Thr** – треонин, **Ala** – аланин, **Tyr** – тирозин, **His** – гистидин, **Gln** – глутамин, **Asn** – аспарагин, **Lys** – лизин, **Asp** – аспарагиновая кислота, **Glu** – глутаминовая кислота, **Cys** – цистеин, **Try** – триптофан, **Arg** – аргинин, **Gly** – глицин.

Звездочкой обозначены стартовые кодоны, а триплеты **ochre, amber, opal** действуют как стоп кодоны.

(по F. Crick)


Корректирующие (помехоустойчивые) коды
Блоковые
Древовидные (сверточные)
Линейные
Нелинейные
Систематические
Несистематические
Циклические
Нециклические
Двоичные
Недвоичные
Для независимых ошибок
Для пакетов ошибок
Каскадные
Некаскадные

Коды делятся на *линейные* и *нелинейные*. Кодовые комбинации линейных корректирующих кодов отображаются точками (векторами) линейного пространства с присущей ему аксиоматикой. Практически все известные схемы корректирующего кодирования основаны на линейных кодах.

Различают *разделимые* и *неразделимые* корректирующие коды. В разделимых кодах всегда можно выделить информационные символы, содержащие передаваемую информацию, и контрольные символы, которые являются избыточными и служат исключительно для коррекции ошибок, вносящих каналом связи (линейные блочные коды). Неразделимые коды не имеют четкого разделения кодовой комбинации на информационные и контрольные символы. К ним относятся коды с постоянным весом и коды Плоткина. Разделимые блочные коды, в свою очередь, делятся на *систематические и несистематические*. В систематическом коде позиции занимаемые информационными и проверочными кодовыми символами строго упорядочены. Причем в линейных систематических кодах проверочные символы образуются как линейные комбинации от информационных символов. Систематические коды более удобны на практике, чем несистематические коды, у которых в комбинациях не содержатся в явном виде информационные символы. К систематическим кодам относятся: коды с проверкой на четность, коды с повторением, корреляционные, инверсные и итеративные коды, коды Хэмминга, Голея, Рида-Маллера, Маклональда, Варшамова и другие.

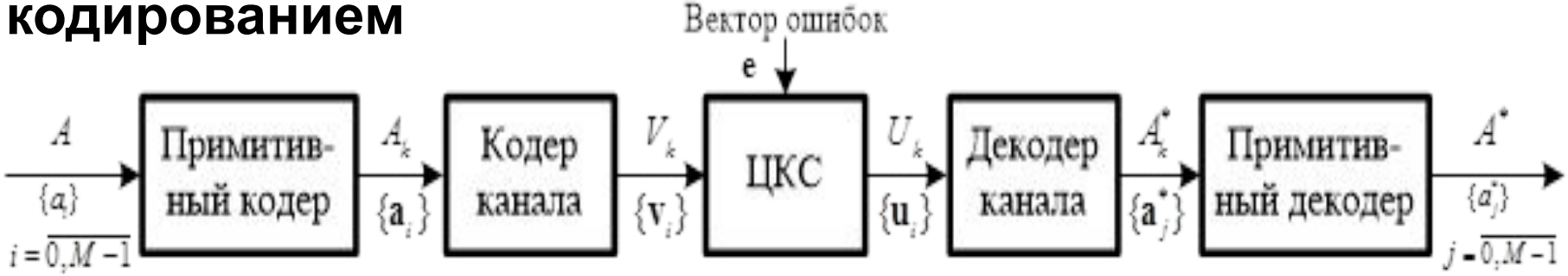
Разновидностью систематических кодов являются *циклические коды*. Кроме всех свойств систематического кода, циклические коды имеют следующее свойство: если некоторая кодовая комбинация принадлежит коду, то получающаяся путем циклической перестановки символов новая комбинация также принадлежит данному коду. К наиболее известным циклическим кодам относятся следующие коды: коды Хэмминга, Боуза-Чоудхури-Хоквингема, Файра, Абрамсона, Миласа-Абрамсона, Рида-Соломона мажоритарные, компаундные коды и др.

В зависимости от основания кода все *коды* разделяются на *двоичные* (m=2) и *недвоичные* (m>2).

Корректирующие коды можно разбить на коды *исправляющие* случайные и *независимые ошибки* и коды, *исправляющие пакеты ошибок*. На практике, в основном, применяются коды, исправляющие случайные ошибки, поскольку для исправления пакетов ошибок часто оказывается легче использовать коды для исправления независимых ошибок с устройствами перемежения и восстановления. Первое из них осуществляет перемешиванием порядка следования символов в закодированной последовательности перед передачей в канал, а второе – восстановление исходного порядка символов после приема. При правильном проектировании данных устройств можно считать, что образующиеся в канале связи пакеты ошибок перед декодированием будут разбиты на случайные ошибки.

Важным этапом в развитии теории корректирующего кодирования является создание *каскадных кодов*, в основе построения которых лежит идея совместного использования не одного, но нескольких кодов. Эффективность каскадного кода выше, чем одного кода. Так кодовое расстояние кода из последовательного соединения двух кодов равно произведению кодовых расстояний каждого из его составляющих кодов.

Простейшая система передачи информации с кодированием



Элемент ДС $a_i \in A, i = \overline{0, M-1}$, отождествляется с его индексом i, который в примитивном кодере представляется так: $i = \sum_{j=0}^{k-1} \alpha_j m^j$, где k- длина кодовой комбинации

$$\mathbf{a}_i = (\alpha_0, \alpha_1, \ldots \alpha_j \ldots \alpha_{k-1})_i,$$

α_0 – младший, α_{k-1}- старший разряды. Например, при $m = 2$, $i = 21$, $k = 5$, $\mathbf{a}_{21} \Rightarrow (10101)$ (Часто кодовую комбинацию примитивного кода начинают не с младшего, а со старшего разряда; тогда кодовую комбинацию будем записывать в виде: $\mathbf{a}_i = (\alpha_{k-1}, \ldots \alpha_j \ldots \alpha_1, \alpha_0)_i$.)

Далее k-значная *кодовая комбинация* $\mathbf{a}_i$ (в дальнейшем просто *комбинация*) подается на вход кодера канала, в котором по определенному правилу формируется n-значная комбинация вида

$$\mathbf{v}_i = (v_0, v_1, \ldots v_l \ldots v_{n-1})_i, \quad l = \overline{0, n-1}, \quad n > k.$$

Совокупность комбинаций $\{\mathbf{v}_i\}, i=\overline{0,M-1}$- *образует корректирующий* (помехоустойчивый) *код*, обладающий избыточностью $r_k=(n-k)/n$, так как из общего числа возможных n-значных комбинаций $N_0=m^n$, в ЦКС могут передаваться только $M=m^k$ *разрешенных*. Остальные комбинации, число которых $N_z=N_0-M$, образуют область запрещенных, не передаваемых по ЦКС.

Итак, *код относится к классу корректирующих кодов*, если выполняются условия:

$$M<N_0,$$

$$d_{\min}>1,$$

где $d_{\min}$- кодовое расстояние кода, равное минимальному расстоянию по Хеммингу между различными комбинациями кода $\{\mathbf{v}_i\}, i=\overline{0,M-1}$.

В цифровом канале связи (ЦКС) на любую переданную (разрешенную) комбинацию накладывается вектор (комбинация) ошибок $\mathbf{e}$. Тогда на вход декодера канала поступает комбинация вида

$$\mathbf{u}=\mathbf{v}_i \oplus_m \mathbf{e},$$

где $\oplus_m$ - знак суммирования по модулю m.

В декодере канала решаются две задачи: декодирование с обнаружением ошибок и декодирование с исправлением ошибок.

При декодировании с обнаружением ошибок, т.е. констатации факта их наличия в принятой комбинации $\mathbf{u}$, методом сопоставлений сравнивают принятую комбинацию с каждой из разрешенных, хранящихся в памяти декодера. Если принятая комбинация не совпадает ни с одной из разрешенных, следовательно, она относится к области запрещенных и тем самым обнаруживается наличие ошибок. Необнаруженная ошибка имеет место только в том случае, если помеха превратила переданную (разрешенную) комбинацию в другую разрешенную комбинацию данного кода.

При декодировании с исправлением ошибок множество $N_z = N_0 - M$ запрещенных комбинаций разбивают на M неперекрывающихся подмножеств, каждое из которых закрепляют за одной конкретной разрешенной комбинацией. Для подавляющего числа каналов связи наилучший результат получается при закреплении за разрешенной комбинацией тех запрещенных, которые наиболее ближе к ней в смысле расстояния Хемминга. При приеме кодовой комбинации $\mathbf{u}$ декодер путем метода сопоставлений выносит решение о том, что передавалась та комбинация из множества $\{\mathbf{v}_i\}$, до которой $\mathbf{u}$ ближе всего. Этот метод получил название, как *метод декодирования по минимуму расстояния*. Если комбинация $\mathbf{u}$ образовалась из подмножества, принадлежащих $\mathbf{v}_i$, то тем самым ошибки исправляются. В противном случае происходит ошибочное декодирование.

При использовании корректирующего кода обнаружить ошибочные комбинации можно в $M(N_0-M)$ случаях из $M(N_0-1)$ возможных. Из общего числа обнаруживаемых комбинаций исправляются только (N_0-M). Отсюда доля обнаруживаемых δ_{ob} и доля исправляемых δ_{is} декодером ошибочных комбинаций соответственно равны

$$\delta_{ob}=\frac{M(N_0-M)}{M(N_0-1)}=\frac{1-M/N_0}{1-1/N_0};\qquad \delta_{is}=\frac{(N_0-M)}{M(N_0-M)}=\frac{1}{M}.$$

Следует также отметить, что кодовое расстояние кода характеризует корректирующую способность кода, т.е. способность кода обнаруживать и исправлять ошибки различной кратности q, где под *кратностью ошибок* понимают общее число искаженных кодовых символов в принятой кодовой комбинации. Так, при $d_{\min}=1$ (примитивный код) достаточно однократной ошибки ($q=1$), чтобы переданная комбинация была принята неверно. Очевидно, для обнаружения всех однократных ошибок, $d_{\min}$ должно быть не менее двух.

Чтобы обнаружить ошибки кратности q_{ob} необходимо выполнить условие

$$d_{\min} \geq q_{ob} + 1 .$$

Для исправления ошибок кратности q_{is}, необходимо, чтобы принятая с ошибками комбинация оказалась ближе к исходной разрешенной, чем к другим разрешенным, т.е $q_{is} \leq 0.5 d_{\min}$. Отсюда для исправления ошибки кратности q_{is} справедливо условие

$$d_{\min} \geq 2q_{is} + 1 .$$

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000								
1	001								
2	010								
3	011								
4	100								
5	101								
6	110								
7	111								

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1						
1	001	1	0						
2	010								
3	011								
4	100								
5	101								
6	110								
7	111								

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1	1	2				
1	001	1	0	2	1				
2	010	1	2	0	1				
3	011	2	1	1	0				
4	100								
5	101								
6	110								
7	111								

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1	1	2	1	2	2	3
1	001	1	0	2	1	2	1	3	2
2	010	1	2	0	1	2	3	1	2
3	011	2	1	1	0	3	2	2	1
4	100	1	2	2	3	0	1	1	2
5	101	2	1	3	2	1	0	2	1
6	110	2	3	1	2	1	2	0	1
7	111	3	2	2	1	2	1	1	0

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	**0**	1	1	2	1	2	2	**3**
1	001	1	**0**	2	1	2	1	**3**	2
2	010	1	2	**0**	1	2	**3**	1	2
3	011	2	1	1	**0**	**3**	2	2	1
4	100	1	2	2	**3**	**0**	1	1	2
5	101	2	1	**3**	2	1	**0**	2	1
6	110	2	**3**	1	2	1	2	**0**	1
7	111	**3**	2	2	1	2	1	1	**0**

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1	1	2	1	2	2	3
1	001	1	0	2	1	2	1	3	2
2	010	1	2	0	1	2	3	1	2
3	011	2	1	1	0	3	2	2	1
4	100	1	2	2	3	0	1	1	2
5	101	2	1	3	2	1	0	2	1
6	110	2	3	1	2	1	2	0	1
7	111	3	2	2	1	2	1	1	0

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1	1	2	1	2	2	3
1	001	1	0	2	1	2	1	3	2
2	010	1	2	0	1	2	3	1	2
3	011	2	1	1	0	3	2	2	1
4	100	1	2	2	3	0	1	1	2
5	101	2	1	3	2	1	0	2	1
6	110	2	3	1	2	1	2	0	1
7	111	3	2	2	1	2	1	1	0

		0	1	2	3	4	5	6	7
		000	001	010	011	100	101	110	111
0	000	0	1	1	2	1	2	2	3
1	001	1	0	2	1	2	1	3	2
2	010	1	2	0	1	2	3	1	2
3	011	2	1	1	0	3	2	2	1
4	100	1	2	2	3	0	1	1	2
5	101	2	1	3	2	1	0	2	1
6	110	2	3	1	2	1	2	0	1
7	111	**3**	2	2	1	2	1	1	0

Пример:

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Корректирующий линейный код (КЛК)

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.
В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.
В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.
В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2\ 10^{-2} + 510^{-3}$.
В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Пример:
Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.
В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.
В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и
в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Пример:
Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.
В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.
В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и
в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Обнаружение и исправление ошибок

Пример:

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Пример:

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

- **Пример:**

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Код с двумя проверками на четность

Пример:

Двоичное число $K_2 = 11001{,}101 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0, +1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$.

В десятичной форме это же число равно $K_{10} = 25{,}125 = 2 \cdot 10^1 + 5 \cdot 10^0, +1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 510^{-3}$.

В восьмеричной - $K_8 = 31{,}5 = 3 \cdot 8^1 + 1 \cdot 8^0, +5 \cdot 8^{-1}$ и

в шестнадцатеричной - $K_{16} = 19{,}10 = 1 \cdot 16^1 + 9 \cdot 16^0, +10 \cdot 16^{-1}$.

Сверточное (реккурентное) кодирование

Структурная схема кодера состоит из регистра сдвига, содержащего K ячеек памяти, n_0 сумматоров по модулю 2 и коммутатора. Выход каждой ячейки регистра соединен либо нет (поэтому соединения обозначены пунктиром) с каждым из сумматоров.

Двоичные информационные символы, поступающие в регистр сдвига от источника информации, сдвигаются в регистре на символов вправо, а выходы сумматоров по модулю 2 опрашиваются коммутатором и полученная последовательность кодовых символов с его выхода подается на модулятор передатчика. Величины , , и порядок подключения сумматоров по модулю 2 к ячейкам регистра сдвига определяют правило сверточного кодирования.

Сверточные коды характеризуются также скоростью и *свободным кодовым расстоянием* . Если первые выходных комбинаций совпадают с входными, то сверточный код – *систематический*, в противном случае код *несистематический*.

Каскадное и турбо кодирование

Сообщения $\{\mathbf{a}_i\}$ от источника ДС сначала кодируются внешним (n_1, k_1) корректирующим кодом. Затем, закодированные символы внешнего кода, кодируются кодером внутреннего (n_2, k_2) корректирующего кода. Общая длина кодовой комбинации каскадного кода равна $n = n_1 n_2$, причем $k = k_1 k_2$ из них являются информационными. Отсюда кодовая скорость и кодовое расстояние данного каскадного кода равны произведению скоростей и кодовых расстояний каждого из кодов: $R = R_1 R_2$, $d_{\min} = d_{\min,1} d_{\min,2}$.

Декодирование каскадного кода проводится в обратном порядке; сначала применяется внутренний декодер, затем внешний. Такая система декодирования позволяет уменьшить сложность декодирования каскадного кода по сравнению с несоставным декодером с той же корректирующей способностью.

Основная идея турбо кодирования, состоящая в кодировании одних и тех же информационных символов M - компонентными реккурентными кодами, позволяет существенно уменьшить вероятность ошибочного декодирования, так как информация о текущем символе a_i может быть извлечена турбо декодером из всех M компонент совместно.

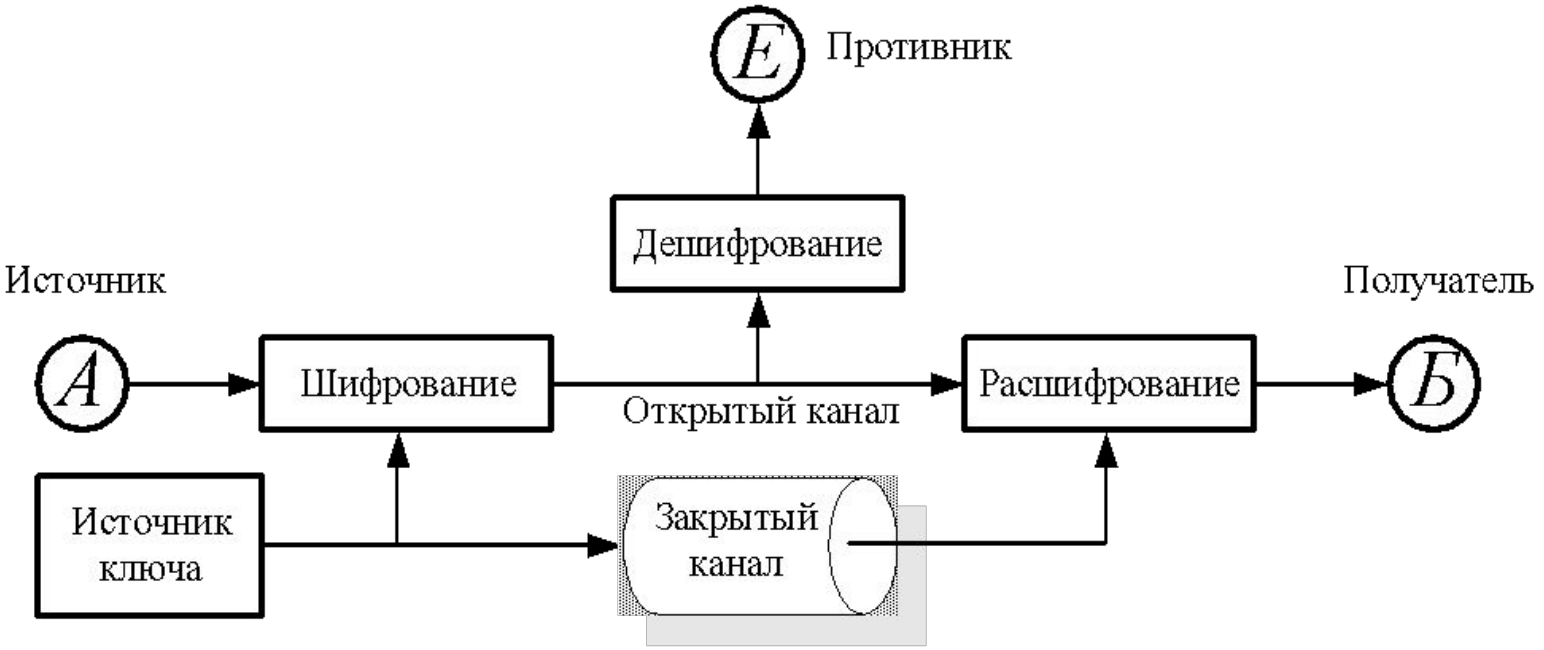
ВВЕДЕНИЕ В ТЕОРИЮ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- *Защита информации* базируется на криптографии и криптоанализе.
- *Криптография* – раздел прикладной математики, изучающий модели, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения видоизменения или несанкционированного использования. Криптография дает возможность преобразовывать *сообщения* таким образом, что прочтение (восстановление) содержащейся в нем *информации* возможно только при знании *ключа*.
- *Криптоанализ* – это раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов (дешифрования) с целью извлечения конфиденциальных параметров, включая открытый текст.
- Криптография и криптоанализ составляют основу – *криптологии*. В криптологии широко используются методы теории вероятностей, теории информации, математической статистики, алгебры, теории чисел и теории алгоритмов.

В качестве сообщений, подлежащих *шифрованию* и *расшифрованию*, рассматриваются *тексты*, построенные на некотором *алфавите*. *Алфавит* – конечное множество используемых при кодировании информации знаков. *Текст* – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах (ИС), можно привести следующие:

- Алфавит Z_2 – двоичный алфавит {0,1};
- Алфавиты Z_8 и Z_{16} – восьмеричный и шестнадцатеричный алфавиты;
- Алфавит Z_{256} – символы, входящие в стандартные коды *ASCII* и КОИ-8;
- Алфавит Z_{33} – 32 буквы русского алфавита (исключая Ё) плюс 1 пробел.
- **И ПРОЧЕЕ**



Отправитель сообщений (А) и их получатель (Б) могут быть физическими лицами, организациями, какими-либо техническими системами. Иногда об *А* и *Б* говорят как об абонентах некоторой сети, о пользователях некоторой компьютерной системы или, еще более формально, как об абстрактных «сторонах» (англоязычный термин «party») или «сущностях» (entry), участвующих в информационном взаимодействии. Но чаще бывает удобно отождествлять участников обмена с некоторыми людьми и заменить формальные обозначения *А* и *Б* на *Алиса* и *Боб*.

Сообщения передаются по так называемому «открытому» каналу связи, доступному для прослушивания некоторым противником *Е*, назовем ее по имени *Ева*, имеющей мощную ЭВМ и владеющей методами криптоанализа.

Простейшие алгоритмы шифрования. Шифр Цезаря применим к русскому языку. В этом шифре каждая буква открытого текста заменяется на другую букву, номер которой в алфавите на три больше. А заменяется на Г, Б на Д и т.д. Три последние буквы русского алфавита Э,Ю,Я шифруются символами _,А,Б соответственно с учетом пробела между словами. Любимое школьниками слово **ПЕРЕМЕНА** после применения к нему алгоритма шифрования Цезаря превращается в слово **ТИУИПИРГ**.

Последующие римские цезари модифицировали шифр, используя смещение в алфавите на четыре, пять и более букв. В общем виде правило шифрования

$$c = (m+k) \bmod N = \begin{cases} (m+k), \text{åñëè } (m+k) < N, \\ (m+k-N), \text{åñëè } (m+k) \geq N. \end{cases}$$

где m и c - номера букв соответственно сообщения и криптограммы, а k - некоторое целое число, называемое ключом шифра (в рассмотренном алгоритме шифрования Цезаря k = 3), N = 33 – мощность алфавита.

Чтобы расшифровать зашифрованный текст, нужно применить «обратный» алгоритм:

$$m = (c-k) \bmod N = \begin{cases} (c-k), \text{åñëè } (c-k) \geq 0, \\ (c-k+N), \text{åñëè } (c-kk) < 0. \end{cases}$$

Ева знает, что шифр был построен по правилу Цезаря, что исходное сообщение было на русском языке, и что был передан шифротекст: ТИУИПИРГ, но ключ *Еве* не известен.

Ева перебирает последовательно все возможные ключи k =1,2,3,…K, (K=N-1=32) (метод «грубой силы»), оценивая получающийся результат.

k	*m*	*k*	*m*	*k*	*m*	*k*	*m*
1	СЗТ	9	ЙЯ	17	БЧ	25	ЩП
2	РЖС	10	ИЮЙ	18	АЦБ	26	ШОЩ
3	**ПЕРЕМЕНА**	11	ЗЭИ	19	ЯХА	27	ЧН
4	ОДП	12	ЖЬ	20	ЮФ	28	ЦМ
5	НГ	13	ЕЫ	21	ЭУ	29	ХЛЦ
6	МВ	14	ДЪ	22	Ь	30	ФК
7	ЛБМ	15	ГЩ	23	Ы	31	УЙ
8	КАЛАЗ	16	ВШГ	24	Ъ	32	**ТИУИПИРГ**

Из таблицы видно, что был использован ключ k=3 и зашифровано сообщение ПЕРЕМЕНА. Причем для того, чтобы проверить остальные возможные значения ключа, потребовалось дешифровать все восемь букв, а в большинстве случаев после анализа двух–трех букв ключ отвергался (только при k=8 надо было дешифровать пять букв, зато при k=22,23,24 хватало и одной, так как в русском языке нет слов, начинающихся с букв: Ь, Ъ, Ы).

Алиса спрятала важные документы в ячейке камеры хранения, снабженной пяти декадным кодовым замком. Теперь она хотела бы сообщить *Бобу* комбинацию цифр, открывающую ячейку. Она решила использовать аналог шифра Цезаря, адаптированный к алфавиту, состоящему из десятичных цифр: $c = (m + k) \bmod 10$. Допустим, она послала *Бобу* шифротекст: 26047. *Ева* пытается расшифровать его, последовательно перебирая все возможные ключи, где $m = (c - k) \bmod 10$. Так при *k*=1 имеем: (26047-11111)mod10=15936. Результаты её дальнейших попыток сведены в таблицу

k	*m*	*k*	*m*	*k*	*m*	*k*	*m*	*k*	*m*
1	15936	3	93714	5	71592	7	59370	9	37158
2	04825	4	82603	6	60481	8	48269	0	26047

Мы видим, что все полученные варианты равнозначны и *Ева* не может понять, какая именно комбинация истинна. Анализируя шифротекст, она не может найти значения секретного ключа. Конечно, до перехвата сообщения, у *Евы* было 10^5 возможных значений кодовой комбинации, а после – только 10. Однако важно отметить то, что в данном случае всего 10 значений ключа. Поэтому при таком ключе (одна десятичная цифра) *Алиса* и *Боб* не могли рассчитывать на большую секретность.

Зашифрованное сообщение должно поддаваться чтению только при наличии ключа шифрования.

Число операций, необходимых для определения использованного ключа по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей.

Число операций, необходимых для расшифрования информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений), или требовать неприемлемо высоких затрат на эти вычисления.

Знание алгоритма шифрования не должно влиять на надежность защиты.

Незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при шифровании одного и того же исходного текста.

Незначительное изменение исходного текста должно приводить к существенному изменению вида

Структурные элементы алгоритма шифрования должны быть неизменными.

Дополнительные элементы, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте.

Длина шифрованного текста не должна превосходить длину исходного.

Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования.

Любой ключ (из множества возможных ключей) должен обеспечивать надежную защиту информации.

Алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Основы оптимального приема дискретных сообщений

Кто или Что это?

Исходный алфавит передаваемых сообщений на приеме известен.

Неизвестным является лишь то, какие элементы из этого алфавита будут переданы, и в какой последовательности.

Наличие искажений и помех в канале приводит к тому, что приёмник не всегда выдает правильное решение о принимаемых сообщениях.

В этой связи актуальным является вопрос о построении приемного устройства (демодулятора), наилучшим (оптимальным) способом обрабатывающего результаты наблюдений, что обеспечит предельно достижимую (потенциальную) верность

Пусть источник дискретных сообщений вырабатывает сообщения $a_i, i=\overline{0,M-1}, a_i \in \mathrm{A}$. При $M=2$ множество A задает двоичный ансамбль сообщений. При $M>2$ множество A определяет многопозиционный (многоуровневый) ансамбль. Статистическая структура источника дискретных сообщений, характеризующая его информационную содержательность, задается вероятной мерой P_{A} или распределением вероятностей $p_i = p(A=a_i), i=\overline{0,M-1}$. Каждому сообщению a_i на выходе передающего устройства системы связи соответствует сигнал $x_i(t) = x(t;a_i), i=\overline{0,M-1}$, $x \in \mathrm{X}, t \in T_x$, где X - множество значений сигнала, T_x - его длительность. На множестве X задана вероятностная мера $P_{\mathrm{A}} = P_{\mathrm{X}}$ совпадающая с вероятностной мерой исходного ансамбля сообщений ввиду однозначности преобразования $\mathrm{X} = \mathrm{U}\,\mathrm{A}$.

Итак, двойка $(\mathrm{X}, P_{\mathrm{X}})$ характеризует ситуацию на входе канала связи.

Канал связи характеризуется тройкой $(\mathrm{X},\mathrm{Y},P_{\mathrm{Y|X}})$**, где** Y **множество значений, принимаемых откликом канала,** $P_{\mathrm{Y|X}}$ **условная вероятностная мера, заданная на** Y **при известном** $x \in \mathrm{X}$**. Мера** $P_{\mathrm{Y|X}}$ **определяется стохастической структурой канала и случайными помехами; она задает косвенное описание канала связи. При этом прямое описание канала задается оператором** V **взаимодействия сигнала** x **и помехи** ξ**. В общем виде оно имеет вид**

$$Y(t) = y(w,t) = \mathrm{V}\left[x(t,a), \boldsymbol{\theta}(w), \xi(t)\right], w \in \mathrm{W}_y, t \in T_y,$$

где $Y(t) = y(w,t)$ **- случайное колебание, наблюдаемое на выходе канала связи,** W_y **- множество его случайных исходов,** T_y **- интервал наблюдения,** $\boldsymbol{\theta}(w) = \left[\theta_1(w), \theta_2(w), \ldots\right]$ **- случайный вектор, характеризующий набор параметров структуры канала, называемых сопутствующими или неинформационными,** $\xi(t), \xi \in \Xi$ **- случайная помеха (шум).**

Стохастический характер наблюдаемого колебания $Y(t)$ приводит к тому, что любое устройство обнаружения или различения сигналов, сколько бы тщательно оно не было спроектировано, **не застрахован от ошибок**. Таким образом, любой различитель (в частности обнаружитель) время от времени выносит решения, не соответствующие реальной обстановке передачи сообщений, например, считая, что в наблюдаемом колебании присутствует i -ый сигнал (сообщение), тогда как в действительности в $Y(t)$ содержится j -ый сигнал (сообщение).

Если решения выносятся по результатам анализа $y(t)$ на интервале T_y совпадающем с длительностью T_x одной посылки сигнала, то говорят о ***поэлементном приёме***. Если интервал наблюдения T_y охватывает несколько посылок сигнала при последовательной передаче дискретных сообщений, например, $T_y = nT_x, n > 1$, то говорят о ***приёме в целом***.

Приемник, в котором *выбранная мера расхождения* принятого сообщения от переданного *минимальна*, называется *оптимальным*. В системах передачи дискретных сообщений в качестве такой меры часто используется средняя вероятность ошибки p_e. Тогда при заданных условиях передачи и заданной модели канала оптимальный приемник характеризуется *идеальным оператором обработки* и *минимальной вероятностью ошибки* $p_{e,\min}$. Этот минимум определяет *потенциальную помехоустойчивость* системы передачи дискретных сообщений. При заданных условиях приёма сигналов потенциальная помехоустойчивость не может быть превзойдена реальным приемником. Сравнивая помехоустойчивость реальных приемников с потенциальной помехоустойчивостью, можно выяснить степень технического совершенства реальных приёмников и возможные резервы повышения их помехоустойчивости.

Средний риск. В задачах проверки гипотез $H_i, i=\overline{0,M-1}$ задается матрица потерь $\Pi=\left[\Pi_{ij}\right], i,j=\overline{0,M-1}$. Кроме того, наряду с заданным каналом $(\mathrm{X},\mathrm{Y},P_{\mathrm{Y|X}})$, полагается известной вероятностная мера P_{X}. Для дискретного источника эта мера определяется распределением вероятностей гипотез $p_i=p(H_i), i=\overline{0,M-1}$.

Средний риск вводится как математическое ожидание матрицы потерь

$$\overline{\mathrm{R}}=\mathrm{M}\{\Pi_{ij}\}=\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\Pi_{ij}p(H_i\cap H_j)=\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\Pi_{ij}p(H_j)p(\mathbf{y}\in Y_i\,|\,H_j),$$

где M – символ математического ожидания.

Учитывая то, что условные вероятности $p(\mathbf{y}\in Y_i\,|\,H_j)$ выражаются через функцию правдоподобия

$$p(\mathbf{y}\in Y_i\,|\,H_j)=\int_{Y_i}l_i(\mathbf{y})d\mathbf{y}=\int_{Y_i}W(\mathbf{y}\,|\,H_j)d\mathbf{y},$$

окончательно для среднего риска получаем

$$\overline{\mathrm{R}}=\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\Pi_{ij}p(H_j)\int_{Y_i}W(\mathbf{y}\,|\,H_j)d\mathbf{y}.$$

Средняя вероятность ошибки. Ошибка возникает тогда, когда решение γ_i не совпадает с истиной гипотезой H_j. При $i = j$ выносится правильное решение. Если матрица потерь простая, т.е. $\Pi_{ij} = 1 - \delta_{ij}$, где δ_{ij}- символ Кронекера, то получаем

$$\overline{\mathrm{R}} = \sum_{i=0}^{M-1} \sum_{j=0 | j \neq i}^{M-1} p_j \int_{Y_i} W(\mathbf{y} \mid H_j) d\mathbf{y} = p_e .$$

В данном случае средний риск - это средняя вероятность ошибки p_e. Эквивалентный критерий - средняя вероятность правильного решения $p_{pr} = 1 - p_e$.

Апостериорная вероятность гипотезы. Если матрица потерь Π неизвестна, то рационально выбрать критерий, в котором она не фигурирует. Это может быть апостериорная вероятность гипотезы $p(H_i \mid \mathbf{y})$, вытекающая из формулы Байеса

$$p(H_i \mid \mathbf{y}) = p_i W(\mathbf{y} \mid H_i) / \sum_{i=0}^{M-1} p_i W(\mathbf{y} \mid H_i),\ p_i = p(H_i). \qquad)$$

В теории связи применяются и другие критерии. Очень часто (особенно в задачах оценивания параметров) за критерий качества принимают саму функцию правдоподобия $l[\mathbf{y}]$.

Байесовский показатель оптимальности основан на критерии среднего риска (и предполагает его минимизацию (в общем случае обеспечение нижней грани):

$$\overline{\mathrm{R}}_B = \min_{\mathrm{D}} \overline{\mathrm{R}} = \min_{\mathrm{D}} \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} \Pi_{ij} p(H_j) \int_{Y_i} W(\mathbf{y} \mid H_j) d\mathbf{y}$$

Решение выносится в пользу той гипотезы H_i, для которой обеспечивается минимум среднего риска. В этом случае решающий функционал $\mathrm{D}(\mathbf{y})$, заданный на пространстве наблюдений Y^n оптимален в пространстве решений Γ.

Показатель минимума средней вероятности ошибки (показатель Зигерта - Котельникова). В этом случае используется критерий. Он связан с минимизацией величины средней вероятности ошибки:

$$\overline{\mathrm{R}}_{ZK} = \min_{\mathrm{D}} p_e = \min_{\mathrm{D}} \sum_{i=0}^{M-1} \sum_{j=0 \mid j \neq i}^{M-1} p_j \int_{Y_i} W(\mathbf{y} \mid H_j) d\mathbf{y} .$$

Данный показатель называют ещё показателем «идеального наблюдателя», полагая, что имеется некоторый наблюдатель на приеме, который задает матрицу Π так, что её элементы Π_{ij} равны нулю при правильных решениях ($i = j$) и одинаковы и равны единице при ошибочных решениях ($i \neq j$).

На практике часто используется эквивалентный показатель, а именно показатель максимума правильного решения

$$\max_{\mathrm{D}} p_{pr} = \max_{\mathrm{D}} \sum_{i=0}^{M-1} p_i \int_{Y_i} W(\mathbf{y} \mid H_i) d\mathbf{y} .$$

Показатель максимума апостериорной вероятности задается так: среди множества гипотез H_j, $j=\overline{0,M-1}$, выбирается такой номер "i", при котором достигается максимум, а именно:

$$i=\arg\max_{0\le j\le M-1} p(H_j\,|\,\mathbf{y})=\arg\max_{0\le j\le M-1}\{p_j W(\mathbf{y}\,|\,H_j)/W(\mathbf{y})\}.$$

Минимаксный показатель оптимальности. Введенные выше показатели предполагают, что известна вероятностная мера P_{X} источника сообщений. Если же P_{X} неизвестна, то можно минимизировать средний риск в условиях наихудшей меры:

$$\max_{0\le j\le M-1}\min_{D}\overline{\mathrm{R}}=\max_{0\le j\le M-1}\min_{D}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\Pi_{ij}p_j\int_{Y_i}W(\mathbf{y}\,|\,H_j)d\mathbf{y}\,.$$

В теории статистических решений показывается, что решение по данному показателю будет таким же, если использовать условные риски

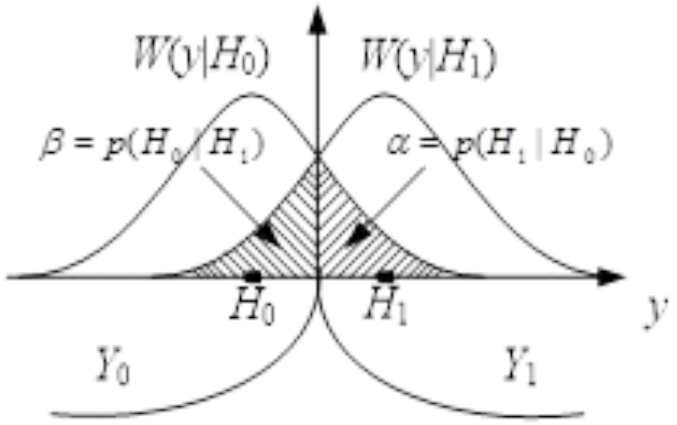
$$\overline{\mathrm{R}}_j=\sum_{i=0}^{M-1}\Pi_{ij}\int_{Y_i}W(\mathbf{y}\,|\,H_j)d\mathbf{y}\,,$$

а решения основывались на показателе оптимальности вида: $\min_{D}\max_{0\le j\le M-1}\overline{\mathrm{R}}_j$.

Показатель оптимальности Неймана-Пирсона. Остановимся детальнее на примере приема двоичных сообщений. Здесь определяются лишь две гипотезы H_0 и H_1. Гипотезу H_0 называют основной, а H_1- альтернативной. Ставится задача проверки гипотезы H_0 против альтернативы H_1. При этом определяют два ошибочных решения, характеризуемых условными вероятностями:

$$\alpha = p(H_1 \mid H_0) = \int_{Y_1} W(\mathbf{y} \mid H_0) d\mathbf{y}\ ,\ \beta = p(H_0 \mid H_1) = \int_{Y_0} W(\mathbf{y} \mid H_1) d\mathbf{y}\ .$$

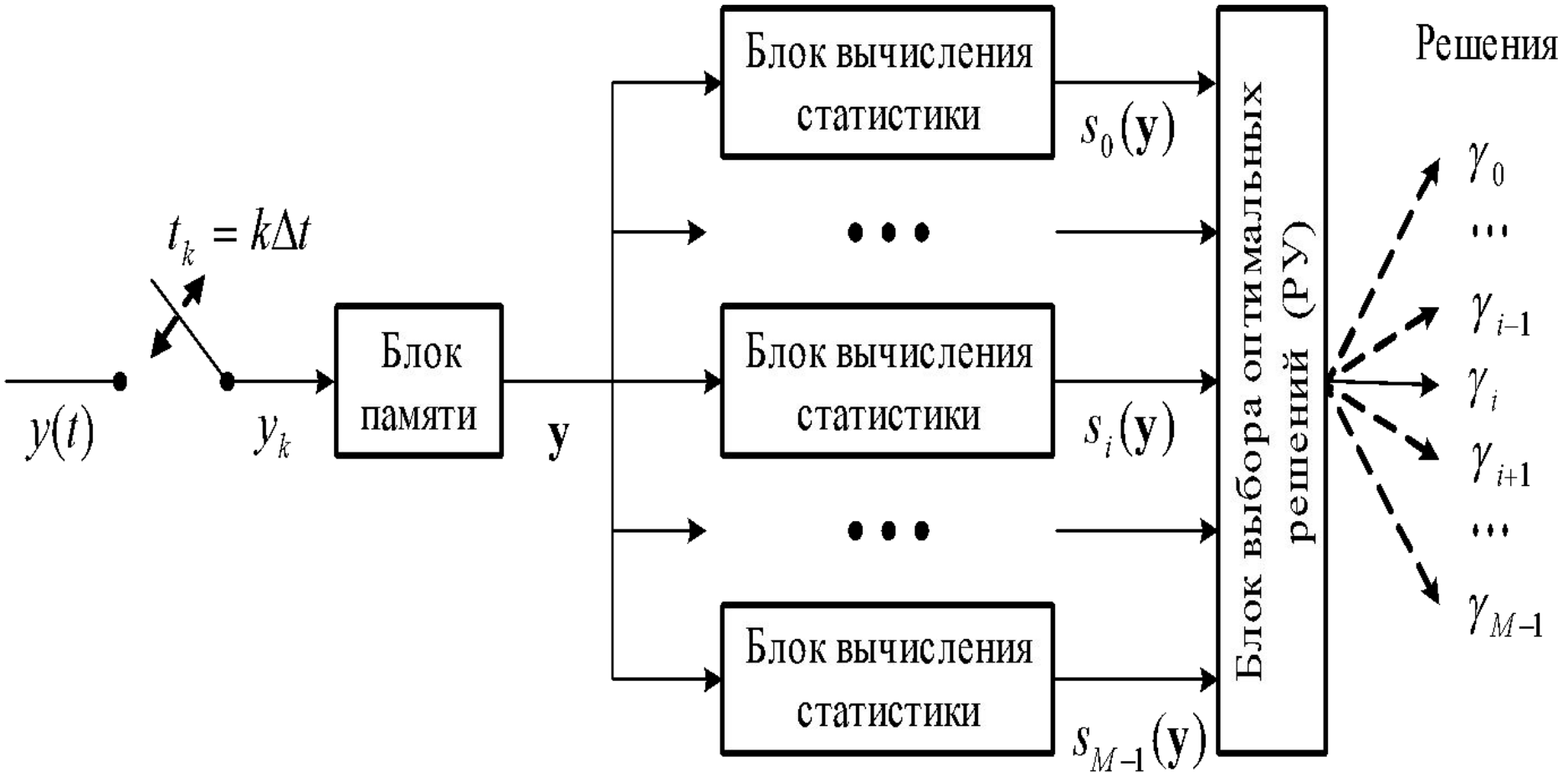
Здесь Y_0- область принятия гипотезы, а Y_1- область отвержения гипотезы или критическая область. Если наблюдение $\mathbf{y}$ попадает в Y_1, так что отвергается H_0, а на самом деле гипотеза H_0 является истиной, то говорят об ошибке первого рода с вероятностью α. Если $\mathbf{y}$ попадает в Y_0, а правильной является H_1, то говорят об ошибке второго рода β.



Кроме вероятностей ошибок α и β в задаче проверки гипотезы H_0 против альтернативы H_1 рассматриваются также вероятности правильных решений:

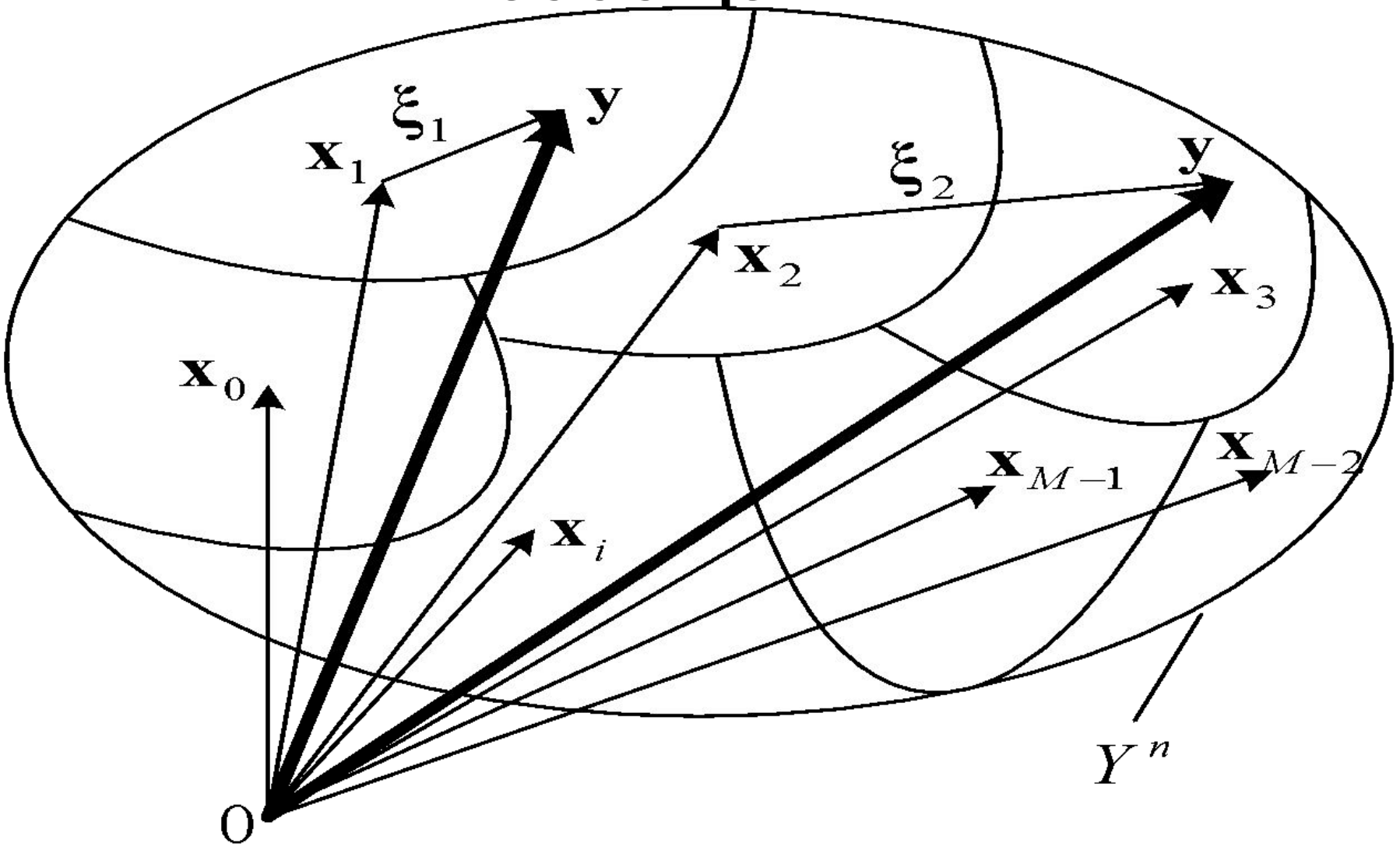
$$p(H_1 \mid H_1) = 1 - \beta,\quad p(H_0 \mid H_0) = 1 - \alpha$$

Структурная схема оптимального приемника дискретных сообщений



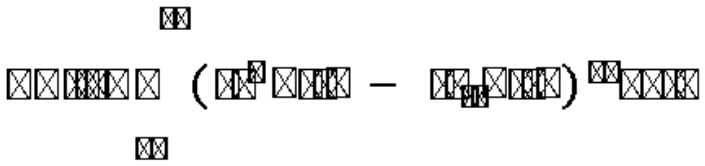
Входной ключ формирует из колебаний $y(t)$ отсечены $y_k = y(t_k = k\Delta t)$, следующие через интервал дискретизации Δt. В блоке памяти на интервале $T_y = n\Delta t$ формируется n-мерный вектор наблюдений $\mathbf{y} = (y_0, y_1, \ldots y_{n-1}), \mathbf{y} \in Y^n$. В блоке вычисления статистики, называемого также оптимальным приемно-фильтрующим устройством (ОПФУ), на основе априорных данных об источнике сообщений, операторе передачи и канале связи, вычисляются те или иные статистики $s_i(\mathbf{y}), i = \overline{0, M-1}$. В блоке выбора оптимальных решений или просто решающем устройстве (РУ) на основе выбранного показателя оптимальности выносятся решения $\{\gamma_i\}$ о передаваемых сообщениях $a_i, i = \overline{0, M-1}$.

Иллюстрация геометрической трактовки приема дискретных сообщений

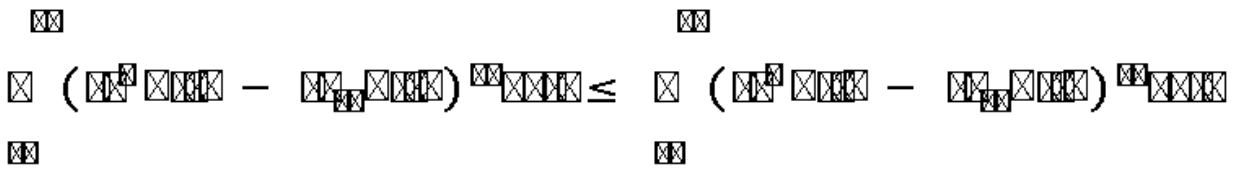


Совокупность возможных реализаций наблюдаемого вектора $\mathbf{y} \in Y^n$ можно интерпретировать точками n - мерного пространства наблюдений Y^n (евклидова пространства). Переданные сигналы будем обозначать векторами (точками) $\mathbf{x}_i, i = \overline{0, M-1}$, откладываемых от начала координат в пространстве Y^n. Когда правило решения $\gamma = \mathrm{D}(\mathbf{y})$ выбрано, то это означает, что каждой точке пространства Y^n, например, $\mathbf{y} = \mathbf{x}_i + \xi$, приписывается одна из M гипотез $H_i, i = \overline{0, M-1}$. Оптимальные правила решения приводят к таким взаимным расположениям границ областей гипотез $H_i, i = \overline{0, M-1}$, при которых средняя вероятность ошибочных решений минимальна $p_{e,\min}$.

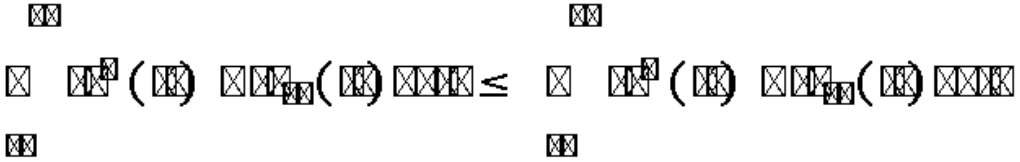
Корреляционный приемник сравнивает поступивший сигнал с имеющимися в нем образцовыми сигналами, которые могли быть переданы от передатчика, т.е. с , и вычисляет расхождения. Для случая белого гауссова шума показано, что оптимальным является сравнение по минимуму среднеквадратичного отклонения, что обеспечит минимум вероятности ошибочного приема.



Для двоичного сигнала: и , при условии равенства энергий этих сигналов сравнение:



примет вид:



При идентичных сигналах ρ = 1, при противоположных ρ = –1 и ортогональных ρ = 0, где =

Согласованный фильтр

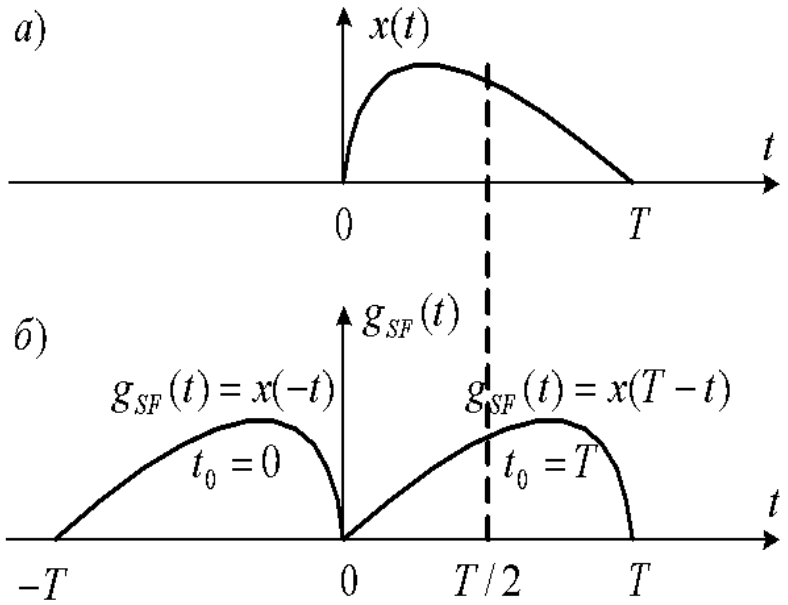
Для решения задач обнаружения и различения детерминированных сигналов, наблюдаемых в смеси с гауссовским шумом, блоки вычисления статистик в схеме оптимального приёмника, могут представлять собой линейные фильтры, которые должны удовлетворять некоторому критерию оптимальности, а именно, получения на выходе фильтра *максимально возможного отношения пикового значения сигнала к среднеквадратическому значению шума*. Выбор такого критерия оптимальности объясняется тем, что в задачах обнаружения и различения сигналов основная цель заключается не в воспроизведении формы сигнала, которая заранее известна, но в наиболее надежной фиксации лишь факта наличия или отсутствия дискретного сообщения в

Для того, чтобы результат фильтрации удовлетворял указанному критерию оптимальности, необходимо согласовать форму импульсной реакции $h(t)$ фильтра с формой детерминированного сигнала $s(t)$, $0 \le t \le T$.

Задача *синтеза оптимального линейного фильтра* состоит в следующем. Требуется найти такую импульсную реакцию $h_{опт}(t)$ оптимального фильтра, которая в момент t_0 обеспечивает *максимум* отношения пикового значения квадрата сигнальной составляющей $s_{вых}(t_0)$ к дисперсии $\sigma^2_{вых}(t_0) = M[n^2_{вых}(t_0)]$ шумовой составляющей на выходе фильтра. Т.е.

$$q^2(t_0) = \frac{s^2_{вых}(t_0)}{\sigma^2_{вых}(t_0)} = \frac{\left[\int_0^T h(\tau)\, s(t_0-\tau)\, d\tau\right]^2}{M\left[\int_0^T h(\tau)\, n(t-\tau)\, d\tau\right]^2}$$

Импульсная реакция оптимального линейного фильтра определяется формой сигнала и в этом смысле согласована с ним. **Таким образом, импульсная реакция согласованного фильтра $g_{SF}(t)$ с точностью до постоянной c - есть зеркальное (относительно вертикальной линии в точке $t = t_0/2$) изображение полезного сигнала.**



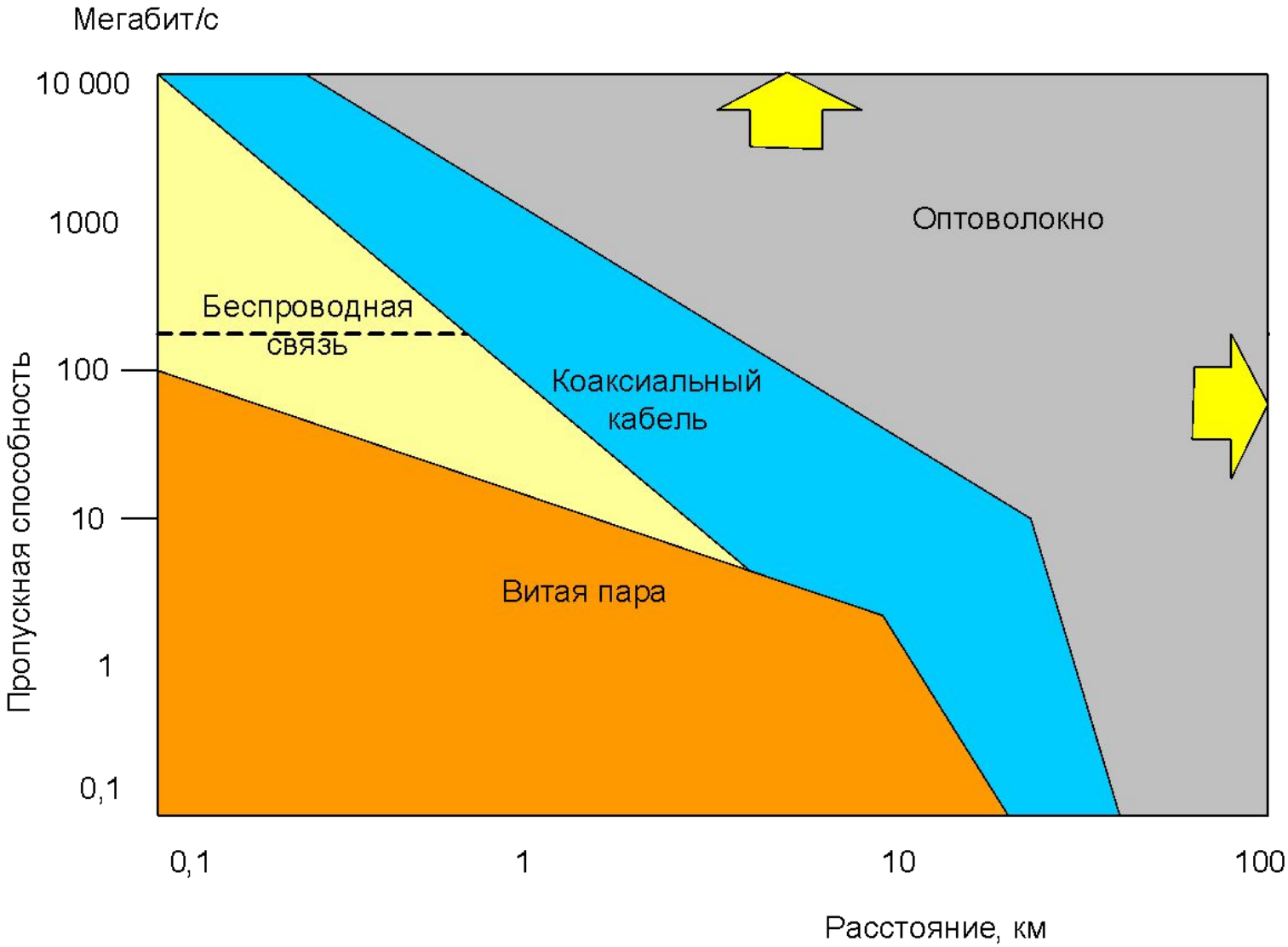
Форма сигнала (*а*) и импульсная реакция (*б*), согласованного с ним фильтра

Основы оптимального приема непрерывных сообщений

Базовые принципы будущих инфокоммуникаций

- Глобализация
- Персонализация
- Мобильность
- Интерактивность
- Информационная безопасность

Пределы передачи данных

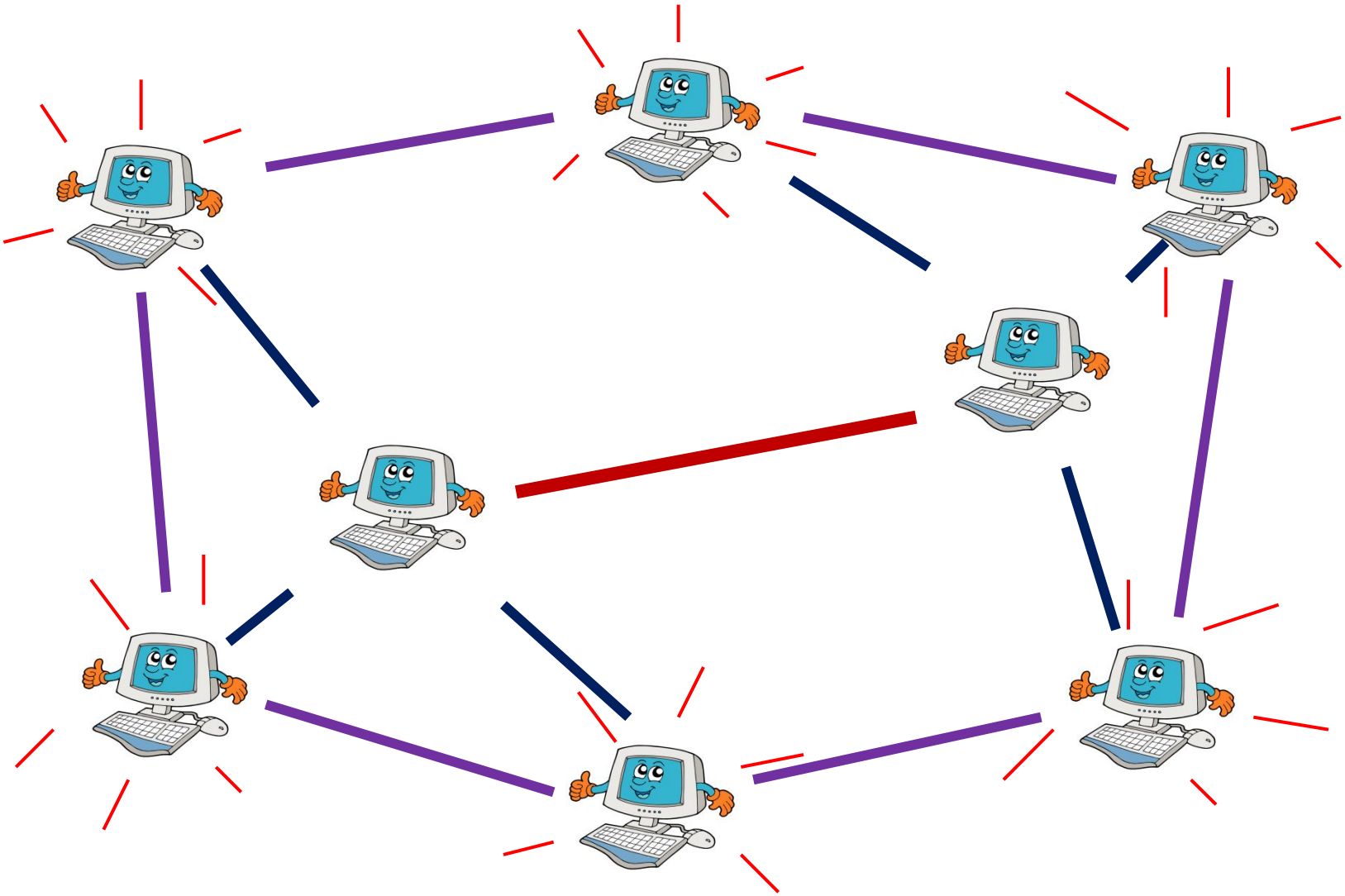


Ограничения

- **Мобильность – ограничивает скорость доступа.**
- **Скорость доступа – ограничивает геометрические размеры области предоставления услуги.**
- **Область – ограничивает количество пользователей.**
- **Персонализация – проблема организации взаимодействия человек-система-человек (единая нумерация, доступ к информации и т.п.)**
- **Информационная безопасность конфликтует с глобализацией.**

Методы многоканальной передачи и распределения информации

Топология сети



Различные топологии сетей

- 1. Полносвязные (каждый с каждым).
- 2. Радиальные.
- 3. Кольцевые.
- 4. Радиально-узловые.
- 5. Смешанные.
- 6. Сотовые (ячеистые).

- **При M абонентах (пользователях) сети каждый из них соединяется с узлом (в мобильной связи с базовой станцией).**
- **Узлы сети (пусть их число равно N) соединены в соответствии с топологией сети. Максимальное число соединений у полносвязной сети. Оно равно:**

$$C_N^2 = \frac{N!}{(N-2)! \cdot 2!} = \frac{(N-1) \cdot N}{2}$$

Типы (виды) сетей

- 1. Сети фиксированной связи (фиксированные сети).
- 2. Сети мобильной (подвижной) связи (мобильные сети).
- 3. Кабельные сети:
  - Волоконно-оптические сети.
  - Металлические сети: «витые пары»; симметричные кабели; коаксиальные кабели; волноводы.
- 4. Радио сети.
- 5. Спутниковые сети.

Типы (виды) сетей по назначению

- Телефонная сеть.
- Телеграфная сеть.
- Радиотрансляционная сеть.
- Телевизионная сеть.
- ИНТЕРНЕТ.
- Сети специального назначения (выделенные сети).

Типы (виды) сетей

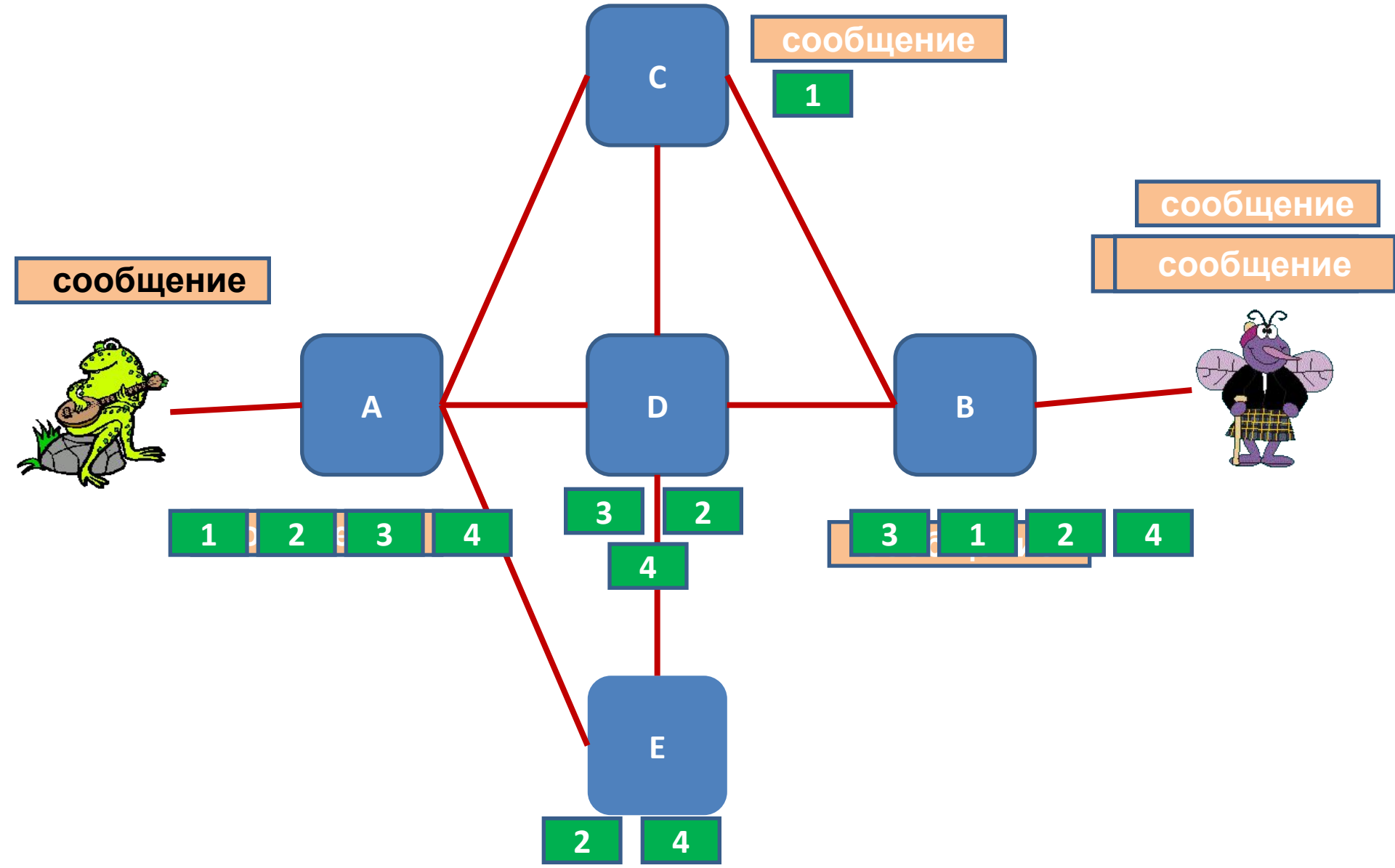
- **Сети с коммутацией каналов (КК).**
- **Сети с коммутацией сообщений (КС).**
- **Сети с коммутацией пакетов (КП).**

Характеристики (параметры) сетей

- Нагрузка (трафик) на сети.
- Топология.
- Способ коммутации.
- Скорость передачи (полоса пропускания).
- Пропускная способность.
- Достоверность (верность).
- Время доставки сообщения.
- Надежность.
- Живучесть.
- Защищенность (информационная безопасность).

- Любая сеть связи (телекоммуникационная сеть) состоит из узлов и линий (каналов) связи, соединяющих узлы.
- Нагрузка – это важнейший исходный параметр, в соответствии с которым происходит расчет и построение сети, а именно: узлов, линий (каналов) связи и проч. Данная задача является технико-экономической с общей постановкой: построить сеть с требуемыми показателями качества при минимальных затратах. Нагрузка измеряется количеством и видом передаваемых сообщений, их продолжительностью и проч. Общим показателем является время занятия приборов, под которыми понимаются линии (каналы) связи и всевозможное оборудование в узлах. Нагрузка весьма изменчива в зависимости от времени года, суток, часов и т.д. Поэтому для ее описания используются методы статистического анализа. Все сети являются системами массового обслуживания, для которых применяются соответствующие методы расчетов и проектирования, использующих теорию телетрафика, теорию вероятностей, теорию надежности и проч.
- Топология выбирается из соображений надежности и живучести, а так же обеспечения других параметров

В узлах реализуются виды коммутации (КК, КС, КП). При КК вызывающий **абонент** набирает номер или посылает служебную информацию, в соответствии с которыми устанавливается соединение с другим вызываемым **абонентом.** После этого передаются сообщения. В завершении передается сигнал об окончании соединения и оно разрушается (разрывается). Эта система с ожиданием и отказами. При КС сообщение от вызывающего **абонента** в сопровождении служебной информации, содержащей помимо прочего адрес вызываемого **абонента**, передается на узел, где заносится в память. Далее по мере наличия свободных линий все это сообщение со служебной информацией последовательно передается от узла к узлу вплоть до вызываемого **абонента**. Эта сеть с ожиданием. При КП сообщение от вызывающего **абонента** разбивается на блоки, которые дополняются служебной информацией. В результате образуются пакеты, которые могут доставляться до вызываемого **абонента** различными путями, но так же как и при КС от узла к узлу. Это так же сеть с ожиданием, хотя при КП и КС возможны отказы, но при проектировании вероятность этого очень мала.


C
сообщение
1
сообщение
сообщение
сообщение
A
D
B
1
2
3
4
3
2
4
3
1
2
4
E
2
4

- Скорость передачи определяется линиями (каналами) связи, соединяющих узлы. Понятие скорости используется для цифровых систем передачи и измеряется количеством символов, как правило двоичных, переданных за одну секунду. Единицей измерения является бит/сек, называемый иногда Бод. Поскольку помимо полезной информации от абонента дополнительно передается служебная информация, служащая для обозначения адреса вызываемого абонента, обеспечения требуемой помехоустойчивости, синхронизации и проч., то под пропускной способностью понимается «полезная» скорость передачи информации или «полезный» объем переданных данных без учета затрат на служебную информацию и различные потери при коммутации в узлах. Измеряется в бит/сек или байт/сек. (В данном случае пропускную способность не следует путать с потенциальной пропускной способностью системы, например, канала связи с полосой пропускания ΔF, определяющей теоретически достижимую максимальную границу).

- В цифровых системах связи показателем качества передаваемых сигналов служит вероятность ошибки, т.е. вероятность неверного приема двоичных символов. Данный показатель называется достоверностью или верностью передачи. В аналоговых системах передачи показателем качества являются искажения, вносимые в сигнал при его передаче по сети связи.
- Важным показателем качества функционирования сети связи является время доставки сообщений или антипод данного показателя время задержки сообщения в сети. Использование того или иного показателя зависит от конкретных требований, предъявляемых к качеству передачи сообщений по сети. В ряде случаев необходимо, что бы время доставки сообщений не превосходило определенного значения. А с другой стороны бывает удобнее нормировать время задержки сообщения в сети. Например при КП пакеты записываются в накопителях в узлах связи. Далее они «дожидаются» своей очереди при наличии свободных каналов связи к следующему узлу. Если каналов будет недостаточно, то сообщения будут задерживаться и даже может произойти переполнение буферного накопителя, что может привести к потере пакетов. Для недопущения этого следует правильно выбирать пропускную способность каналов связи и объем буферных накопителей. Кроме того важен общий механизм функционирование сети, как целостной системы связи. Такой механизм называется ПРОТОКОЛОМ, обеспечивающим правила и порядок взаимодействия всех составляющих сети связи.
- ПРОТОКОЛ очень важен для сети, т.к. от этого зависит все то, что происходит при передаче сообщений. В качественном отношении протокол можно сравнить с языком , на котором разговаривают люди. Если разговаривать на разных языках, то никакого понимания не будет. Помимо этого протокол призван оптимизировать обработку сигналов на всех этапах передачи сообщений по каналам связи и при обработке в узлах.

- Надежность – важнейший показатель функционирования сети, чаще всего определяется средним временем безотказной работы (временем наработки на отказ) и временем восстановления при нарушении работы. Для различных сетей показатели надежности могут существенно отличаться, поскольку это определяется не только техническими, но и экономическими факторами. Для вычислительных сетей, например, среднее время безотказной работы должно быть достаточно большим и составлять, как минимум, несколько тысяч часов. Так же нормируется и время восстановления в зависимости от требований к сети.
- Живучесть – это способность сети противостоять последствиям природных катаклизмов или преднамеренному разрушению сети злоумышленниками. Определяется топологией сети, протоколом, способами защиты сетей от вредных воздействий, охранными мероприятиями и т.д.
- Защищенность (информационная безопасность) определяется протоколом, а так же специальными мерами, обеспечивающими надлежащий уровень информационной безопасности. В количественном отношении характеризуется вероятностью доступа со стороны злоумышленников к информационным ресурсам или вероятностью распознавания (дешифрирования) сообщений. Могут применяться и другие количественные оценки, как, например, время дешифрирования криптозащиты и проч.

Для расчетов сетей связи используются аналитические и программные модели. Наиболее простой моделью, которую часто используют для начального проектирования, является модель Пуассона. Для нее характерно проявление трех свойств: стационарности, отсутствия последствия и ординарности. *Стационарность* требует, чтобы вероятность появления в непересекающихся промежутках времени $\tau_1, \tau_2, \ldots \tau_e$ требований зависела только от числа и длин промежутков, но не зависела от их расположения на временной оси. *Отсутствие последствия* говорит о том, что количество требований, поступивших в промежутке времени $[t_0, t_0 + t)$, стохастически не зависит от поведения потока до момента времени t_0. *Ординарность* указывает, что вероятность $p_{\Delta t}(n > 1)$ того, что в промежутке времени длиной Δt поступит более одного требования, равна нулю при Δt стремящемся к 0.

Это модель *простейшего потока*. ФРВ интервалов между событиями этого потока имеет экспоненциальный вид с параметром λ, называемым интенсивностью потока.

$$F(\tau) = P((w) < \tau) = \pi_1(\tau) = 1 - e^{-\lambda\tau}, \tau \geq 0, \lambda > 0,$$

и полностью определяет вероятностное описание потока.

Вероятность поступления i вызовов в промежутке времени τ подчиняется распределению Пуассона

$$P_\tau(i) = \frac{(\lambda\tau)^i}{i!} e^{-\lambda t}, \quad i = 0, 1, \ldots .$$

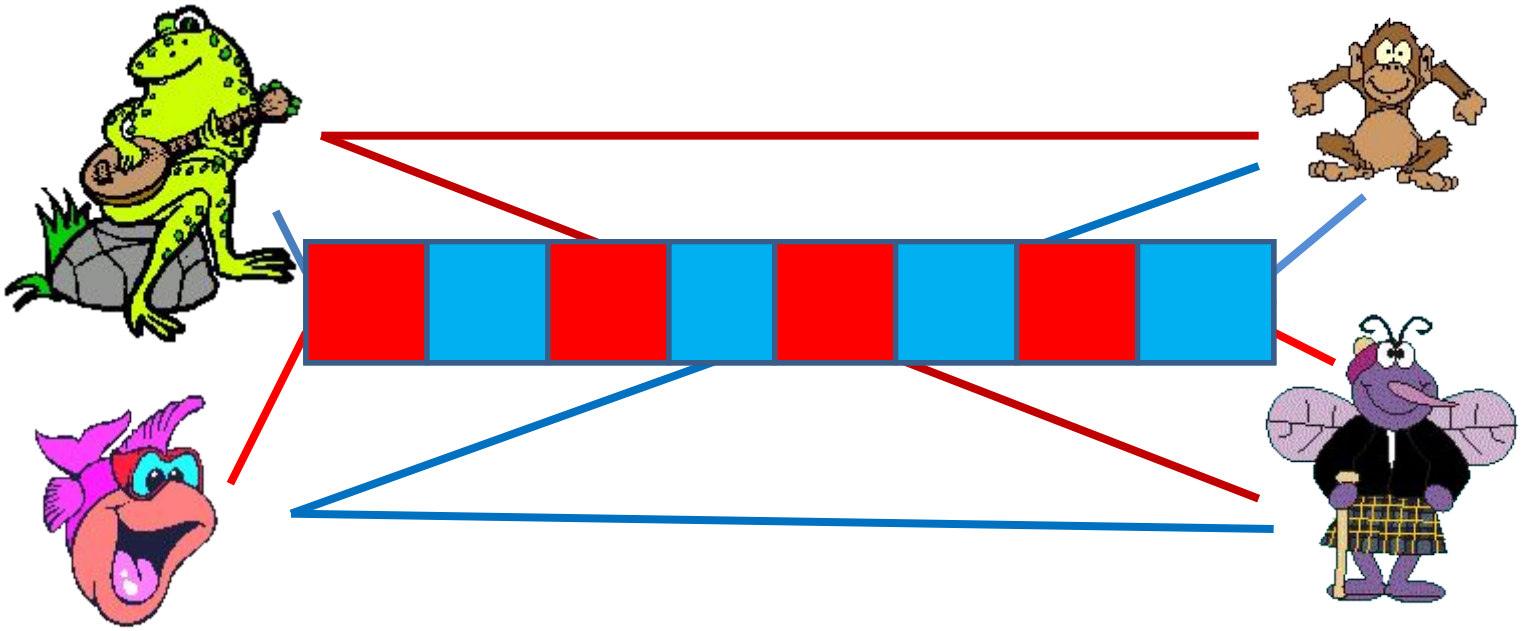
Пуассоновские потоки встречаются и на практике, причем достаточно часто, так как к их образованию приводит наложение «большого числа» случайных потоков с большими расстояниями между поступлением требований. При объединении независимых простейших потоков с параметрами $\lambda_i, i = \overline{1, e}$, суммарный поток также будет простейшими с параметром $\lambda_\Sigma = \sum_{i=1}^{e} \lambda_i$.

Указанное обстоятельство обусловило широкое использование модели пуассоновского простейшего потока в теории массового обслуживания и специальной *теории телетрафика*, исследующей процессы обслуживания информационных потоков на сетях.

Методы многоканальной передачи

Москва

Лондон



Общие принципы многоканальной передачи

- **Многоканальные системы передачи (МСП), обеспечивающие организацию по одной линии связи большого числа одновременно и независимо действующих каналов, являются наряду с устройствами коммутации, основой Взаимоувязанной сети связи (ВСС) нашей страны**
- **Многоканальной системой передачи (МСП) называется совокупность технических средств, обеспечивающих одновременную и независимую передачу сообщений от N источников к N получателям по одной цепи связи или одному стволу. На передающей стороне МСП сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику *канальные переносчики*. Затем модулированные *канальные сигналы* объединяются по этому или иному правилу, в результате чего формируется *групповой сигнал*. Такая операция называется *уплотнением каналов*.**
- **На приемной стороне МСП после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Такая операция называется *разделением (селекцией) каналов*.**
- **Для надежного разделения сигналы отдельных каналов наделяются некоторыми заранее обусловленными *признаками,* которые должны быть такими, чтобы в приемной части системы**

Из курса функционального анализа известно, что элементы линейных непересекающихся множеств линейно-независимы. Поэтому необходимым и достаточным условием линейной разделимости сигналов является условие их линейной независимости.

По определению элементы (сигналы) $x_1(t)$, $x_2(t)$, ... , $x_N(t)$, сигнального пространства X линейно независимы, если их линейная комбинация удовлетворяет тождеству

$$C_1X_1(t)+C_2X_2(t)+\ldots+C_NX_N(t) \equiv 0 ,$$

только при условии равенства всех коэффициентов C_i, $i=\overline{1,N}$, нулю. Если найдется хотя бы один коэффициент C_k не равный нулю, то указанные сигналы – линейно зависимы и не удовлетворяют условию линейной разделимости.

В общем случае необходимым и достаточным условием линейной независимости элементов сигнального пространства является не равенство нулю определителя Грама, составленного из скалярных произведений элементов $x_i(t)$, $i=\overline{1,N}$, пространства X,

$$\Gamma[x_1, x_2, \ldots x_N] = \begin{vmatrix} (x_1,x_1) & (x_1,x_2) & \ldots & (x_1,x_N) \\ (x_2,x_1) & (x_2,x_2) & \ldots & (x_2,x_N) \\ \ldots & \ldots & & \ldots \\ (x_N,x_1) & (x_N,x_2) & \ldots & (x_N,x_N) \end{vmatrix}$$

где (x_i, x_k) – скалярное произведение сигналов $x_i(t)$ и $x_k(t)$.

Определитель Грама равен нулю, если сигналы $x_i(t)$, $x_2(t)$, ... $x_N(t)$ – линейно зависимы, и положителен, если они линейно независимы.

- **Однако, наибольшее применение при линейном уплотнении и разделении каналов находят ансамбли ортогональных функций, что позволяет строить более простые и эффективные устройства.**
- **Примерами ортогональных ансамблей функций являются : 1) любые функции, имеющие неперекрывающиеся между собой частотные спектры; 2) последовательности неперекрывающихся между собой во времени импульсов, в частности, прямоугольных; 3) ортогональные ансамбли функций Радемахера-Уолша**

Условие линейной разделимости канальных сигналов в МСП с ЧРК можно записать в виде:

$$G_{xi}(\omega)=\begin{cases}\neq 0\ ,\ \omega_i'<\omega<\omega_i'',\\ =0\ ,\omega<\omega_i'\ ,\ \omega>\omega_i'',\end{cases}\qquad i=\overline{1,N},\qquad \textbf{(A)}$$

где $G_{xi}(w)$ — энергетический спектр i-ого канального сигнала; w'_i и w''_i — границы полосы частот, отводимой в линейной цепи (стволе) для i-ого канального сигнала.

Из этого выражения (A) следует, что в МСП с ЧРК канальные сигналы ортогональны. Действительно, пусть сформированы канальные сигналы $x_i(t)$, $i=\overline{1,N},$, удовлетворяющие данному условию (A). Тогда, используя соотношения для прямого и обратного преобразований Фурье сигналов $x_i(t)$ и $x_k(t)$, получаем

$$\int_{-\infty}^{\infty}x_i(t)x_k(t)dt=\int_{-\infty}^{\infty}x_i(t)\left[\frac{1}{2\pi}\int_{-\infty}^{\infty}S_{x_k}(i\omega)e^{i\omega t}d\omega\right]dt=$$
$$=\frac{1}{2\pi}\int_{-\infty}^{\infty}S_{x_k}(i\omega)\left[\int_{-\infty}^{\infty}x_i(t)e^{i\omega t}dt\right]d\omega,$$

где спектральная плотность i-ого канального сигнала, комплексно сопряженная спектральной плотности $S_{xi}(iw)$.

Следовательно, с учетом выражения (A) можем записать

$$\int_{-\infty}^{\infty}x_i(t)x_k(t)dt=\frac{1}{2\pi}\int_{-\infty}^{\infty}S_{x_k}(i\omega)S^{*}{}_{x_i}(i\omega)d\omega=\begin{cases}\varepsilon_i\ ,k=i,\\ 0\ \ ,k\neq i.\end{cases}\qquad \textbf{(B)}$$

Это и есть условие ортогональности разнесенных по спектру сигналов. Величина

$$\varepsilon_i=\int_{-\infty}^{\infty}x_i{}^2(t)dt=\frac{1}{2\pi}\int_{-\infty}^{\infty}G_{x_i}(\omega)d\omega,\quad i=\overline{1,N},\qquad \textbf{(C)}$$

равна энергии канальных сигналов.

Условие линейной разделимости канальных сигналов в МСП с ВРК можно записать в виде:

$$x_i(t)=\begin{cases}\neq 0, & t_i' < t < t_i'', \\ 0, & t < t_i', t > t_i'', \end{cases} \qquad t \in \mathrm{T}, \qquad \textbf{(D)}$$

где $x_i(t)$ – импульс i-ого канала произвольной формы (часто – это прямоугольный импульс), заданный на интервале $\Delta t_i = t_i'' - t_i'$, $i = \overline{1,N}$; $t_i' t_i''$ – границы временного интервала, данные для i-ого канального сигнала на интервале T.

Если импульсам $x_i(t)$ на периоде T выделены неперекрывающиеся временные интервалы Δt_i, $i = \overline{1,N}$, то соответствующие им канальные сигналы ортогональны

$$\int_T x_i(t)x_k(t)dt = \begin{cases}\varepsilon_i, k = i, \\ 0, k \neq i\end{cases} \qquad t \in \mathrm{T}. \qquad \textbf{(E)}$$

Величина ε_i – это энергия импульсов на интервале Δt_i

$$\varepsilon_i = \int_{t_i'}^{t_i''} x_i^2(t)dt, \quad i = \overline{1,N}.$$

Ортогонализация Грама-Шмидта

Счетное множество линейно независимых векторов $\{a_i\} = a_1 \dots a_n$ можно преобразовать во множество ортогональных векторов $\{b_i\} = b_1 \dots b_n$ или множество ортонормированных векторов $\{e_i\} = e_1 \dots e_n$ той же размерности, при условии, что каждый вектор a_i или b_i выражаются через линейную комбинацию векторов a_i. (Вектор называется нормированными, если его скалярный квадрат равен единице)

Введем операцию проекции вектора a_i на вектор a_j

$\text{пр}_{a_j} a_i = \frac{(a_i, a_j)}{(a_j, a_j)} a_j$, **где** (a_i, a_j) **— скалярное произведение векторов. Тогда имеем:**

$$b_1 = a_1$$

$$b_2 = a_2 - \text{пр}_{b_1} a_2$$

$$b_3 = a_3 - \text{пр}_{b_1} a_3 - \text{пр}_{b_2} a_3$$

……

$$b_n = a_n - \sum_{i=1}^{n-1} \text{пр}_{b_i} a_n = a_n - \sum_{i=1}^{n-1} \frac{(a_n, b_i)}{(b_i, b_i)} b_i.$$

Ортонормированный вектор получаем по формуле:

$$e_i = \frac{b_i}{\|b_i\|}$$

Для справки

Вектор $\vec{a} = \{a_x; a_y; a_z\}$ и вектор $\vec{b} = \{b_x; b_y; b_z\}$.

Скалярное произведение $(\vec{a}; \vec{b}) = a_x b_x + a_y b_y + a_z b_z = c$.

Модуль $|\vec{a}| = \sqrt{(\vec{a}; \vec{a})} = \sqrt{a_x^2 + a_y^2 + a_z^2} = \sqrt{d}$

Вектор $\vec{a} = \{a_x; a_y; a_z\}$, умножив на число 3, получаем $\vec{c} = \{ka_x; ka_y; ka_z\}$.

Сумма $\vec{a} + \vec{b} = \{a_x + b_x; a_y + b_y; a_z + b_z\}$.

Задачи по курсу ОТС (часть 2)

- Максимальная частота спектра аналогового сигнала равна 2 Кгц. Какое число уровней квантования используется для кодирования отсчетов, если скорость цифрового сигнала равна 20 кбит/с?
- Для кодирования значений отсчетов аналогового сигнала используется 1024 уровня. Какова скорость цифрового сигнала и максимальная частота спектра аналогового сигнала, если скорость отсчетов равна 16 кбит/с?
- Максимальная частота спектра аналогового сигнала равна 2,5 кГц. Каждый отсчет кодируется кодовой комбинацией, отображающей один из 16 уровней квантовния. Какова длительность элементов цифрового сигнала?
- Каково расстояние между отсчетами аналогового сигнала, если скорость цифрового сигнала равна 32 кбит/с, а число уровней квантования равно 16?
- Длительность элементов цифрового сигнала равна 20 мкс. Максимальная частота спектра аналогового сигнала равна 5 кГц. Сколько уровней квантования применялось для кодирования отсчетов?

ПРИЛОЖЕНИЕ

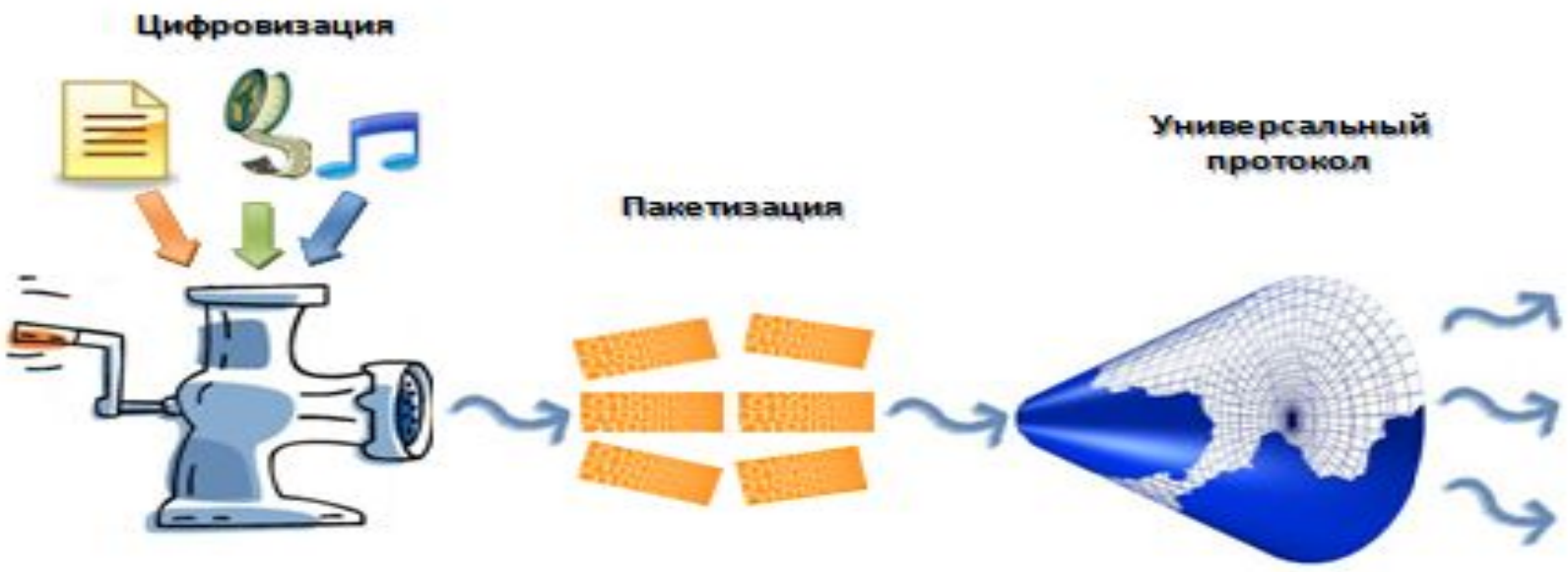
- **К материалам по теме: «Методы многоканальной передачи и распределения информации»**
- **Материалы приложений отмечаются различными значками, например:**

или

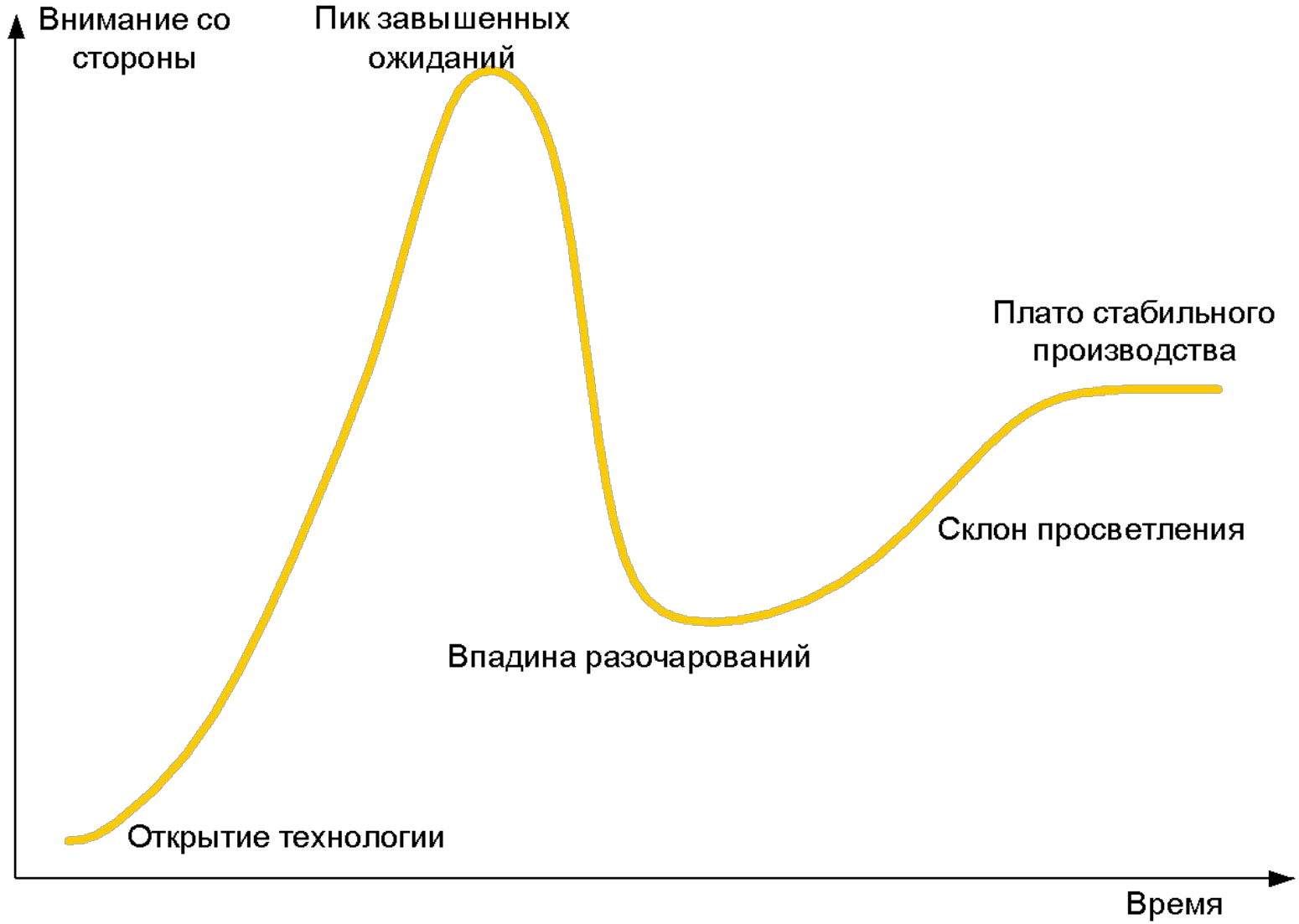
или

и т.д.

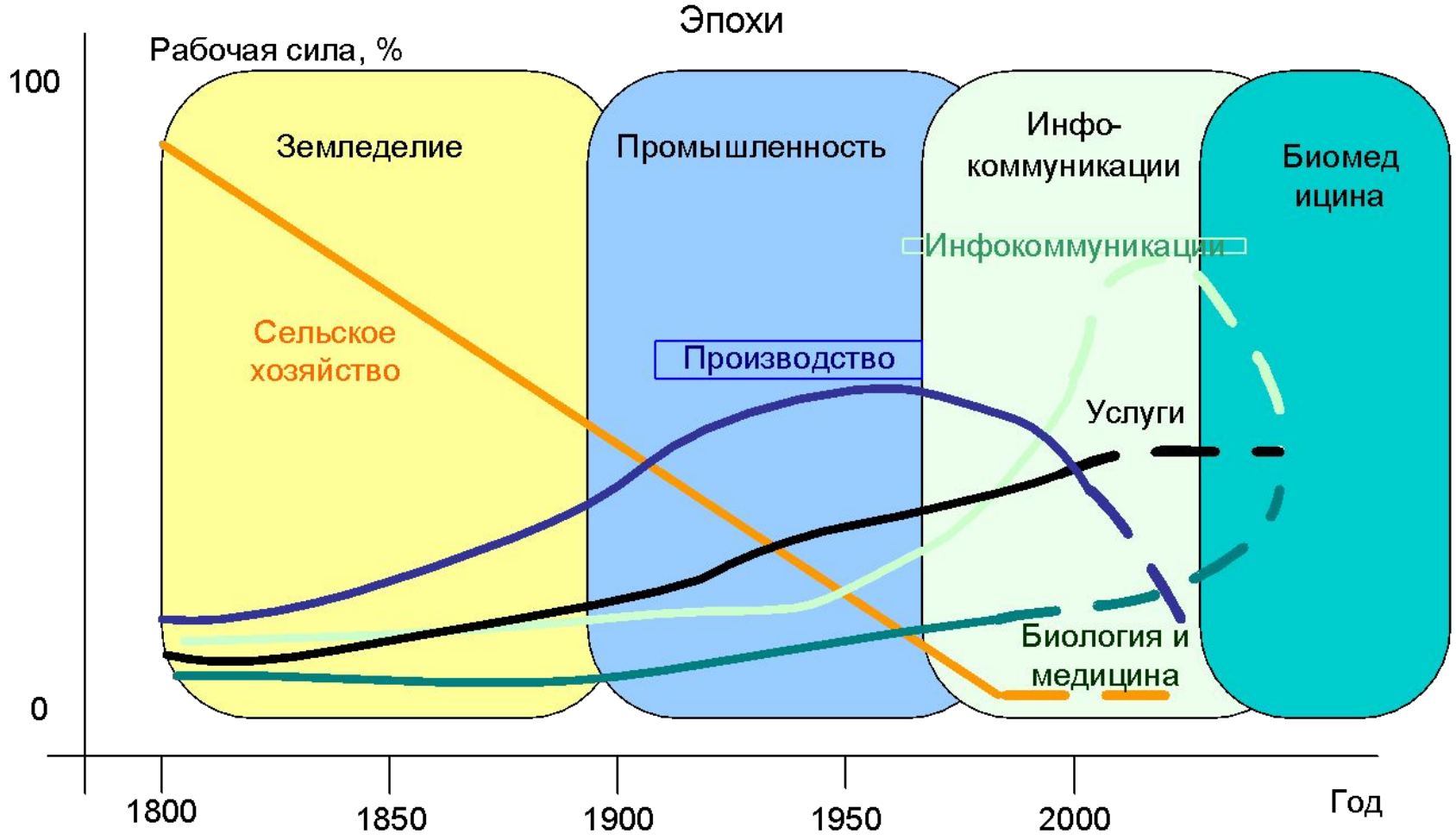
Структура глобальных инфокоммуникаций



Реакция на новые технологии



Прогноз занятости



Потенциальные возможности

Орган ощущения	Пропускная способность рецептора	Нейронная передача
Глаза	200 Гбит/с	200Мбит/с
Уши	4 Мбит/с	2 Мбит/с
Кожа	1,5 Гбит/с	10 Мбит/с
Язык	150 Мбит/с	11 Мбит/с
Нос	20 Гбит/с	30 Мбит/с
Суммарно	200 Гбит/с	250 Мбит/с

Информационные ресурсы необходимые человеку в будущем

- Текстовые сообщения – 1 Кбит/с
- Голосовая связь – 10 Кбит/с
- Видеосвязь – 1 Мбит/с
- Просмотр IPTV – 20 Мбит/с
- Телеметрия состояния здоровья человека – до 100 Мбит/с
- Передача данных - до 10 Гбит/с

НУМЕРАЦИЯ В ТЕЛЕФОНИИ

- В 1999 году план нумерации на сетях связи стран 7-й зоны (Россия, Казахстан) всемирной нумерации строился по зоновому принципу, согласно которому каждой зоне нумерации назначается трехзначный код ABC или DEF.
- Код ABC может быть назначен географической зоне нумерации. При этом недопустимо использование ресурсов нумерации одной географической зоны на территории другой географической зоны.
- Код DEF может быть назначен негеографической зоне нумерации.
- Международный номер состоит из кода страны (1 - 3 знака) и национального (значащего) номера абонента, либо кода страны для Глобальной службы и Глобального абонентского номера, либо кода страны для Сетей, кода идентификации Сети и абонентского номера.
- Максимальное число знаков в международном номере может быть до 15 (рек. Е.164 МСЭ-Т).
- При исходящей автоматической международной связи используется следующий план набора международного номера:
- Пмн Кс Nн, либо
- Пмн Кс Nгл, либо
- Пмн Кс Ки Na, где
- Пмн - префикс выхода на международную сеть (международный префикс); в настоящее время Пмн = 8 - 10, в перспективе Пмн = 00.
- Кс - 1 - 3-значный код страны для Географической зоны (страны, группы стран в сводном плане нумерации, выделенной географической зоны), либо 3-значный код страны для Сети, либо 3-значный код страны для Глобальной службы;
- Nн - национальный (значащий) номер абонента;
- Nгл - номер абонента Глобальной службы;
- Ки - код идентификации Сети;
- Na - номер абонента.

НУМЕРАЦИЯ В ИНТЕРНЕТ

- IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например: 128.10.2.30 - традиционная десятичная форма представления адреса, 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса. Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса.
- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей). В сетях класса A количество узлов должно быть больше 216 , но не превышать 224.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 28-216. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он

НУМЕРАЦИЯ В ИНТЕРНЕТ

Класс A

0	N сети	N узла

Класс B

1	0	N сети	N узла

Класс C

1	1	0	N сети	N узла

Класс D

1	1	1	0	адрес группы multicast

Класс E

1	1	1	1	0	зарезервирован

НУМЕРАЦИЯ В ИНТЕРНЕТ

Класс	Наименьший адрес	Наибольший адрес
A	001.000.000.000	126.000.000.000
B	128.000.000.000	191.255.000.000
C	192.000.001.000	223.255.255.000
D	224.000.000.000	239.255.255.255
E	240.000.000.000	247.255.255.255

127.X.X.X - адрес зарезервированный под localhost (для настройки серверов)

НУМЕРАЦИЯ В ИНТЕРНЕТ

- Одним из основных отличий внедряемого в настоящее время протокола IPv6 от протокола IPv4 является использование более длинных адресов. Адреса получателя и источника в IPv6 имеют длину 128 бит или 16 байт. Версия 6 обобщает специальные типы адресов версии 4 в следующих типах адресов:
- Unicast - индивидуальный адрес. Определяет отдельный узел - компьютер или порт маршрутизатора. Пакет должен быть доставлен узлу по кратчайшему маршруту.
- Cluster - адрес кластера. Обозначает группу узлов, которые имеют общий адресный префикс (например, присоединенных к одной физической сети). Пакет должен быть маршрутизирован группе узлов по кратчайшему пути, а затем доставлен только одному из членов группы (например, ближайшему узлу).
- Multicast - адрес набора узлов, возможно в различных физических сетях. Копии пакета должны быть доставлены каждому узлу набора, используя аппаратные возможности групповой или широковещательной доставки, если это возможно.

Коммутаторы

- **Впервые ручной коммутатор был применен в 1878 году в США, где в городе Нью-Хэвен, штат Коннектикут, была открыта первая телефонная станция. Этот ручной коммутатор, стоимостью 28,5 долларов, обслуживал 21-ого абонента. При этом оператор должен был прослушивать все разговоры, чтобы определить момент их завершения.**

Коммутаторы

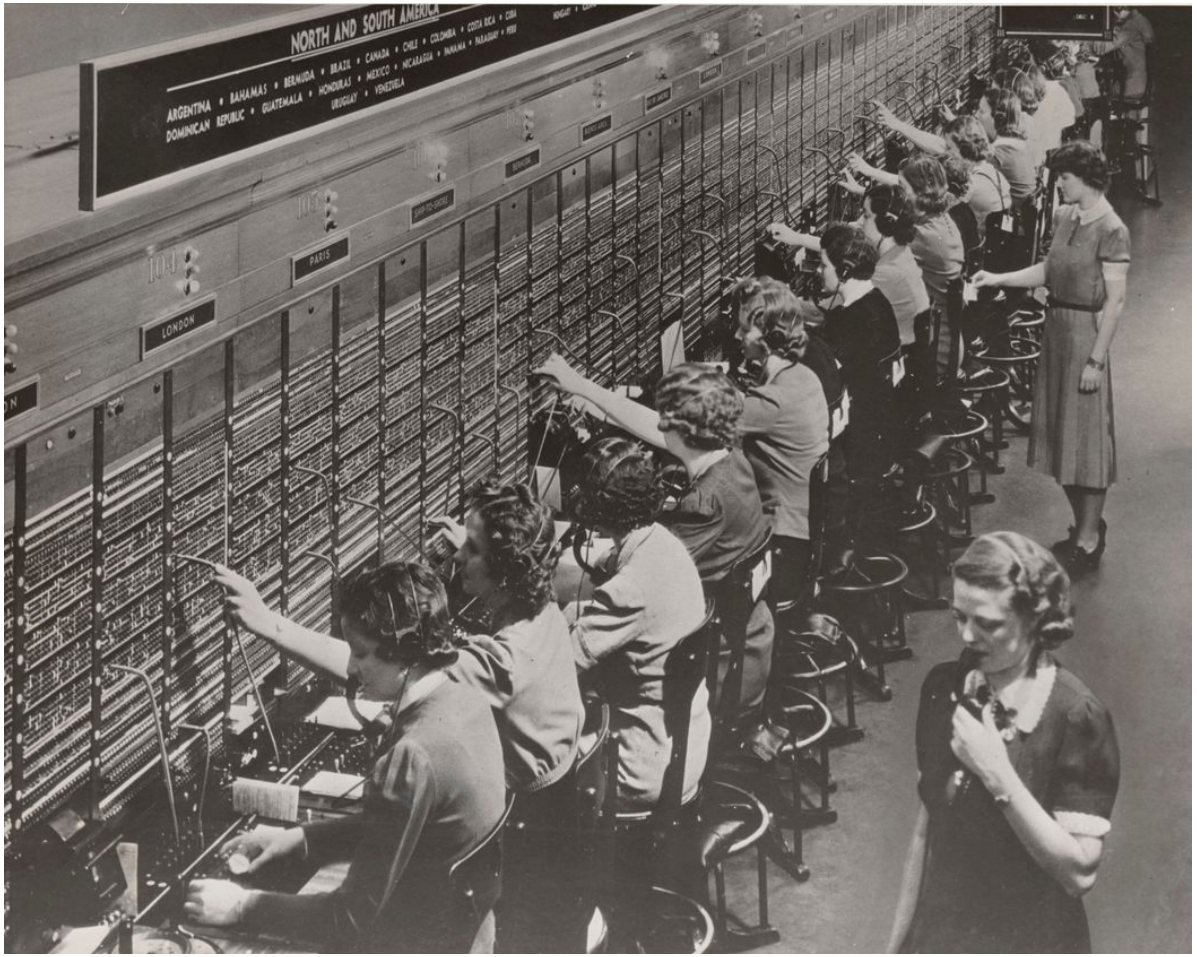
Коммутаторы

Коммутаторы

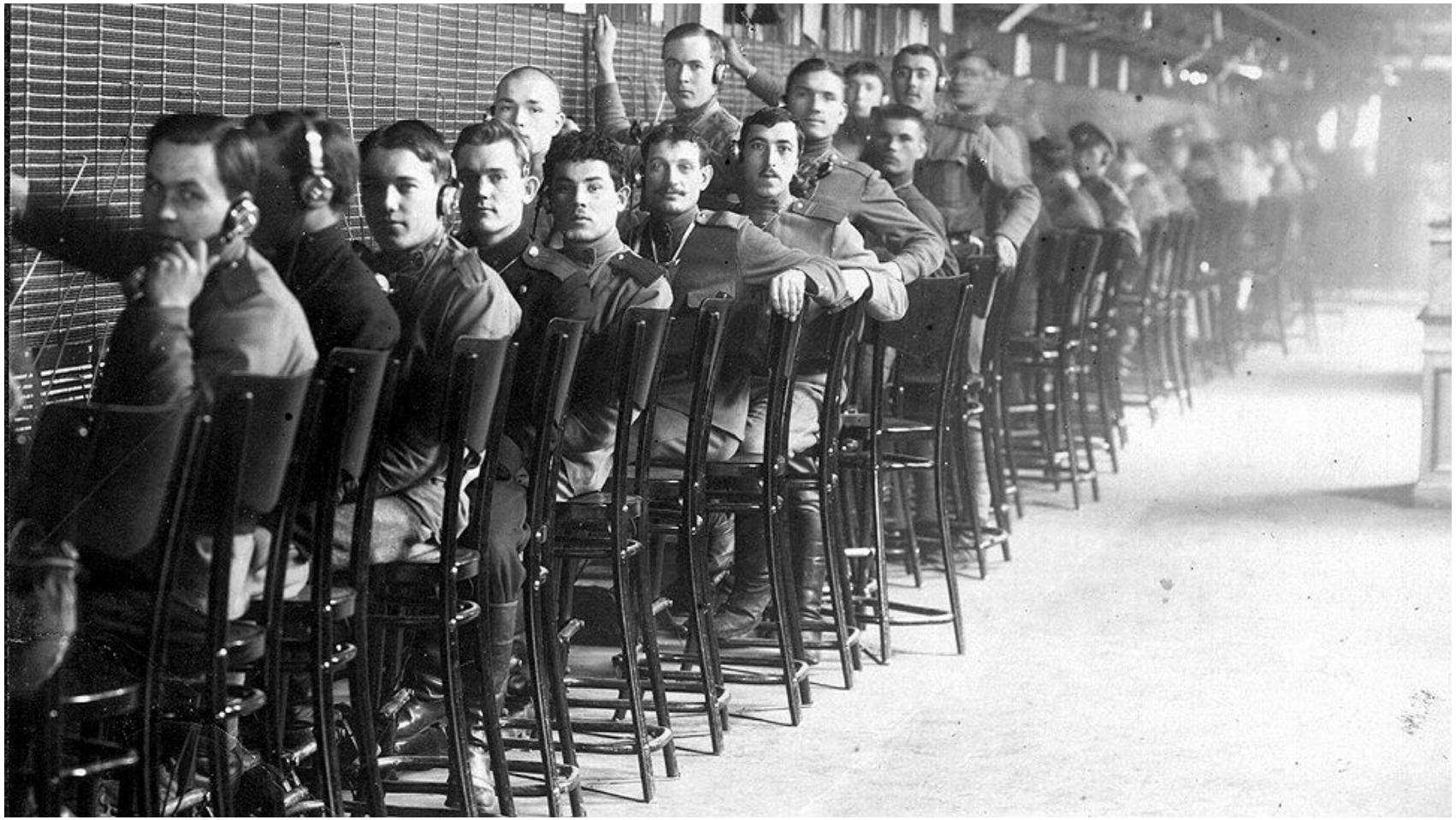
Коммутаторы

Коммутаторы

Коммутаторы



Коммутаторы



Коммутаторы

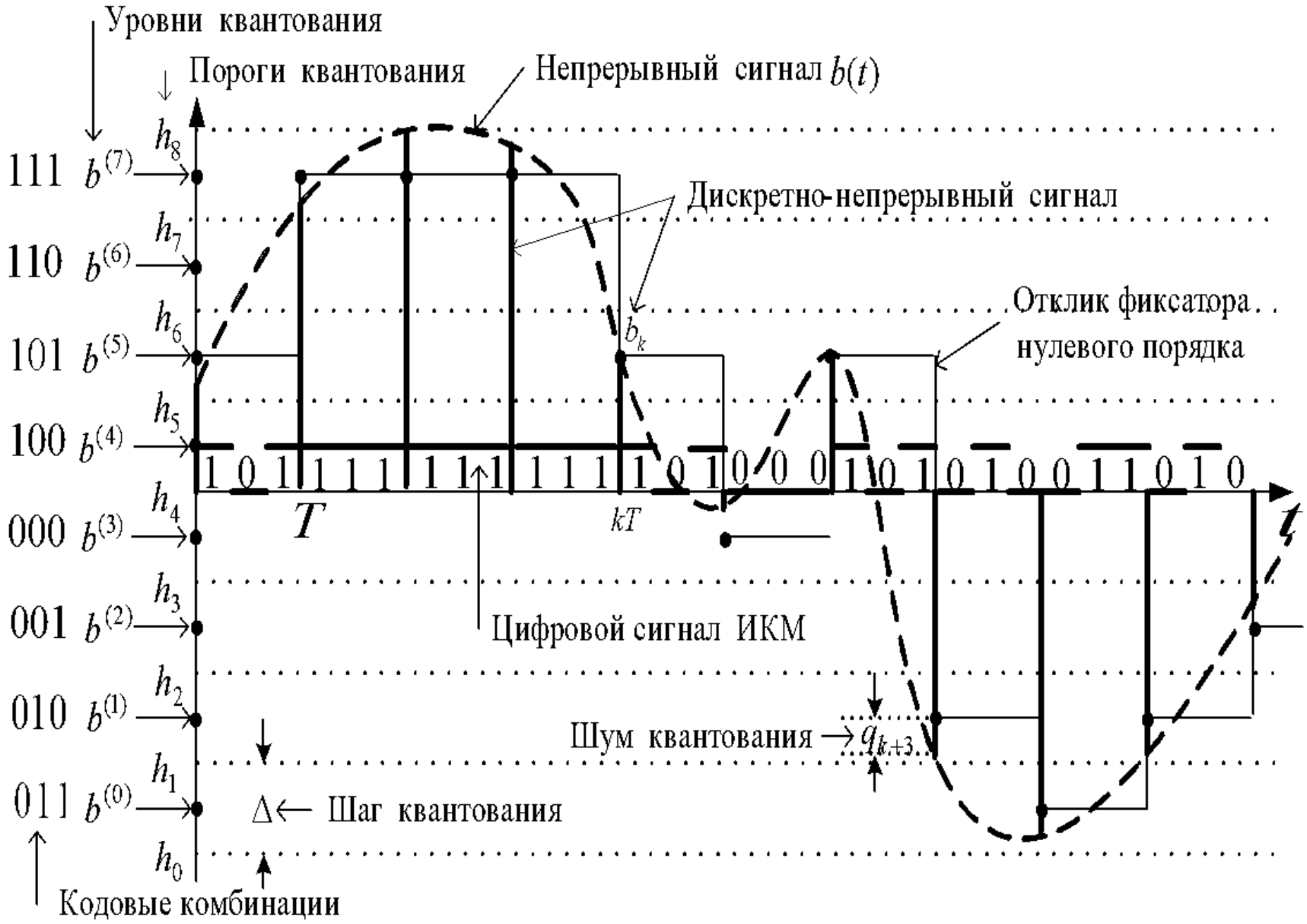
Коммутаторы

Системы передачи и коммутации

Технологии передачи

- **xDSL** (англ. *digital subscriber line*, цифровая абонентская линия) — семейство технологий, позволяющих значительно повысить пропускную способность абонентской линии телефонной сети общего пользования путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигналов. Технологии xDSL появились в середине 90-х годов как альтернатива цифровому абонентскому окончанию ISDN. В аббревиатуре xDSL символ **«x»** используется для обозначения первого символа в названии конкретной технологии, а DSL обозначает цифровую абонентскую линию DSL (англ. *Digital Subscriber Line* — цифровая абонентская линия; также есть другой вариант названия — Digital Subscriber Loop — цифровой абонентский шлейф). Технологии xDSL позволяют передавать данные со скоростями, значительно превышающими те скорости, которые доступны даже лучшим аналоговым и цифровым модемам. Эти технологии поддерживают передачу голоса, высокоскоростную передачу данных и видеосигналов, создавая при этом значительные преимущества как для абонентов, так и для провайдеров. Многие технологии xDSL позволяют совмещать высокоскоростную передачу данных и передачу голоса по одной и той же медной паре. Существующие типы технологий xDSL различаются в основном по используемой форме модуляции и скорости передачи данных.
- **Fiber To The X** или **FTTx** (англ. *fiber to the x* — оптическое волокно до точки X) — это общий термин для любой широкополосной телекоммуникационной сети передачи данных, использующей в своей архитектуре волоконно-оптический кабель в качестве «последней мили» для обеспечения всей или части абонентской линии. Термин является собирательным для нескольких конфигураций развёртывания оптоволокна — начиная от FTTN (до узла) и заканчивая FTTD (до рабочего стола). В строгом определении FTTx является только физическим уровнем передачи данных, однако фактически понятием охватывается большое число технологий канального и сетевого уровней. С широкой полосой систем FTTx неразрывно связана возможность предоставления большого числа новых услуг.
- **BWA** (англ. *Broadband Wireless Access* – широкополосный беспроводный доступ) обеспечивает высокоскоростной доступ и экономичность решений.
- **NGN** (англ. *next generation networks* — сети последующего поколения) — мультисервисные сети связи в основе которых лежат IP технологии обеспечивающие интеграцию (конвергенцию) сетей

ЗАГОТОВКИ


Уровни квантования
Пороги квантования
Непрерывный сигнал $b(t)$
Дискретно-непрерывный сигнал
Отклик фиксатора нулевого порядка
b_k
111 $b^{(7)}$
110 $b^{(6)}$
101 $b^{(5)}$
100 $b^{(4)}$
000 $b^{(3)}$
001 $b^{(2)}$
010 $b^{(1)}$
011 $b^{(0)}$
h_8
h_7
h_6
h_5
h_4
h_3
h_2
h_1
h_0
1 0 1 1 1 1 1 1 1 1 1 0 1 0 0 0 1 0 1 0 1 0 0 1 1 0 1 0
T
kT
t
Цифровой сигнал ИКМ
Шум квантования → q_{k+3}
$\Delta \leftarrow$ Шаг квантования
Кодовые комбинации

Модели сигналов:

- *финитный* во времени сигнал характеризуется тем, что отличен от нуля лишь на конечном интервале T_x;
- сигнал с *финитным спектром*; для таких сигналов амплитудный спектр равен нулю вне некоторого конечного интервала частот: $S_x(2\pi f) = 0,\ f \notin [-F_x, F_x]$;
- *каузальный* сигнал удовлетворяет условию: $x(t) = 0$ при $t < 0$;
- *сепарабельный* сигнал представляется счетным множеством линейно независимых составляющих;
- *периодический* сигнал – сигнал, значения которого повторяются на периоде T, т.е. $x_T(t) = x(t+T)$; примеры периодических сигналов:
- *гармонический* сигнал

$$x(t) = U\cos(\omega t + \varphi),\quad T = 2\pi/\omega,$$

где U - амплитуда, ω - частота, φ - начальная фаза;

- *периодическая последовательность импульсов*

$$x_T(t) = U\sum_{k=-\infty}^{\infty} v(t - t_0 - kT),$$

где U - амплитуда, t_0 - временной сдвиг относительно начала координат, $v(t)$ - функция, описывающая форму импульса с единичной амплитудой и длительностью τ_v, $f_0 = 1/T$ - основная частота следования импульсов.

1. Пусть X - множество сигналов $x(t), t \in T$, с конечной энергией $E_x = \int_0^T x^2(t)dt < \infty$.

Учитывая то, что все физические процессы имеют конечную энергию, такое множество достаточно для представления физических процессов, описывающих электрические сигналы. Введем функцию вида:

$$d(\mathbf{x},\mathbf{y}) = \sqrt{\int_0^T |x(t) - y(t)|^2 \, dt} \; .$$

Нетрудно проверить, что такая функция удовлетворяет аксиомам а,б,в и может рассматриваться как расстояние между сигналами $x(t)$ и $y(t)$ с конечными энергиями.

Пару $(X,d)_{L_2}$ называют пространством L_2 сигналов с конечной энергией. Здесь сигналы изображаются точками, а близость между сигналами – расстоянием между соответствующими точками или среднеквадратичным расстоянием.

2. Пусть X - множество сигналов $\mathbf{x} = (x_1, x_2, ..., x_n)$. Зададим расстояние формулой

$$d(x, y) = \sqrt{\sum_{i=1}^{n} | x_i - y_i |^2} .$$

Пару $(X, d)_{R^n}$ называют n мерным евклидовым пространством R^n. Такое пространство особенно часто используют в теории связи при анализе дискретно-аналоговых сигналов.

Множество X образует *вещественное линейное пространство*, если для его элементов выполняются аксиомы:

а) любой элемент $\mathbf{x} \in \mathbf{X}$ принимает вещественные значения;

б) если $\mathbf{x} \in \mathbf{X}$ и $\mathbf{y} \in \mathbf{X}$, то $\mathbf{x} + \mathbf{y} \in \mathbf{X}$, т.е. при суммировании свойства сохраняются.

Операция суммирования коммутативна: $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ и ассоциативна: $\mathbf{z} + (\mathbf{x} + \mathbf{y}) = (\mathbf{z} + \mathbf{x}) + \mathbf{y}$;

в) для любого сигнала $\mathbf{x} \in \mathbf{X}$ и вещественного числа α определен сигнал $\alpha\mathbf{x} \in \mathbf{X}$;

г) множество X содержит нулевой элемент 0, такой, что $\mathbf{x} + \mathbf{0} = \mathbf{x}$ для всех $\mathbf{x} \in \mathbf{X}$.

В случае, когда математические модели сигналов описываются комплексными функциями, то, допуская в аксиоме в) умножение на комплексное число, приходим к понятию о *комплексном линейном пространстве*.

Элементы линейного пространства называют также векторами. Для них вводят важные понятия *линейной независимости* и *линейной зависимости* векторов.

Векторы $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ - линейно независимы, если равенство

$$\sum_{i=1}^{n} \alpha_i \mathbf{x}_i = 0$$

достигается тогда и только тогда, когда $\alpha_i = 0, i = \overline{1,n}$.

Абстрактное множество X произвольных векторов $\mathbf{x}, \mathbf{y}, \ldots$ называют **нормированным пространством**, если это линейное пространство, для каждого элемента которого $\mathbf{x} \in \mathbf{X}$ введена функция-норма $\| \mathbf{x} \|$, удовлетворяющая следующим аксиомам:

а) $\| \mathbf{x} \| > 0$, причем $\| \mathbf{x} \| = 0$, только тогда, когда $\mathbf{x} = \mathbf{0}$;

б) $\| \alpha \mathbf{x} \| = | \alpha | \cdot \| \mathbf{x} \|$;

в) $\| \mathbf{x} + \mathbf{y} \| \leq \| \mathbf{x} \| + \| \mathbf{y} \|$ - аксиома неравенства треугольника.

3. Пусть X - множество сигналов $\mathbf{x} = (x_1, x_2, ..., x_n)$ с двоичными элементами $x_i = (0,1), i = \overline{1,n}$. Зададим функцию расстояния в виде

$$d(x, y) = \sum_{i=1}^{n} | x_i - y_i | = \sum_{i=1}^{n} x_i \oplus y_i ,$$

где $\otimes$ - знак суммирования по модулю два (по правилам: 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0). Введенную функцию называют расстоянием Хемминга. Такое расстояние широко используется в теории кодирования, а пару $(X d)_{2n}$ называют n – мерным пространством Хемминга.

1. Норма множества $L_2(T)$ сигналов с конечной энергией

$$\| \mathbf{x} \| = \sqrt{\int_0^T x^2(t)dt} = \sqrt{E_x} \ .$$

С физической точки зрения квадрат длины вектора равен энергии сигнала. Если нормированное пространство $L_2(T)$ рассматривается как метрическое, то расстояние в нем определяется соотношением для $d(\mathbf{x}, \mathbf{y})$.

2. Конечномерное евклидово пространство R^n с нормой

$$\| \mathbf{x} \| = \sqrt{\sum_{i=1}^{n} | x_i |^2}$$

задается метрикой, определяемой соотношениями для $d(\mathbf{x}, \mathbf{y})$.

3. 2n – n-мерное пространство Хэмминга с нормой

$$\| \mathbf{x} \| = \sum_{i=1}^{n} x_i$$

задается метрикой, определяемой соотношениями для $d(\mathbf{x}, \mathbf{y})$.

Бесконечномерное комплексное линейное пространство H называют *гильбертовым*, если для двух его элементов $\mathbf{x}$ и $\mathbf{y}$ вводится комплексное число $(\mathbf{x},\mathbf{y})$, которое называется *скалярным произведением* и для которого справедливы аксиомы:

а) $(\mathbf{x},\mathbf{x}) \geq 0,$ причем $(\mathbf{x},\mathbf{x}) = 0,$ только тогда, когда $\mathbf{x} = \mathbf{0}$;

б) $(\mathbf{x},\mathbf{y}) = \overline{(\mathbf{y},\mathbf{x})}$ - симметрия скалярного произведения, где $\overline{(\mathbf{y},\mathbf{x})}$ величина комплексно сопряженная величине $(\mathbf{x},\mathbf{y})$;

в) $(\mathbf{x}_1 + \mathbf{x}_2,\mathbf{y}) \leq (\mathbf{x}_1,\mathbf{y}) + (\mathbf{x}_2,\mathbf{y});\ \ (\alpha\mathbf{x},\mathbf{y}) = \alpha(\mathbf{x},\mathbf{y})$ - линейность скалярного произведения.

Полагается также, что в пространстве H существует счетное множество линейно-независимых элементов. Пространство с таким свойством - есть *сепарабельное гильбертово пространство*.

Норма элемента гильбертова пространства вводится так

$\| \mathbf{x} \| = \sqrt{(\mathbf{x},\mathbf{x})}$,

а расстояние между элементами

$d(\mathbf{x},\mathbf{y}) = \| \mathbf{x} - \mathbf{y} \| = \sqrt{(\mathbf{x}-\mathbf{y},\mathbf{x}-\mathbf{y})}$.

Спектральное представление сигналов.
Обобщенный ряд Фурье

Сигнал $x(t)$ с ограниченной энергией E_x можно представить *обобщенным рядом Фурье* следующего вида

$$x(t) = \sum_{n=0}^{\infty} c_n \psi_n(t),$$

где $c_n, n = 0,1,2,...$ - коэффициенты ряда, $\{\psi_n(t)\}, n = 0,1,2,...$ - базисные функции.

Система $\{\psi_n(t)\}, n = 0,1,2,...,$ относится к классу ортогональных функций, если она удовлетворяет следующему условию

$$\int_{-\infty}^{\infty} \psi_k(t)\psi_n(t)dt = \begin{cases} E_{\psi n}, k = n, \\ 0, \quad k \neq n, \end{cases} \qquad E_{\psi n} = \int_{-\infty}^{\infty} \psi_n^2(t)dt.$$

где $\{E_{\psi n}\}$ – энергии базисных функций.

Периодическая функция (сигнал) с периодом T_x может быть представлена *тригонометрическим рядом Фурье* вида

$$x_{T_x}(t) = 0.5a_0 + \sum_{n=1}^{\infty} a_n \cdot \cos n\omega_0 t + \sum_{n=1}^{\infty} b_n \cdot \sin n\omega_0 t, \quad \omega_0 = 2\pi / T_x.$$

С учетом формул Эйлера:

$$\cos n\omega_x t = \left(e^{jn\omega_x t} + e^{-jn\omega_x t}\right)/2, \quad \sin n\omega_x t = \left(e^{jn\omega_x t} - e^{-jn\omega_x t}\right)/2j,$$

ряд преобразуется к следующему виду

$$x_{T_x}(t) = \frac{1}{2}\left[a_0 + \sum_{n=1}^{\infty}(a_n - jb_n)e^{n\omega_0 t} + \sum_{n=1}^{\infty}(a_n + jb_n)e^{-n\omega_0 t}\right].$$

Обозначая

$$\underline{X}_n = \begin{cases} 0.5(a_n - jb_n), & n > 0, \\ 0.5a_0, & n = 0, \\ 0.5(a_n + jb_n), & n < 0, \end{cases}$$

получаем представление сигнала экспоненциальным рядом Фурье

$$x_{T_x}(t) = \sum_{n=-\infty}^{\infty} \underline{X}_n e^{jn\omega_0 t}, \quad \underline{X}_n = S_x(jn\omega_0),$$

где $\omega_0 = 2\pi / T_x$ – основная частота следования сигнала, $\omega_n = n\omega_0$ – частота, кратная основной частоте, $\{\underline{X}_n\}$- комплексные амплитуды спектра сигнала.

$$X_n = \frac{1}{T_x}\int_0^{T_x} x_{T_x}(t)e^{-jn\omega_0 t}dt, \quad n = 0,\pm 1,\pm 2,\ldots.$$

$$x(t) = \frac{1}{\pi}\int_0^{\infty} S_x(j\omega)e^{j\omega t}d\omega$$

$$X(k) = \sum_{n=0}^{N-1} x(n)\, e^{-\frac{2\pi}{N} nk i}, \quad k = 0, \dots, N-1$$

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k)\, e^{\frac{2\pi}{N} nk i}, \qquad n = 0, \dots, N-1$$

$$x(n) = \sum_{k=0}^{N-1} X(k)\, e^{\frac{2\pi}{N} nk i}, \quad n = 0, \dots, N-1$$

В результате ДПФ N отсчетам (в общем случае комплексным) сигнала $x(n)$, ставится в соответствие N отсчетов (в общем случае комплексных) спектрального отображения $X(k)$.

Для вычисления одного отсчета $X(k)$ необходимо выполнение N операций комплексного умножения и сложения. Следовательно, для вычисления N отсчетов спектрального отображения $X(k)$ потребуется N^2 операций комплексного умножения и сложения. Этот показатель принято называть вычислительной сложностью и обозначать $O(N^2)$.

Пусть число отсчетов N кратно степени 2-ки. Т.е. $N = 2^n$, $n = 1; 2; 3; \dots$. Разделим все отсчеты $x(n)$ на две группы, разместив в первой группе отсчеты с нечетными номерами, а во второй – соответственно с четными. Поскольку в этих группах будет по $\frac{N}{2}$ отсчетов, то, следовательно, в два раза уменьшится количество комплексных умножений и сложений при вычислении в каждой из двух групп. Продолжим далее деление групп надвое. Учитывая, что $N = 2^n$ всего возможно ровно n делений. Тогда вычислительная сложность $O(N \log_2 N)$.

Быстрое преобразование Фурье