# Теория информации

- Курсовая работа
- 1. Построить код Хаффмана для букв русского алфавита.
- 2. Выбрав ключи, закодировать фамилию, имя и отчество кодом Цезаря и далее, используя «квадрат» Виженера.
- 3. Используя код п.1 закодировать свои фамилию, имя и отчество, полученные из п.2.
- 4. Для двух заданных источников дискретных сообщений рассчитать энтропию объединения. (Индивидуальное задание по номеру в журнале).

| Номер | | | | | |
|---|---|---|---|---|---|
| 1 | | 0,5 | 0,25 | 0,125 | 0,125 |
| 2 | | 0,5 | 0,125 | 0,25 | 0,125 |
| 3 | | 0,5 | 0,125 | 0,125 | 0,25 |
| 4 | | 0,25 | 0,5 | 0,125 | 0,125 |
| 5 | | 0,125 | 0,5 | 0,25 | 0,125 |
| 6 | | 0,125 | 0,5 | 0,125 | 0,25 |
| 7 | | 0,25 | 0,125 | 0,5 | 0,125 |
| 8 | | 0,125 | 0,25 | 0,5 | 0,125 |
| 9 | | 0,125 | 0,125 | 0,5 | 0,25 |
| 10 | | 0,25 | 0,125 | 0,125 | 0,5 |
| 11 | | 0,125 | 0,25 | 0,125 | 0,5 |
| 12 | | 0,125 | 0,125 | 0,25 | 0,5 |
| 13 | | 0,25 | 0,25 | 0,25 | 0,25 |
| 14 | | 0,625 | 0,125 | 0,125 | 0,125 |
| 15 | | 0,125 | 0,625 | 0,125 | 0,125 |
| 16 | | 0,125 | 0,125 | 0,625 | 0,125 |
| 17 | | 0,125 | 0,125 | 0,125 | 0,625 |
| 18 | | 0,375 | 0,25 | 0,25 | 0,125 |
| 19 | | 0,375 | 0,25 | 0,125 | 0,25 |
| 20 | | 0,375 | 0,125 | 0,25 | 0,25 |
| 21 | | 0,25 | 0,375 | 0,25 | 0,125 |
| 22 | | 0,25 | 0,375 | 0,125 | 0,25 |
| 23 | | 0,125 | 0,375 | 0,25 | 0,25 |
| 24 | | 0,25 | 0,25 | 0,375 | 0,125 |
| 25 | | 0,25 | 0,125 | 0,375 | 0,25 |
| 26 | | 0,125 | 0,25 | 0,375 | 0,25 |
| 27 | | 0,25 | 0,25 | 0,125 | 0,375 |
| 28 | | 0,25 | 0,125 | 0,25 | 0,375 |
| 29 | | 0,125 | 0,25 | 0,25 | 0,375 |
| 30 | | 0,375 | 0,375 | 0,125 | 0,125 |
| 31 | | 0,375 | 0,125 | 0,375 | 0,125 |
| 32 | | 0,375 | 0,125 | 0,125 | 0,375 |

# Теория информации

## Матрица условных вероятностей $P(y_j|x_i)$

| | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | $y_6$ |
|---|---|---|---|---|---|---|
| $x_1$ | 0,25 | 0,25 | 0,125 | 0,125 | 0,125 | 0,125 |
| $x_2$ | 0,25 | 0,125 | 0,25 | 0,125 | 0,125 | 0,125 |
| $x_3$ | 0,125 | 0,25 | 0,125 | 0,25 | 0,125 | 0,125 |
| $x_4$ | 0,125 | 0,125 | 0,25 | 0,125 | 0,25 | 0,125 |

# Теория информации

**ТЕМЫ РЕФЕРАТОВ:**

1. **История возникновения и развития информационных устройств.**
2. **История и современность в первичных способах кодирования сообщений.**
3. **Аналого-цифровые методы преобразований сигналов.**
4. **Информатизация современного общества.**
5. **Информационная безопасность, проблемы и пути решения.**
6. **Информационные технологии в медицине.**
7. **Информационные технологии в образовании.**

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
Кафедра «Общей теории связи»

# ОБРАЗЕЦ ПО ОФОРМЛЕНИЮ ПЕРВОЙ СТРАНИЦЫ

**КУРСОВАЯ РАБОТА**

Выполнил: студент группы (указать номер группы. Фамилию, имя и отчество не указывать, но написать:

Фамилия…….

Имя……...

Отчество……..

Фамилия имя и отчество будут заполняться при защите курсовой работы и декодировании выполненных заданий)

Проверил: (указать должность, фамилию имя и отчество преподавателя)

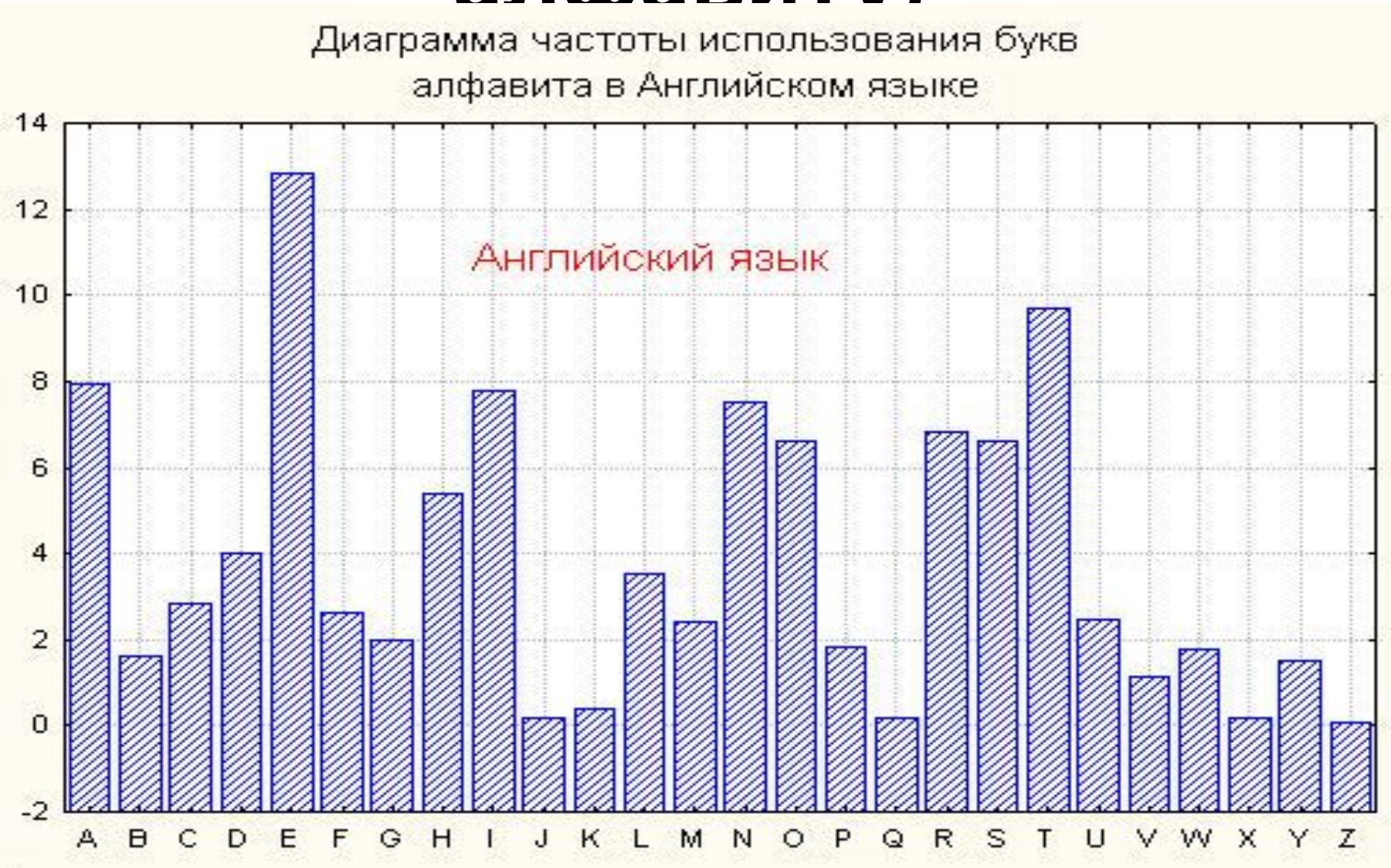
Москва, (указать год)

# КУРСОВАЯ РАБОТА СОДЕРЖИТ:

- **Фамилия, Имя, Отчество в виде кодовой последовательности кодом Хаффмана ……**
- **Ключ «Цезаря» …….**
- **Ключ «Виженера» ……..**
- **Квадрат «Виженера» …….**
- **Код Хаффмана (дерево и таблица)…….**

# Статистика букв (по убыванию)

# Статистика букв (по алфавиту)

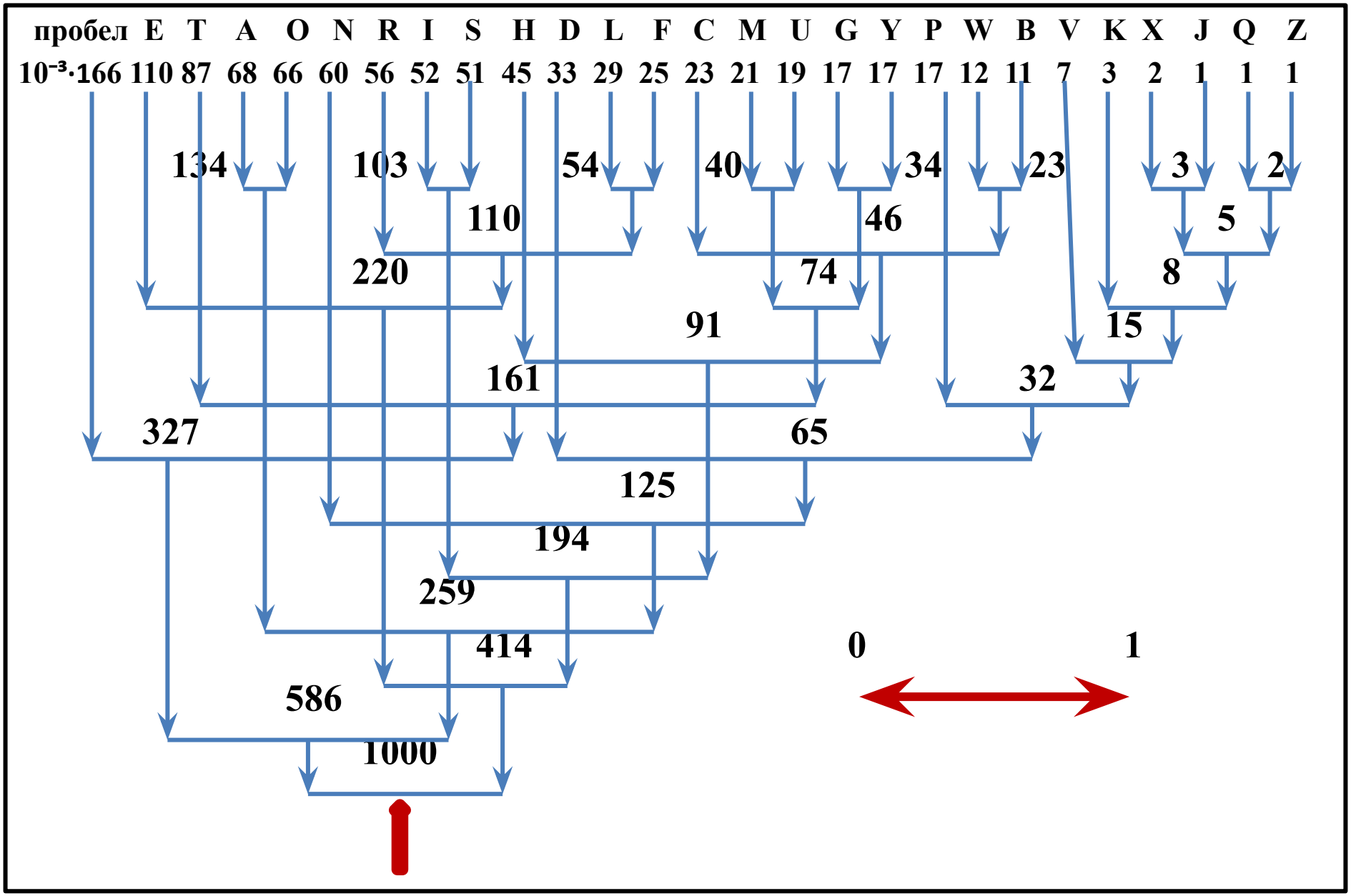


| ПРОБЕЛ | E | T | A |
|---|---|---|---|
| 0,166 | 0,110 | 0,087 | 0,068 |
| O | N | R | I |
| 0,066 | 0,060 | 0,056 | 0,052 |
| S | H | D | L |
| 0,051 | 0,045 | 0,033 | 0,029 |
| F | C | M | U |
| 0,025 | 0,023 | 0,021 | 0,019 |
| G | Y | P | W |
| 0,017 | 0,017 | 0,017 | 0,012 |
| B | V | K | X |
| 0,011 | 0,007 | 0,003 | 0,002 |
| J | Q | Z | |
| 0,001 | 0,001 | 0,001 | |

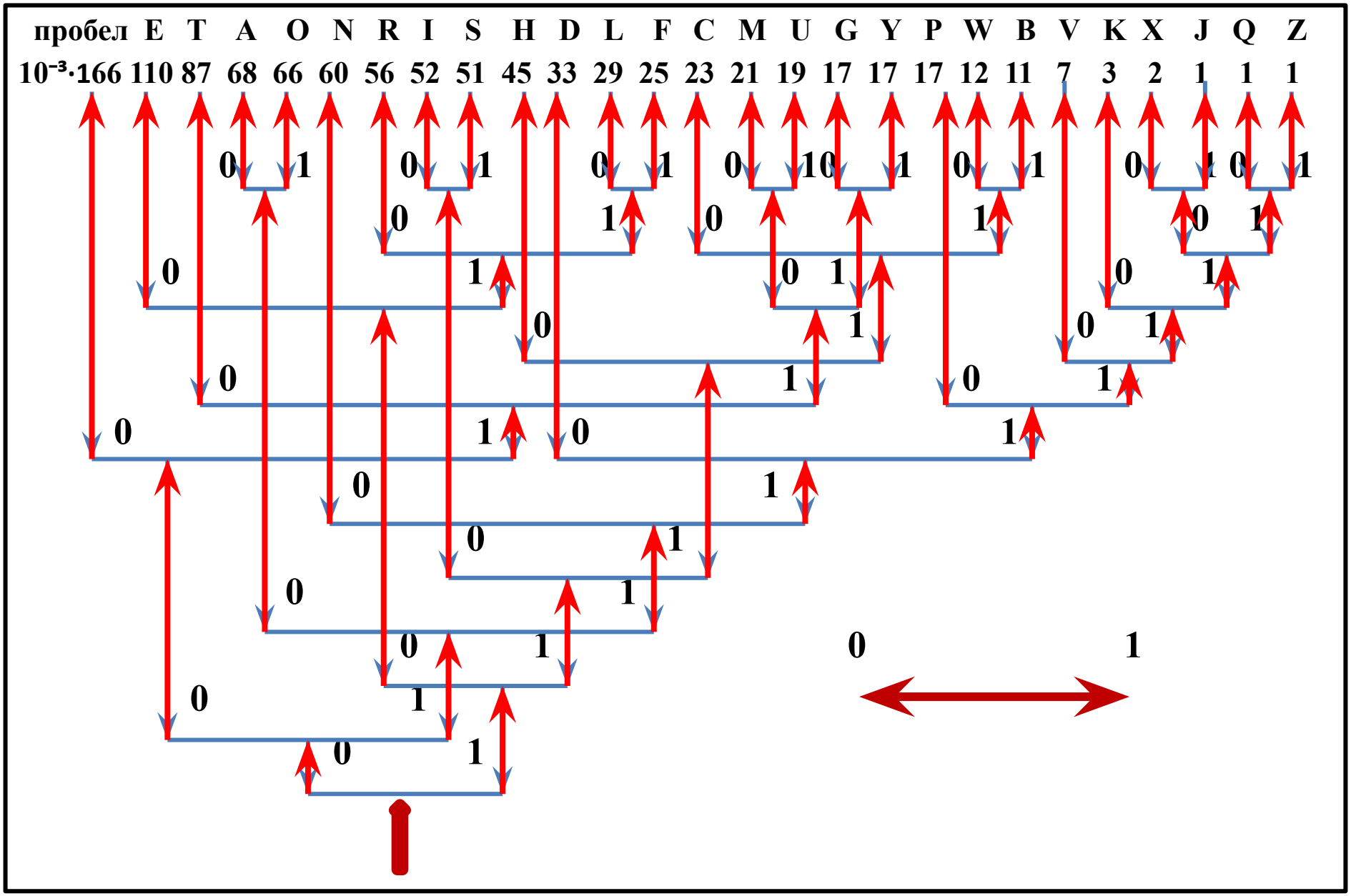
# Последовательность построения дерева Хаффмана

1. 1(Q)+1(Z)=2(QZ)
2. 1(J)+2(X)=3(JX)
3. 2(QZ)+3(JX)=5(QZJX)
4. 3(K)+5(QZJX)=8(KQZJX)
5. 7(V)+8(KQZJX)=15(VKQZJX)
6. 11(B)+12(W)=23(BW)
7. 15(VKQZJX )+17(P)=32(VKQZJXP)
8. 17(Y)+17(G)=34(YG)
9. 19(U)+21(M)=40(UM)
10. 23(C)+23(BW)=46(CBW)
11. 25(F)+29(L)=54(FL)
12. 32(VKQZJXP)+33(D)= 65(VKQZJXPD)
13. 34(YG)+40(UM)=74(YGUM)
14. 45(H)+46(CBW)=91(HCBW)
15. 51(S)+52(I)=103(SI)
16. 54(FL)+ 56(R)=110(FLR)
17. 60(N)+ 65(VKQZJXPD)=125(NVKQZJXPD)
18. 66(O)+68(A)= 134(OA)
19. 74(YGUM)+87(T)=161(YGUMT)
20. 91(HCBW)+103(SI)=194(HCBWSI)
21. 110(E)+110(FLR)= 220(EFLR)
22. 125(NVKQZJXPD)+134(OA)=259(NVKQZJXPDOA)
23. 161(YGUMT)+166(_)=327(YGUMT_)
24. 194(HCBWSI)+220(EFLR)=414(HCBWSIEFLR)
25. 259(NVKQZJXPDOA)+327(YGUMT_)=586(NVKQZJXPDOAYGUMT_)
26. 414(HCBWSIEFLR)+586(NVKQZJXPDOAYGUMT_)=1000(HCBWSIEFLRNVKQZJXPDOAYGUMT_)

# Дерево Хаффмана

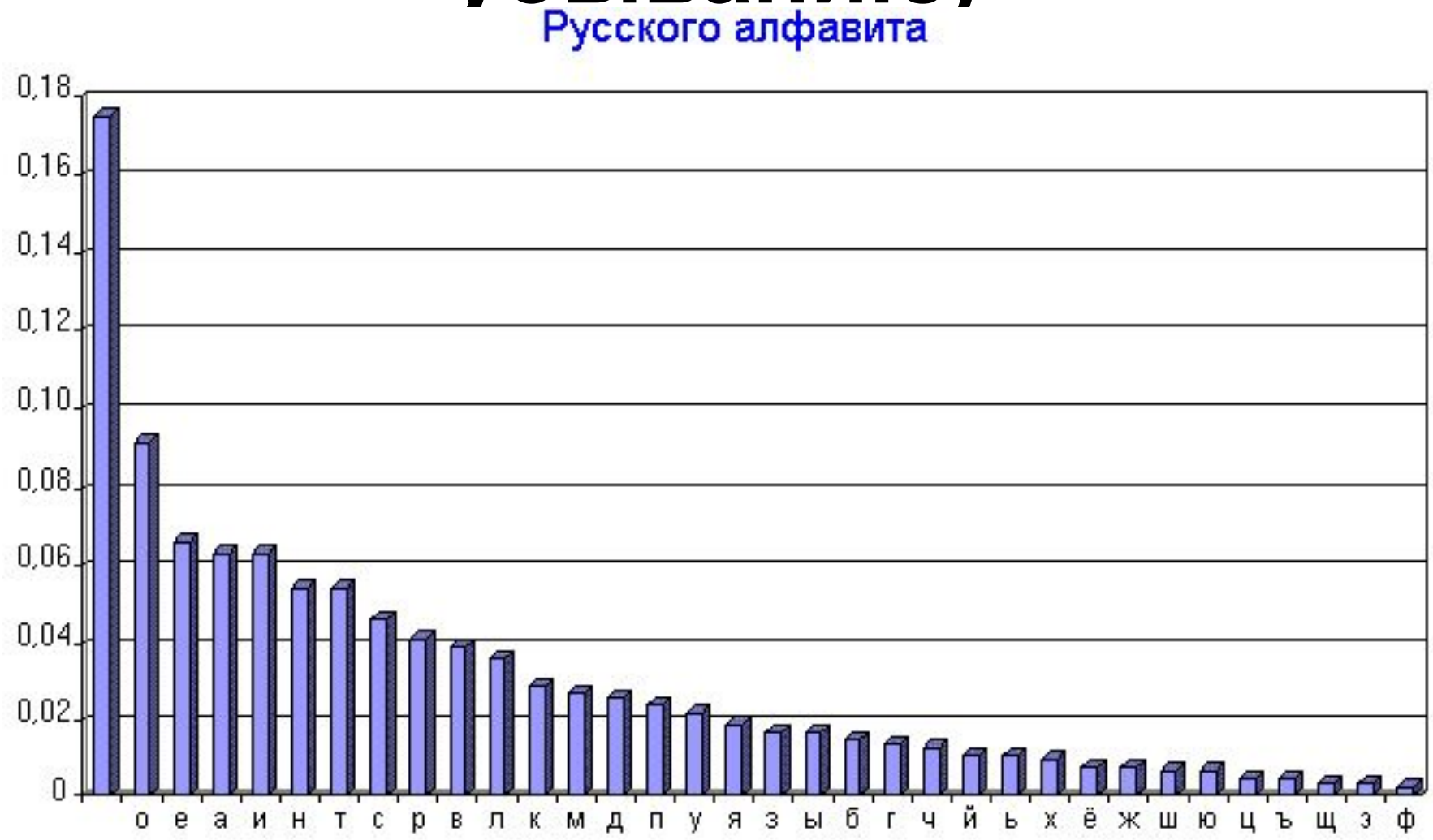


# Дерево Хаффмана



| ПРОБЕЛ | E | T | A |
|---|---|---|---|
| 000 | 100 | 0010 | 0100 |
| O | N | R | I |
| 0101 | 0110 | 1010 | 1100 |
| S | H | D | L |
| 1101 | 1110 | 01110 | 10110 |
| F | C | M | U |
| 10111 | 11110 | 001100 | 001101 |
| G | Y | P | W |
| 001110 | 001111 | 011110 | 111110 |
| B | V | K | X |
| 111111 | 0111110 | 01111110 | 0111111100 |
| J | Q | Z | |
| 0111111101 | 0111111110 | 0111111111 | |

# Статистика букв (по убыванию)

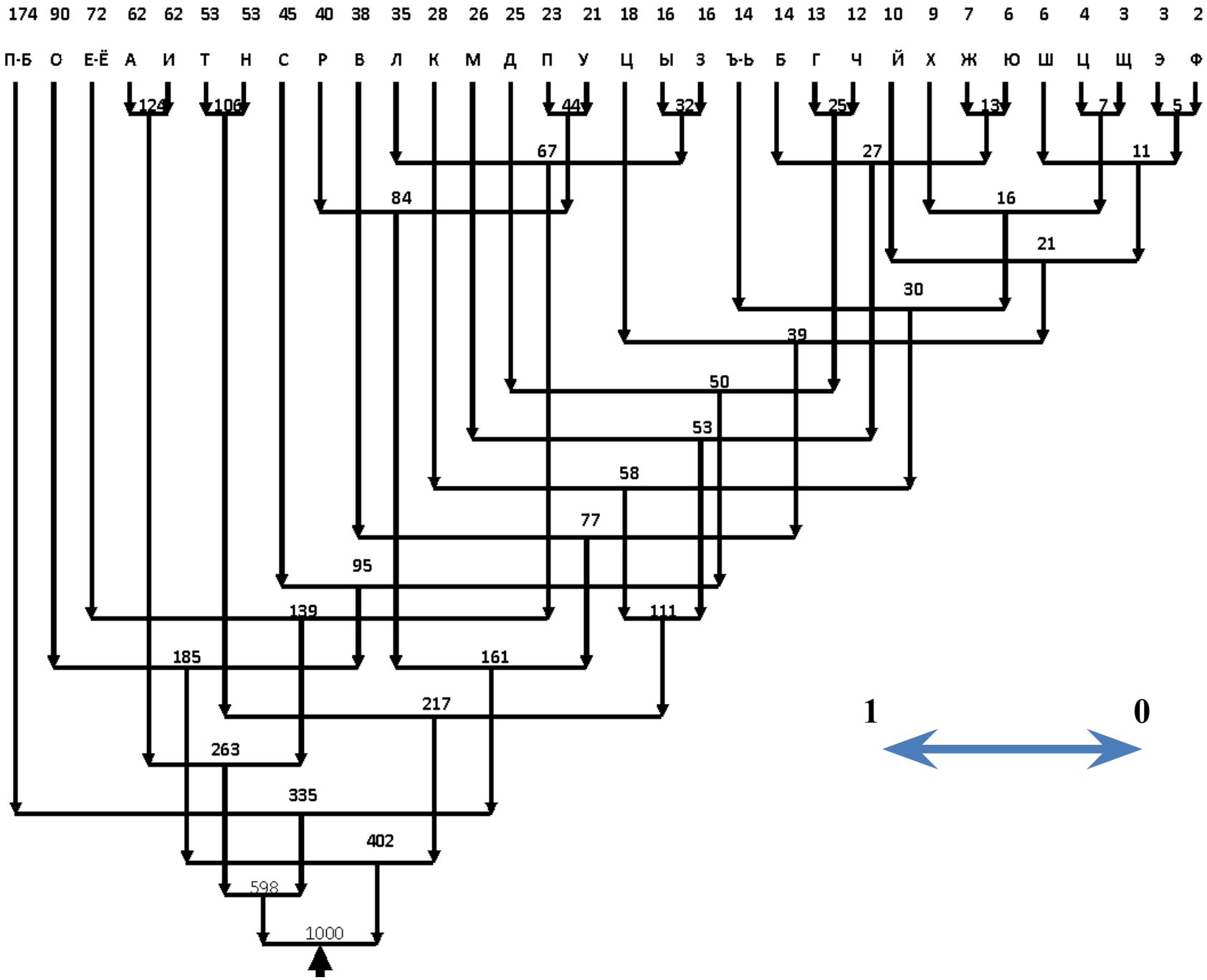


# Статистика букв (по алфавиту)

| ПРОБЕЛ | О | Е,Ё | А |
|---|---|---|---|
| 0,174 | 0,090 | 0,072 | 0,062 |
| И | Т | Н | С |
| 0,062 | 0,053 | 0,053 | 0,045 |
| Р | В | Л | К |
| 0,040 | 0,038 | 0,035 | 0,028 |
| М | Д | П | У |
| 0,026 | 0,025 | 0,023 | 0,021 |
| Я | Ы | З | Ь,Ъ |
| 0,018 | 0,016 | 0,016 | 0,014 |
| Б | Г | Ч | Й |
| 0,014 | 0,013 | 0,012 | 0,010 |
| Х | Ж | Ю | Ш |
| 0,009 | 0,007 | 0,006 | 0,006 |
| Ц | Щ | Э | Ф |
| 0,004 | 0,003 | 0,003 | 0,002 |

# Последовательность построения дерева Хаффмана

1. 2(Ф)+3(Э)=5(ФЭ)
2. 3(Щ)+4(Ц)=7(ЩЦ)
3. 5(ФЭ)+6(Ш)=11(ФЭШ)
4. 6(Ю)+7(Ж)=13(ЮЖ)
5. 7(ЩЦ)+9(Х)=16(ЩЦХ)
6. 10(Й)+11(ФЭШ)=21(ЙФЭШ)
7. 12(Ч)+13(Г)=25(ЧГ)
8. 13(ЮЖ)+14(Б)=27(ЮЖБ)
9. 14(Ъ-Ь)+16(ЩЦХ)=30(Ъ-ЬЩЦХ)
10. 16(Ы)+16(З)=32(ЫЗ)
11. 18(Ц)+21(ЙФЭШ)=39(ЦЙФЭШ)
12. 21(У)+23(П)= 44(УП)
13. 25(Д)+25(ЧГ)= 50(ДЧГ)
14. 26(М)+27(ЮЖБ)=53(МЮЖБ)
15. 28(К)+30(Ъ-ЬЩЦХ)=58(КЪ-ЬЩЦХ)
16. 35(Л)+ 32(ЫЗ)=67(ЛЫЗ)
17. 38(В)+ 39(ЦЙФЭШ)=77(ВЦЙФЭШ)
18. 40(Р)+44(УП)= 84(РУП)
19. 45(С)+50(ДЧГ)=95(СДЧГ)
20. 53(Т)+53(Н)=106(ТН)
21. 53(МЮЖБ)+58(КЪ-ЬЩЦХ)= 111(МЮЖБКЪ-ЬЩЦХ)
22. 62(А)+62(И)=124(АИ)
23. 72(Е-Ё)+67(ЛЫЗ)=139(Е-ЁЛЫЗ)
24. 77(ВЦЙФЭШ)+84(РУП)=161(ВЦЙФЭШРУП)
25. 90(О)+95(СДЧГ)=185(ОСДЧГ)
26. 106(ТН)+111(МЮЖБКЪ-ЬЩЦХ)=217(ТНМЮЖБКЪ-ЬЩЦХ)
27. 124(АИ)+139(Е-ЁЛЫЗ)=263(АИЕ-ЁЛЫЗ)
28. 161(ВЦЙФЭШРУП)+174(_)=335(ВЦЙФЭШРУП_)
29. 185(ОСДЧГ)+217(ТНМЮЖБКЪ-ЬЩЦХ)=402(ОСДЧГТНМЮЖБКЪ-ЬЩЦХ)
30. 263(АИЕ-ЁЛЫЗ)+335(ВЦЙФЭШРУП_)= 598(АИЕ-ЁЛЫЗВЦЙФЭШРУП_)
31. 402(ОСДЧГТНМЮЖБКЪ-ЬЩЦХ)+598(АИЕ-ЁЛЫЗВЦЙФЭШРУП_)=1000(ОСДЧГТНМЮЖБКЪ-ЬЩЦХАИЕ-ЁЛЫЗВЦЙФЭШРУП_)


174 90 72 62 62 53 53 45 40 38 35 28 26 25 23 21 18 16 16 14 14 13 12 10 9 7 6 6 4 3 3 2
П-Б О Е-Ё А И Т Н С Р В Л К М Д П У Ц Ы З Ъ-Ь Б Г Ч Й Х Ж Ю Ш Ц Щ Э Ф
124
106
44
32
25
13
7
5
67
27
11
84
16
21
30
39
50
53
58
77
95
139
111
185
161
217
263
335
402
598
1000
1
0

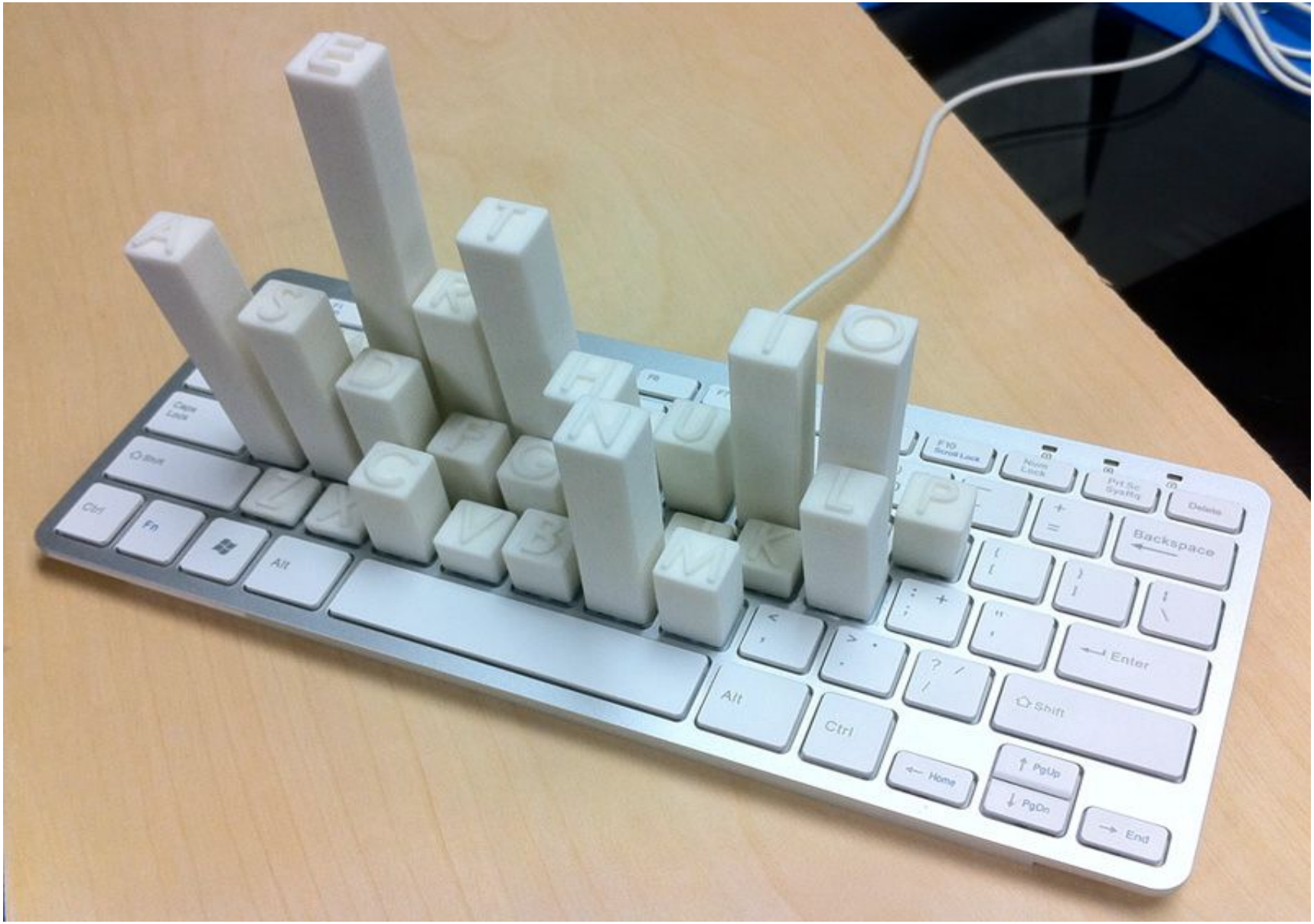
| ПРОБЕЛ | А | Б | В |
|---|---|---|---|
| 101 | 1111 | 000001 | 10001 |
| Г | Д | Е,Ё | Ж |
| 010001 | 01001 | 1101 | 0000001 |
| З | И | Й | К |
| 110000 | 1110 | 1010001 | 00011 |
| Л | М | Н | О |
| 11001 | 00001 | 0010 | 011 |
| П | Р | С | Т |
| 100101 | 10011 | 0101 | 0011 |
| У | Ф | Х | Ц |
| 100100 | 100000000 | 0001001 | 00010001 |
| Ч | Ш | Щ | Ъ,Ь |
| 010000 | 10000001 | 00010000 | 000101 |
| Ы | Э | Ю | Я |
| 110001 | 100000001 | 0000000 | 100001 |

**Зависимости букв русского алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А. А. Марковым (1856 – 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В частности им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г*, *г*), гласная-согласная (*г*, *с*), согласная-гласная (*с*, *г*), согласная-согласная (*с*, *с*) в русском тексте длиной в $10^5$ знаков. Результаты подсчета отражены в следующей таблице:**

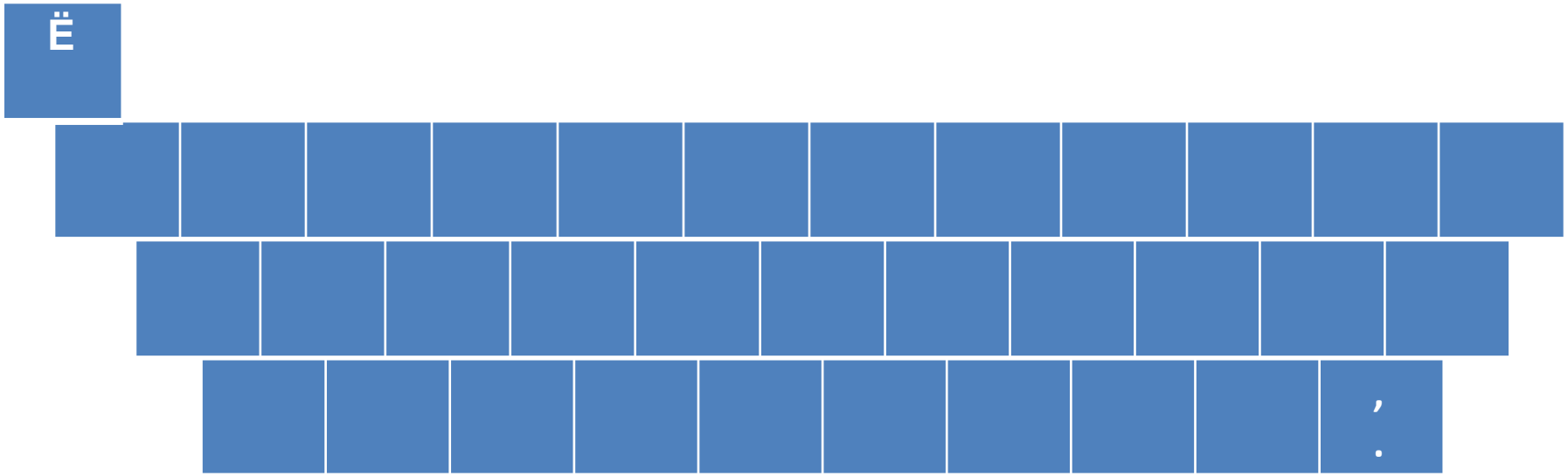
| | Гласная | Согласная | Итого |
|---|---|---|---|
| Гласная | 6 588 | 38 310 | 44 898 |
| Согласная | 38 296 | 16 806 | 55 102 |

**Вычисляемые по этой таблице условные и безусловные вероятности могут служить приближениями соответствующих условных и безусловных вероятностей, вычисленных на текстах большего объема. Было получено $p(г/с)\approx 0.663$, $p(с/г)\approx 0.872$ и $p(г)\approx 0.432$, $p(с)\approx 0.568$. (Сравните с данными из таблицы).**

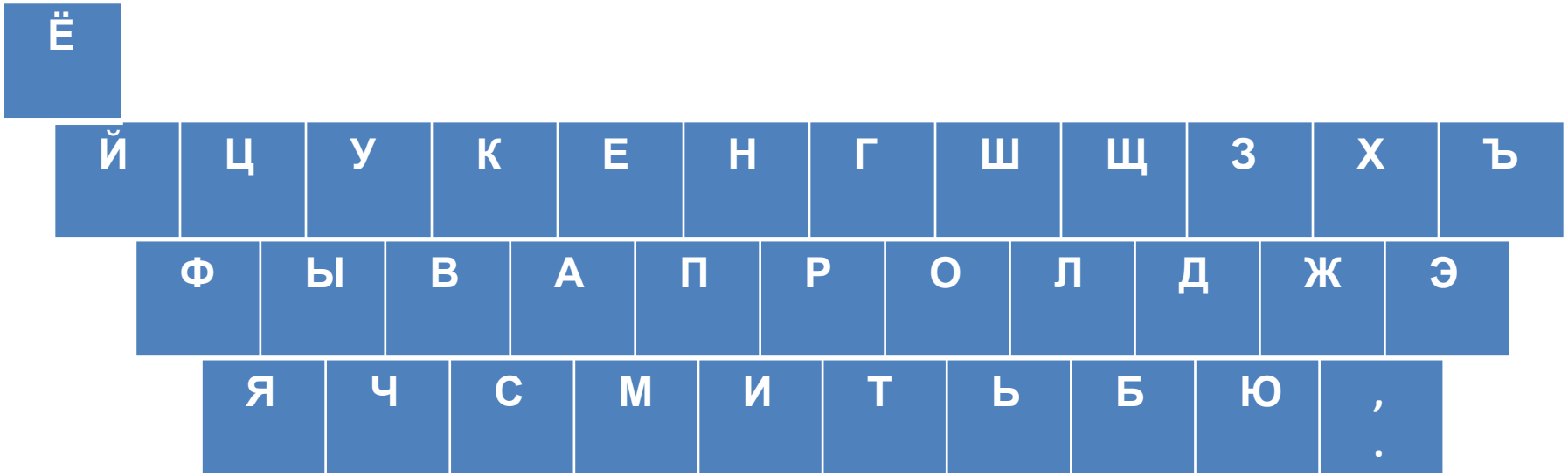
**После А. А. Маркова зависимость появления букв текста исследовал методами теории информации К. Шеннон. Им было показано, в частности, что такая зависимость ощутима на глубину приблизительно в 30 знаков, после чего она практически отсутствует.**


Backspace
Enter
Shift
Alt
Ctrl
Home
PgUp
PgDn
End

# Спроектируем клавиатуру для русского языка!



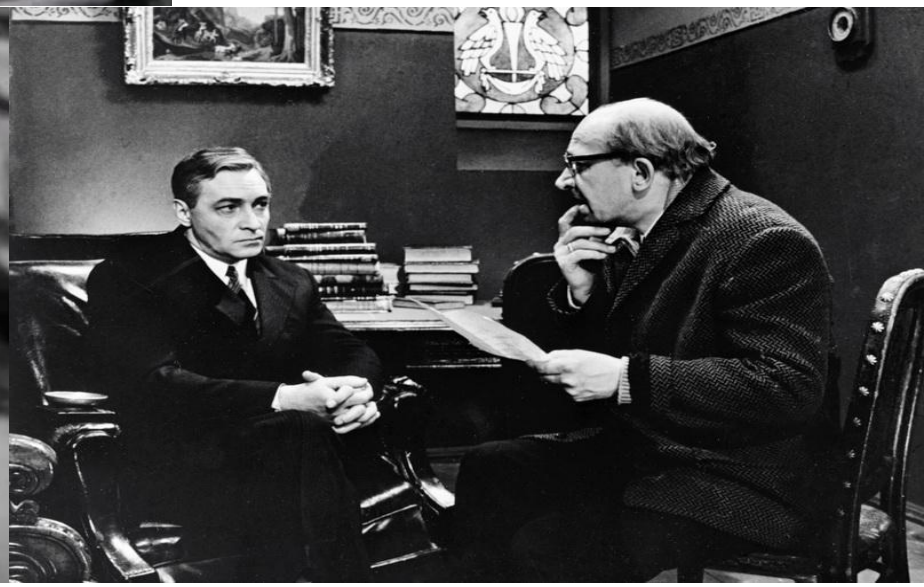
# Клавиатура для русского языка!



Переключатель зон красящей ленты
Клавиша пропуска границы поля
Рычаг установки и гашения табуляции
Клавиша возвратного шага
Клавиша замка регистра
Клавиша табулятора
Клавиши перевода регистра

# Кодирование – это отображение элементов одного множества элементами другого множества

***Оказавшись в Берне, профессор Плейшнер забыл код, которому его учил Штирлиц.***



# Этапы и виды отображений (преобразований)

| | |
|---|---|
| А= В | Возможно однозначное соответствие, как правило взаимно однозначное. Избыточности нет. |
| А> В | Невозможно однозначное соответствие. Избыточности нет. |
| А< В | Возможно однозначное соответствие, как взаимно так и не взаимно однозначное. Имеется избыточность. |

# Цели кодирования

1. Первичное кодирование с целью достижения скорости кодирования равной энтропии источника (избыточность стремиться к 0).
2. Первичное кодирование по п.1, но и с целью минимизации искажений элементов множества А из-за искажений элементов множества В.
3. Не взаимно однозначное кодирование для достижения специальных целей.
4. Шифрование.
5. Кодирование для согласования с характеристиками среды передачи.
6. Помехоустойчивое кодирование (внесение дополнительной избыточности)

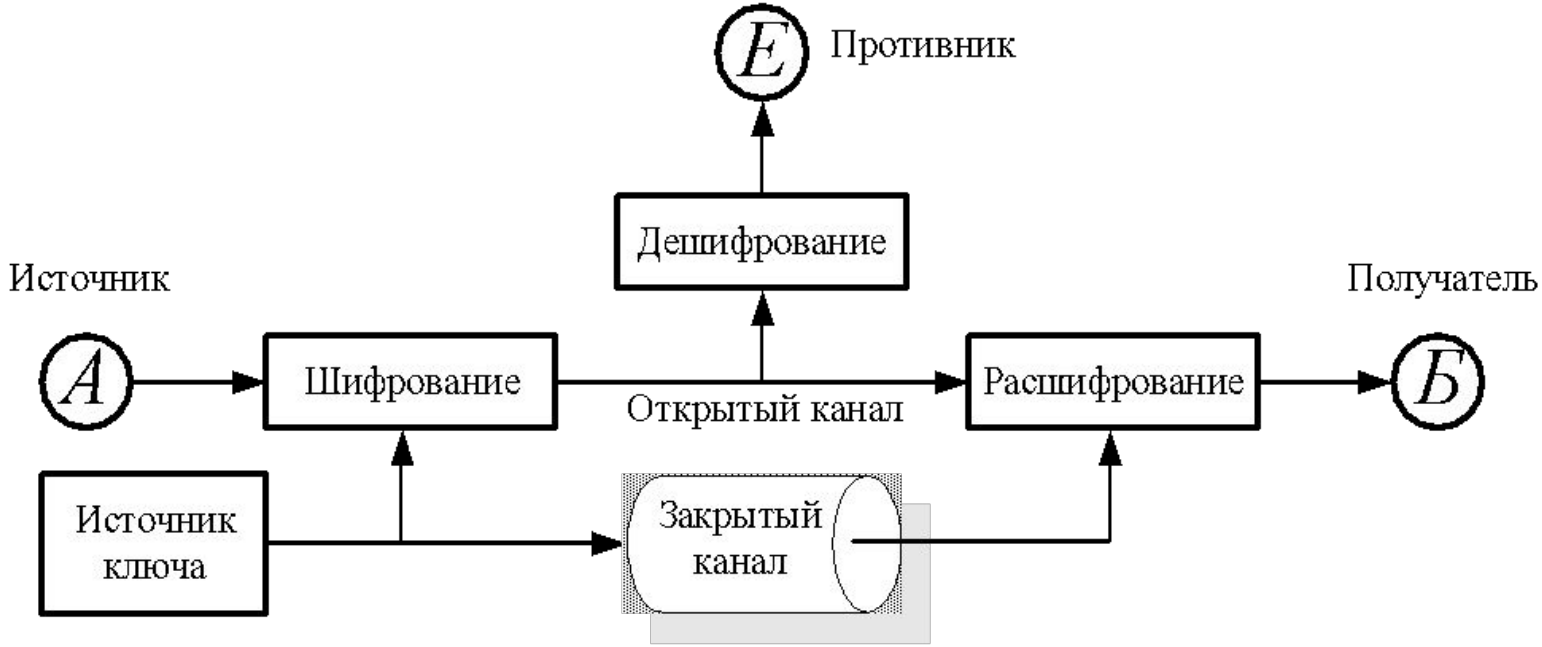
# ВВЕДЕНИЕ В ТЕОРИЮ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

- ***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,**

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.

# Шифрование и расшифровывание с помощью кода Цезаря

**Если $N$ - количество букв в алфавите, $x_i$ - номер буквы из открытого текста, $K$ - ключ (целое число), то зашифрованная буква по коду Цезаря имеет номер:**

$$y_i = x_i + K \pmod N,$$

**при расшифровывании:**

$$x_i = y_i - K \pmod N.$$

**Например, при $K$ = 3 буква «А» станет «Г», а буква «Ю» - «Б».**

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | | 9 | | 17 | | 25 | |
| 2 | | 10 | | 18 | | 26 | |
| 3 | | 11 | | 19 | | 27 | |
| 4 | | 12 | | 20 | | 28 | |
| 5 | | 13 | | 21 | | 29 | |
| 6 | | 14 | | 22 | | 30 | |
| 7 | | 15 | | 23 | | 31 | |
| 8 | | 16 | | 24 | | 32 | |

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | Л | 9 | Г | 17 | Ы | 25 | У |
| 2 | К | 10 | В | 18 | Ъ | 26 | Т |
| 3 | Й | 11 | Б | 19 | Щ | 27 | С |
| 4 | И | 12 | А | 20 | Ш | 28 | Р |
| 5 | З | 13 | Я | 21 | Ч | 29 | П |
| 6 | Ж | 14 | Ю | 22 | Ц | 30 | О |
| 7 | Е | 15 | Э | 23 | Х | 31 | Н |
| 8 | Д | 16 | Ь | 24 | Ф | 32 | М |

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | ЛД | 9 | ГЬ | 17 | Ы | 25 | УМ |
| 2 | КГ | 10 | ВЫ | 18 | Ъ | 26 | ТЛ |
| 3 | ЙВ | 11 | БЪ | 19 | ЩТ | 27 | СК |
| 4 | ИБ | 12 | АЩ | 20 | ШС | 28 | РЙ |
| 5 | ЗА | 13 | ЯШ | 21 | ЧР | 29 | ПИ |
| 6 | ЖЯ | 14 | ЮЧ | 22 | ЦП | 30 | ОЗ |
| 7 | ЕЮ | 15 | ЭЦ | 23 | ХО | 31 | НЖ |
| 8 | ДЭ | 16 | Ь | 24 | ФН | 32 | МЕ |

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | ЛДЫ | 9 | ГЬ | 17 | Ы | 25 | УМГ |
| 2 | КГ | 10 | ВЫТ | 18 | Ъ | 26 | ТЛВ |
| 3 | ЙВ | 11 | БЪ | 19 | ЩТ | 27 | СКБ |
| 4 | ИБШ | 12 | АЩ | 20 | ШС | 28 | РЙ |
| 5 | ЗАЧ | 13 | ЯШП | 21 | ЧРЗ | 29 | ПИЯ |
| 6 | ЖЯ | 14 | ЮЧ | 22 | ЦП | 30 | ОЗЮ |
| 7 | ЕЮ | 15 | ЭЦ | 23 | ХОЕ | 31 | НЖ |
| 8 | ДЭФ | 16 | Ь | 24 | ФН | 32 | МЕЬ |

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | ЛДЫ | 9 | ГЬ | 17 | Ы | 25 | УМГ |
| 2 | КГ | 10 | ВЫТА | 18 | Ъ | 26 | ТЛВ |
| 3 | ЙВ | 11 | БЪ | 19 | ЩТ | 27 | СКБ |
| 4 | ИБШ | 12 | АЩ | 20 | ШС | 28 | РЙ |
| 5 | ЗАЧЕ | 13 | ЯШП | 21 | ЧРЗ | 29 | ПИЯН |
| 6 | ЖЯ | 14 | ЮЧ | 22 | ЦП | 30 | ОЗЮ |
| 7 | ЕЮ | 15 | ЭЦ | 23 | ХОЕ | 31 | НЖ |
| 8 | ДЭФ | 16 | Ь | 24 | ФН | 32 | МЕЬ |

# Взлом кода Цезаря (слово «МЕЬКЧ»)

| Ключ | Слово | Ключ | Слово | Ключ | Слово | Ключ | Слово |
|---|---|---|---|---|---|---|---|
| 1 | ЛДЫ | 9 | ГЬ | 17 | Ы | 25 | УМГ |
| 2 | КГ | 10 | ВЫТА | 18 | Ъ | 26 | ТЛВ |
| 3 | ЙВ | 11 | БЪ | 19 | ЩТ | 27 | СКБ |
| 4 | ИБШ | 12 | АЩ | 20 | ШС | 28 | РЙ |
| 5 | ЗАЧЕТ | 13 | ЯШП | 21 | ЧРЗ | 29 | ПИЯНЪ |
| 6 | ЖЯ | 14 | ЮЧ | 22 | ЦП | 30 | ОЗЮ |
| 7 | ЕЮ | 15 | ЭЦ | 23 | ХОЕ | 31 | НЖ |
| 8 | ДЭФ | 16 | Ь | 24 | ФН | 32 | МЕЬ |

# «Квадрат» Виженера

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

# Шифрование и расшифровывание с помощью квадрата Виженера

**Передается:**

**ТЕОРИЯ ИНФОРМАЦИИ**

**Ключевое слово:**

**МТУСИ**

**Зашифрованная последовательность:**

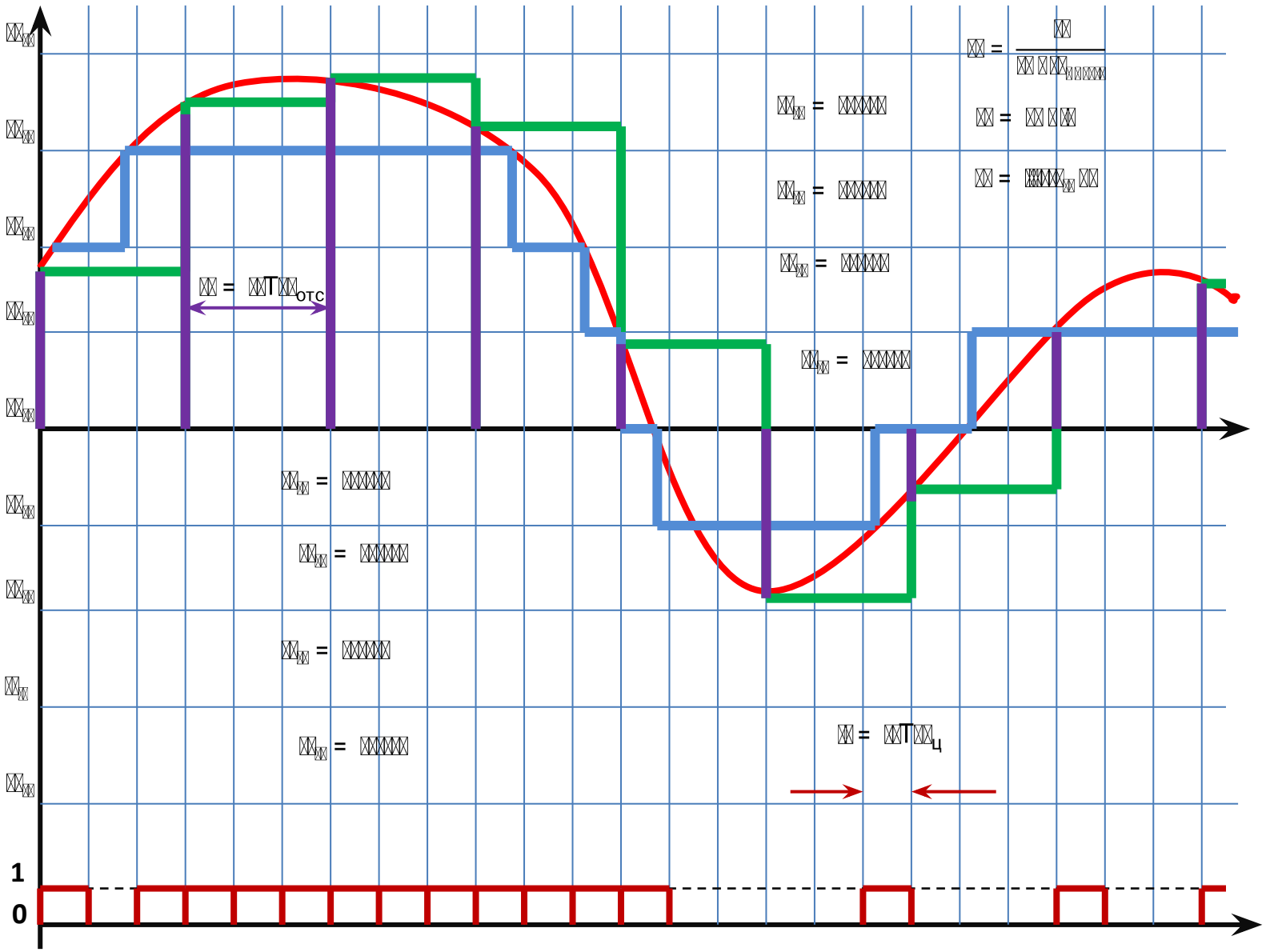
| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Исходн.** | т | е | о | р | и | я | _ | и | н | ф | о | р | м | а | ц | и | и |
| **Ключ** | м | т | у | с | и | м | т | у | с | и | м | т | у | с | и | м | т |
| **Шифр** | х | л | й | й | т | а | р | ю | х | ж | д | ф | э | р | х | о | д |

# Шифрование и расшифровывание с помощью квадрата Виженера

**При расшифровывании по буквам ключа берутся строчки из «квадрата» и в них находится буква зашифрованной последовательности.**

**Затем по «столбику» определяется расшифрованная буква. В итоге имеем:**

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ключ** | м | т | у | с | и | м | т | у | с | и | м | т | у | с | и | м | т |
| **Шифр** | х | л | й | й | т | а | р | ю | х | ж | д | ф | э | р | х | о | д |
| **Исходн.** | т | е | о | р | и | я | _ | и | н | ф | о | р | м | а | ц | и | и |


1
0

| 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 |

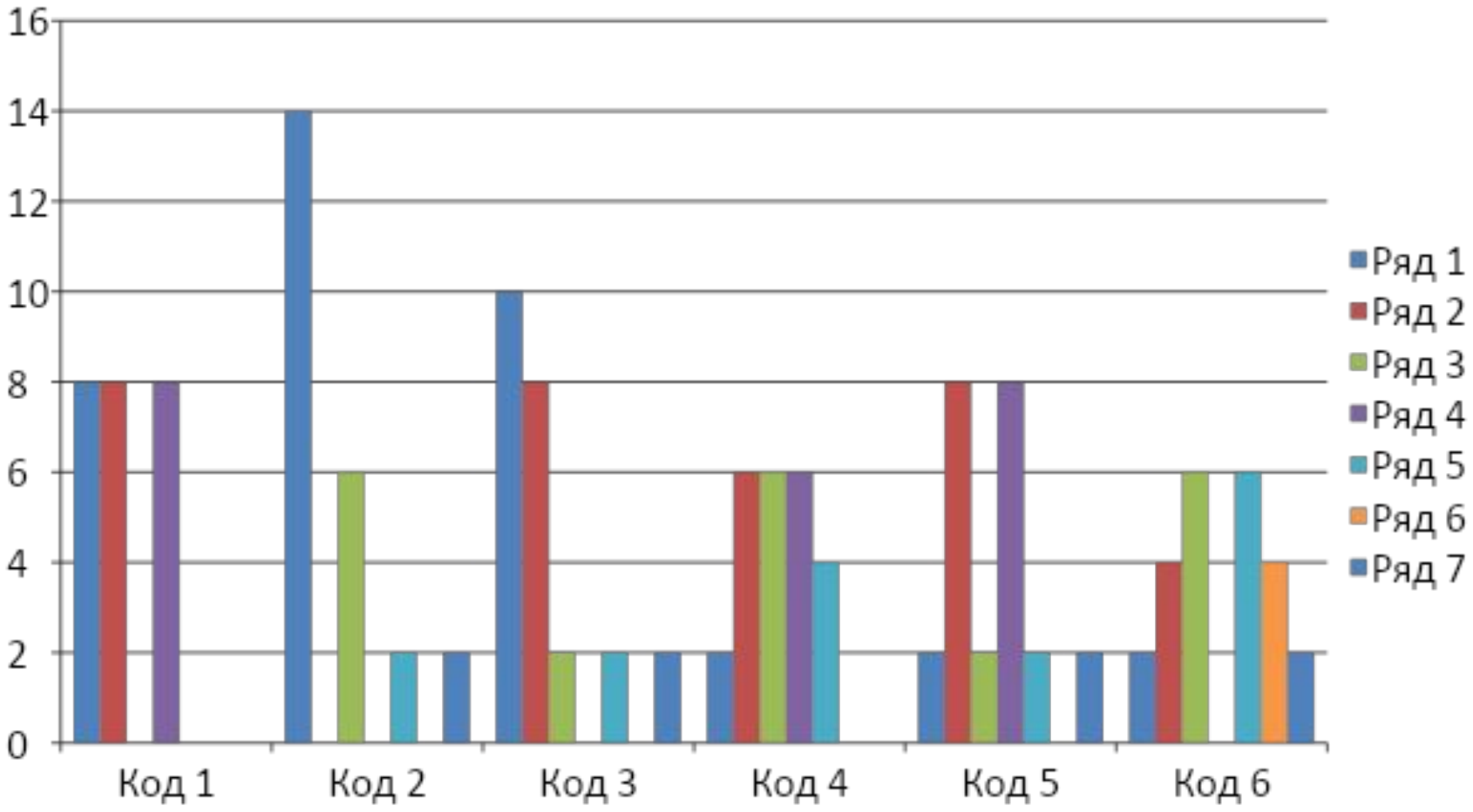
| Код в ИКМ (3) | 011 | 010 | 001 | 000 | 100 | 101 | 110 | 111 | Итого |
|---|---|---|---|---|---|---|---|---|---|
| 3, 2, 1 | 7, 2, 1 | 5, 2, 1 | 3, 2, 1 | 1, 2, 1 | 1, 2, 1 | 3, 2, 1 | 5, 2, 1 | 7, 2, 1 | 7x2+ 5x2+ 3x2+ 2x8+ 1x10= 56 |
| 3-2, 2-1, 3-1 | 5, 3, 6 | 3, 1, 6 | 5, 1, 2 | 3, 3, 2 | 3, 3,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

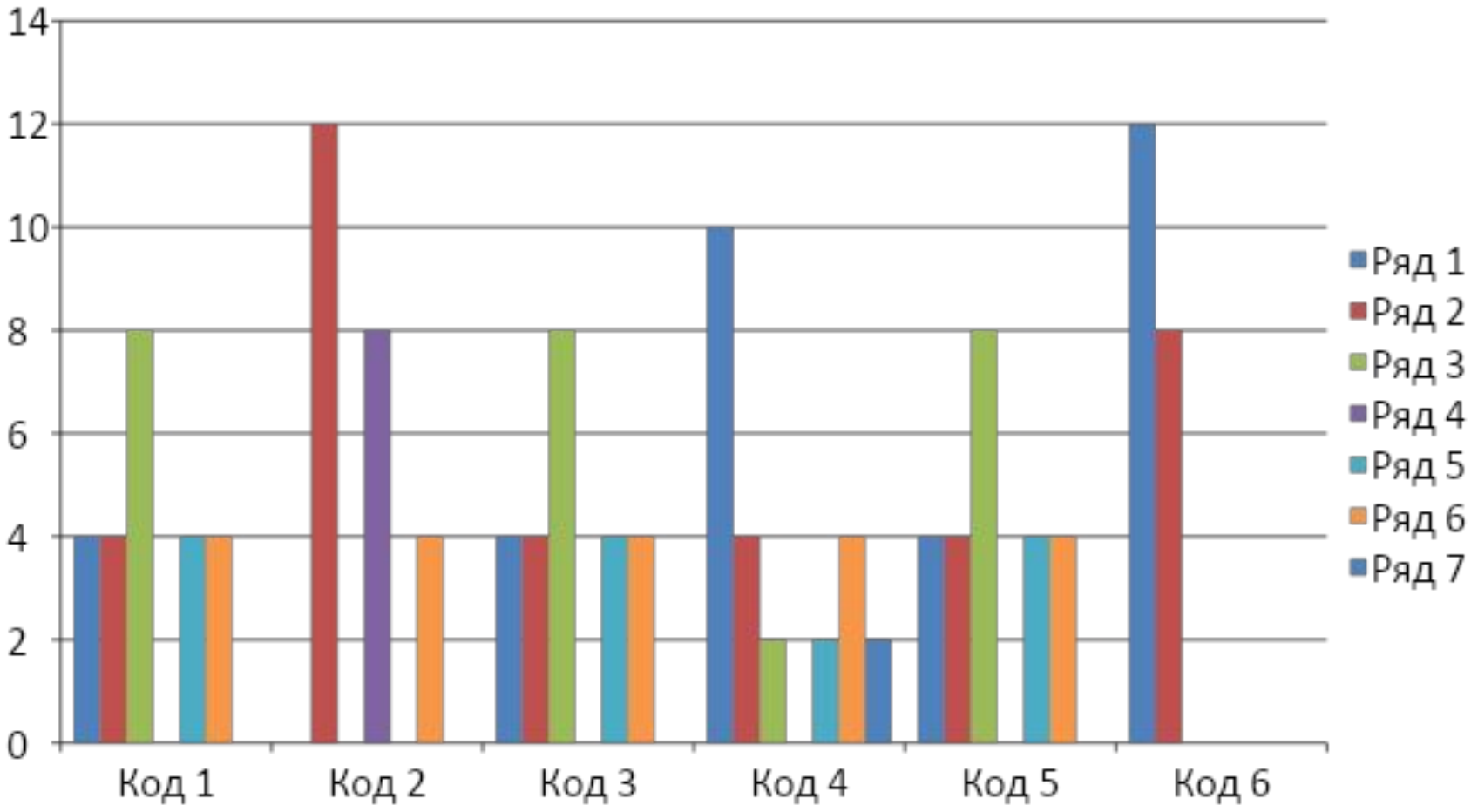
| Код Ми 3 (5) | 000 | 111 | 001 | 110 | 010 | 101 | 011 | 100 | Итого |
|---|---|---|---|---|---|---|---|---|---|
| 3, 2, 1 | 7, 4, 2 | 5, 4, 2 | 3, 4, 2 | 1, 4, 2 | 1, 4, 2 | 3, 4, 2 | 5, 4, 2 | 7, 4, 2 | 7x2+ 5x2+ 4x8+ 3x2+ 2x8+ 1x2= 80 |
| 3-2, 2-1, 3-1 | 3, 6, 5 | 1, 6, 3 | 1, 2, 5 | 3, 2, 3 | 3,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

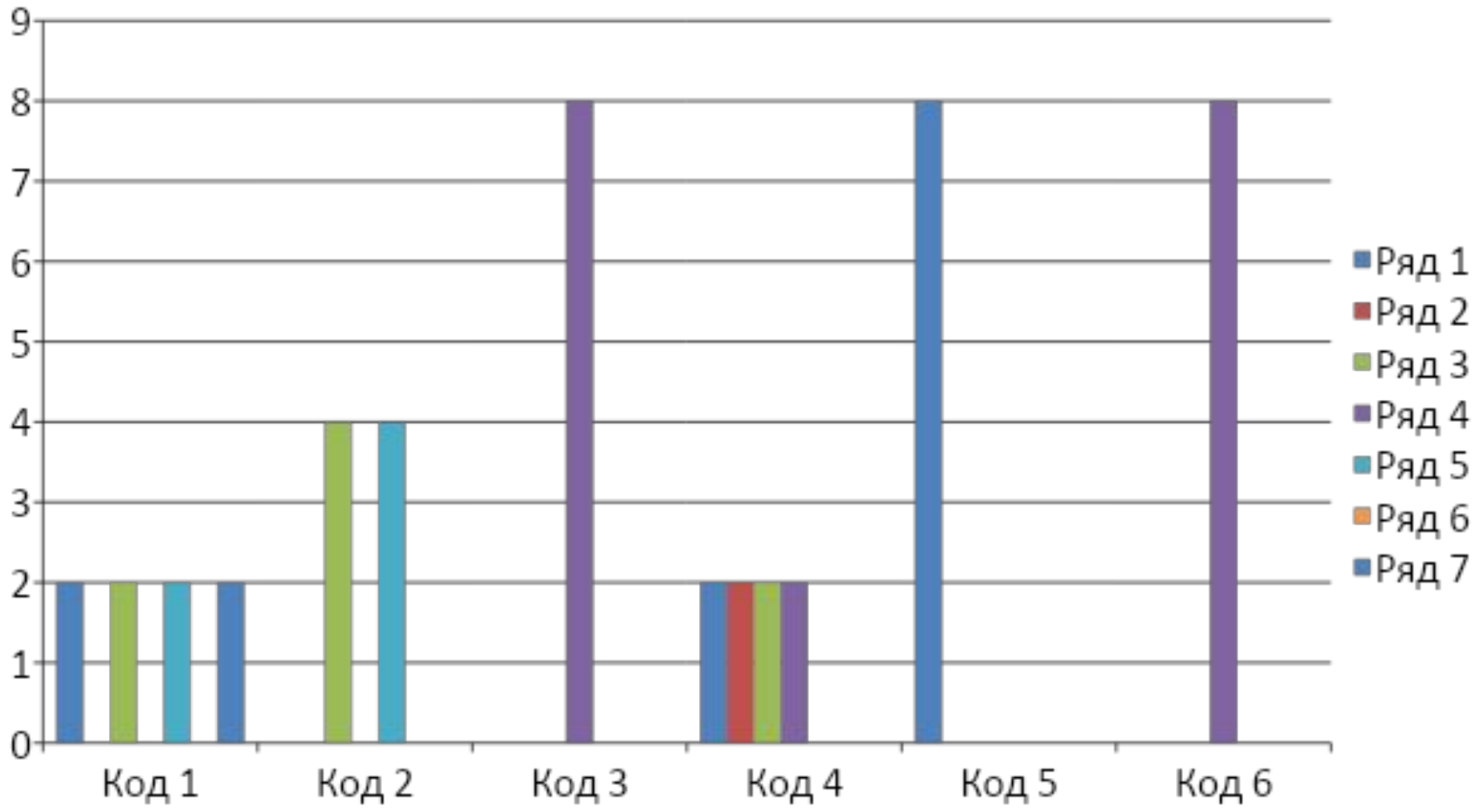
| Код | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Итого 1-кр | 56 | 56 | 56 | 76 | 80 | 96 |



| 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:

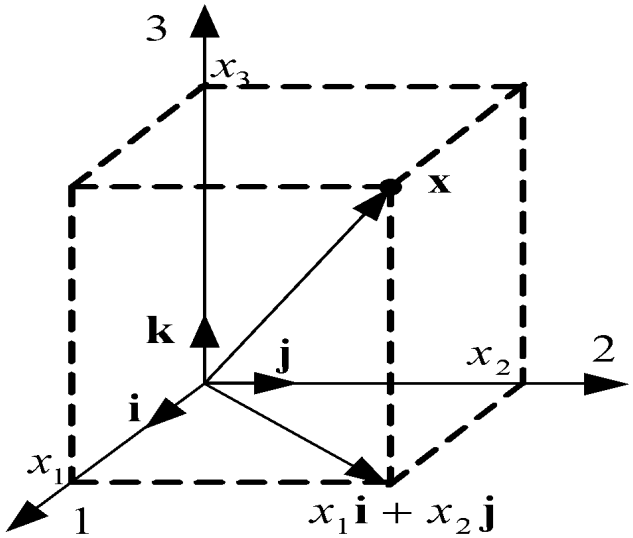
- При n=1 имеем комбинации 0 и 1.
  Для них: $D_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- При n=2 имеем комбинации 00; 01; 10 и 11.

  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: $D_n = \begin{pmatrix} D_{n-1} & D_{n-1} + J \\ D_{n-1} + J & D_{n-1} \end{pmatrix}$,

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

- **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:

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

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

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

$$L_n = \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{cccc} A & B & C & D \\ \begin{matrix} \\ \\ \\ \\ \end{matrix} & \begin{matrix} \\ \\ \\ \\ \end{matrix} & \begin{matrix} \\ \\ \\ \\ \end{matrix} & \begin{matrix} \\ \\ \\ \\ \end{matrix} \\ \\ \\ \\ \end{array} \begin{array}{c} A \\ B \\ C \\ D \end{array}$$

# Матрица потерь для светофора

| | КРАСНЫЙ | ЖЕЛТЫЙ | ЗЕЛЕНЫЙ |
|---|---|---|---|
| КРАСНЫЙ | НЕТ 0 | СРЕДНИЕ 100 | БОЛЬШИЕ 1000 |
| ЖЕЛТЫЙ | МАЛЫЕ 10 | НЕТ 0 | СРЕДНИЕ 100 |
| ЗЕЛЕНЫ | | МАЛЫЕ | НЕТ |