**Федеральное агентство связи**

**Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования**

**ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ**

# ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

ЭБС ПГУТИ

**Самара**

Государственное бюджетное образовательное учреждение высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

# КОНТРОЛЬНЫЕ РАБОТЫ № 1 и 2 «СИСТЕМЫ СЧИСЛЕНИЯ» и «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Методические указания на выполнение контрольных работ
для студентов **заочного** отделения

по дисциплине «Информатика»,
(специальности 230400 и 230400у; 1ИСТ и 1ИСТу)

Автор-составитель доц., к.т.н. **Алексеев А.П.**
Под общей редакцией Алексеева А.П.
Рецензент д.т.н., проф. **Тарасов В.Н.**

ЭБС ПГУТИ

Самара, 2013 г.

## Введение

Контрольная работа позволяет освоить основные приемы перевода чисел из одной системы счисления в другую, изучить форматы данных, ознакомиться с приемами сжатия информации.

Постоянное увеличение объема конфиденциальной информации требует от специалистов знания современных методов криптографии и стеганографии. Данные методические указания позволяют освоить основные приемы шифрования и сокрытия информации.

Рекомендуемая литература


1. Алексеев А.П. Информатика 2007. – М.: СОЛОН-ПРЕСС.- 2007.- 608 с.
2. Алексеев А.П. Введение в Web-дизайн. Учебное пособие.- М.: СОЛОН-ПРЕСС, 2008.- 184 с.
3. Алексеев А.П., Орлов В.В., Сухова Е.Н. Изучение стеганографии на уроках информатики //Информатика и образование, № 8, 2007, стр. 65…72.
4. Алексеев А.П., Алексеев П.А., Мартяшина О.М., Сухова Е.Н. Изучение криптографии на уроках информатики //Информатика и образование, № 4, 2003, стр. 33…42.
5. Алексеев А. П., Орлов В.В. Стеганографические и криптографические методы защиты информации; учебное пособие. Самара: ИУНЛ ПГУТИ – 2010. - 330 с.
6. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем: Учебник для вузов. – СПб.: Питер, 2004. – 668 с.
7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации.- СПб.: Питер, 2005. – 703 с.


ЭБС ПГУТИ

## Контрольная работа № 1
## «Системы счисления»

**Задание 1**

1.1. Перевести числа из двоичной системы счисления (СС) в десятичную СС.

1.2. Перевести числа из десятичной СС в двоичную СС.

1.3. Перевести числа из двоичной СС в восьмеричную и шестнадцатеричную системы счисления.

Номер варианта определяется по последней цифре зачетной книжки (табл. 1).

Таблица 1

| | Задания | | |
|---|---|---|---|
| Вариант | 1.1 | 1.2 | 1.3. |
| 0 | 11001.011 | 123.250 | 1111111.101 |
| 1 | 10110.101 | 185.750 | 1010110.011 |
| 2 | 11100.011 | 112.125 | 1110110.101 |
| 3 | 11011.101 | 192.625 | 1010110.001 |
| 4 | 10100.011 | 116.750 | 1110100.111 |
| 5 | 11110.111 | 115.375 | 1101110.101 |
| 6 | 10011.011 | 178.750 | 1100101.011 |
| 7 | 11110.101 | 159.125 | 1110101.101 |
| 8 | 10111.111 | 145.625 | 1100100.011 |
| 9 | 11010.101 | 129.750 | 1011011.101 |

**Задание 2**

2.1. Выполнить четыре арифметические операции A+B, B-A, A*B, A/B над десятичными числами A и B (табл.2), представленными в двоичной СС. Вычитание произвести с использованием дополнительного кода. Результаты выполненных операций записать в двоичной, восьмеричной, шестнадцатеричной и десятичной СС.

Номер варианта определяется по предпоследней цифре зачетной книжки.

Таблица 2

| Вариант | A | B |
|---|---|---|
| 0 | 48 | 6 |
| 1 | 81 | 9 |
| 2 | 72 | 8 |
| 3 | 45 | 9 |
| 4 | 35 | 7 |
| 5 | 49 | 7 |
| 6 | 54 | 6 |
| 7 | 48 | 8 |
| 8 | 63 | 9 |

ОБС ПГУТИ

| | | |
|---|---|---|
| 9 | 56 | 7 |

**Задание 3**

Представить положительное и отрицательное числа $+n_3n_2n_1$ и $-n_3n_2n_1$ в следующих форматах (здесь $n_3,n_2,n_1$ – три последние цифры зачетной книжки).

3.1. В формате слово (2 байта) со знаком и фиксированной запятой.

3.2. В формате двойное слово (4 байта) с плавающей запятой.

3.3. В упакованном формате.

3.4. В распакованном формате.

**Задание 4**

Выполнить вручную сжатие информации методом RLE.

В качестве исходной фразы взять текст из табл. 3. С помощью таблицы CP-1251 (см. Приложение 1) преобразовать символы заданной фразы в десятичные числа, а затем десятичные числа перевести в двоичные числа. Выполнить архивацию, вычислить контрольные суммы и коэффициент сжатия.

Вариант определяется по последней цифре зачетной книжки.

Таблица 3

| Вариант | Текст |
|---|---|
| 0 | Кккккттттттто тттттам? |
| 1 | Длинношеее животное |
| 2 | Ураааааааааааа в атаку |
| 3 | Долг 3255566667444444 |
| 4 | Телефон 8904222211111 |
| 5 | Ауууууууу заблудились |
| 6 | Свидетельство 22263333 |
| 7 | Возраст 1000000000 лет |
| 8 | Заработали 522211112 |
| 9 | До дембеля 60440000 с |

ЭБ СПбГУТИ

## Контрольная работа № 2
## «Криптографические и стеганографические методы защиты информации»

Задание 1. Расшифровать криптограмму, зашифрованную шифром Цезаря (табл. 1).

Задание 2. Расшифровать криптограмму, зашифрованную шифром атбаш (табл. 2).

Задание 3. Расшифровать криптограмму, зашифрованную с помощью квадрата Полибия (табл. 3).

Задание 4. Расшифровать криптограмму, зашифрованную методом перестановок (табл. 4, 5).

Задание 5. Расшифровать криптограмму, зашифрованную методом гаммирования (табл. 6).

Задание 6. Извлечь информацию, стеганографически скрытую в данных.

Задание 7. Использованными пятью методами (задания 1…5) зашифровать свою фамилию.

*Примечание.*

Размер матрицы в методе перестановок и значение гаммы в задании 7 выбираются студентами самостоятельно.

### Задание 1. Дешифрировать сообщение (шифр Цезаря)

Номер варианта выбирается по последней цифре зачетной книжки.

Таблица 1

| Вар | Шифрограмма |
|---|---|
| 0 | СУОЮФЛЖВХОЛДСРГЕЗУЫЛРЗОЛДСЕНОЗХНЗ |
| 1 | ТСДЗЖЛХЗОЯОБДЛХТУЗЦЕЗОЛЪЛЕГХЯФЛОЦТСДЗЙЖЗРРСЁС |
| 2 | ЪЗПШЦЙЗРСЕСФХЯХЗПДСОЯЫЗЛРЧСУПГЩЛЛСРГФСЖЗУЙЛХ |
| 3 | ТУГЕЛОГЖОВЕФЗШСЖЛРГНСЕЮЗХСОЯНСЛФНОБЪЗРЛВУГКРЮЗ |
| 4 | ЛКСДУЗХГХЗОВНСОЗФГСФСДЗРРСЪХВХДЗОНЛ |
| 5 | ДЗФТУЛРЩЛТРСФХЯАХСРЗСХФХЦХФХЕЛЗТУЛРЩЛТСЕГЛШЛКСДЛОЛЗ |
| 6 | НГНПГОССНУЮОЗРРЮШФУЗЖЛСНСОЯЩСЕГРРЮШ |
| 7 | НХСЕФЗЁЖГФЛЖЛХРГПЗОЛХСХРЛНСЁЖГРЗЦХСРЗХ |
| 8 | ХСХЙЛЕЗХТУЛТЗЕГБЪЛНХСЙЛЕЗХТСЖТЗЕГБЪЛ |
| 9 | ТУЗЙЖЗЪЗПЕЮШСЖЛХЯЛКФЗДВСТУЗЖЗОЛХЗЖГОЯРЗМЫЛМПГУЫУЦХ |

ЭБС ПГУТИ

**Задание 2. Дешифрировать сообщение (шифр атбаш)**

Номер варианта выбирается по предпоследней цифре зачетной книжки.

Таблица 2

| Вар | Шифрограмма |
|---|---|
| 0 | ЭНЪПРЮЪЫДСЯЗЦСЯБМНАНПРЮЪЫСЯЫНЯТЦТНРЮРХ |
| 1 | ЭФЯШЫРХЫЪНАМФЪЪНМГНЭРХСРУГ |
| 2 | ЧЛЮДТЛЫОРНМЦПРАЭУАБМНАЧСЯЗЦМЪУГСРПРЧШЪФУДФРЭ |
| 3 | ФМРТЪЖЯЪММЪЮЪЭДЫЛТЯМГПРОРЙСЪПОРТРФЯЪТДХ |
| 4 | СЪЭРЭНАФРХЦЬОЪМЛЧДЭДЦЬОДЭЯБМ |
| 5 | МЯФЙРЗЪМНАЮДМГСЛШСДТСЛШСДТУБЫАТ |
| 6 | СЯНЛЖЪТСРЬРЛТСДЙФРЬЫЯСЯТРОЪЮЪЫЯ |
| 7 | СЪМСЛШЫДЭЪЖЯМГФРУРФРУГЗЦФСЯЫЛОЯФЯ |
| 8 | КЦУРНРКНФЦХЭЧЬУАЫСЯЭЪЁЦПРЧЭРУАЪМРЮЙРЫЦМГНАЮЪЧСЦЙ |
| 9 | МЯФЬУЛЮРФРЧЯЫЛТЯУНАЗМРНРЭНЪТПЪОЪНМЯУНРРЮООЯШЯМГ |

**Задание 3. Дешифрировать сообщение (квадрат Полибия 6х6)**

Номер варианта выбирается по цифре $n_3$ зачетной книжки.

Таблица 3

| Вар. | Шифрограмма |
|---|---|
| 0 | 35 34 36 34 22 33 24 25 26 34 31 34 41 13 55 52 16 41 42 34 24 42 |
| 1 | 11 35 42 16 26 11 33 16 35 36 24 12 11 13 24 42 13 16 26 11 |
| 2 | 23 34 31 34 42 55 16 36 43 26 24 23 11 41 16 36 16 12 36 34 33 16 26 43 35 24 52 56 |
| 3 | 34 42 14 31 43 35 34 14 34 36 24 41 26 11 15 34 12 16 15 55 12 31 24 23 26 34 |
| 4 | 35 36 24 13 63 23 11 33 33 34 14 34 31 56 13 11 24 23 11 25 46 55 31 63 14 11 62 42 |
| 5 | 35 43 41 42 11 63 32 16 31 56 33 24 46 11 24 12 16 23 13 16 42 36 11 32 16 31 16 42 |
| 6 | 23 11 15 43 32 11 31 12 16 22 11 42 56 42 11 26 33 16 51 16 14 34 31 16 22 11 42 56 |
| 7 | 35 34 15 11 31 56 52 16 34 42 46 11 36 16 25 14 34 31 34 13 11 46 16 31 16 25 |
| 8 | 43 16 22 11 34 15 33 11 41 24 31 11 26 34 31 62 51 26 24 |
| 9 | 12 43 26 13 55 26 36 24 13 55 16 15 11 41 32 55 41 31 35 36 63 32 34 25 |

ЭБС ПГУТИ

**Задание 4. Дешифрировать сообщение (метод перестановок)**
Номер варианта выбирается по последней цифре зачетной книжки.
Ключи к данному заданию приведены в табл.4, а шифрограммы - в табл.5.

Таблица 4

Т

| Вар | Матрица | Ключ записи | Ключ считывания |
|---|---|---|---|
| 0 | 10x10 | 8 2 5 4 1 3 7 9 6 10 | 1 9 3 8 5 4 7 2 6 10 |
| 1 | 10x10 | 10 1 2 3 9 4 8 5 7 6 | 10 1 2 3 6 4 5 7 9 8 |
| 2 | 10x10 | 8 2 5 4 1 3 7 9 6 10 | 1 9 3 8 5 4 7 2 6 10 |
| 3 | 10x10 | 10 9 1 8 2 7 3 6 4 5 | 5 6 4 7 3 8 1 9 2 10 |
| 4 | 9x9 | 3 1 2 4 9 7 8 6 5 | 5 1 2 7 9 4 8 6 3 |
| 5 | 9x9 | 1 2 3 8 7 6 9 5 4 | 1 9 4 2 8 7 6 5 3 |
| 6 | 9x9 | 6 1 5 2 4 3 8 9 7 | 1 2 3 9 8 7 6 5 4 |
| 7 | 7x7 | 1 2 3 7 6 5 4 | 7 1 6 2 5 3 4 |
| 8 | 8x8 | 8 1 5 4 6 2 7 3 | 1 2 3 8 7 6 5 4 |
| 9 | 9x9 | 1 2 3 9 8 7 6 5 4 | 9 1 8 2 7 3 6 4 5 |

Таблица 5

| Вар | Шифрограмма |
|---|---|
| 0 | ППОЕСИЛУЧООЧИТСЗГОВ6ОЛНЛАНЧОО1ГАЯККЕОПО7ТЛЮИОНОЕО2ОИУОЛИУСД9ЕДЬААВТАГ4ЛАЛТТЗАСТ3ЧИСТТЕТДЛ8ВУПЕВЛОДЖ5 |
| 1 | НСОЕХ1ИНКИМИЯ_Е_НГВПИЯ_ОР1ЕОАО_ММТЕ9Т_РДРТЛУО8УБЕЛВИЫ_Д9_ТН_Ы_СКК8ДАЫСАААИР_7ХА_АЕТКЩА4М_АКЖЯ_ЯП5АКТД |
| 2 | ДВРВОУМКГ8ИОИБА9ЙЛГ3ОКВАВИНЖТ7ТРДИЧ1ЕЕЕ7ЛОСОТЬИЫВ6БКОКСТЯДО4СООНЕЯНЧН4ЬЕЕКЯЧЕАО3АТХЙРСВЙУ5ПГТУЮ2ЯОО8 |
| 3 | но_илиен_витряеяттинакинснлаьояоа_н_еасав_теиепфнн_рсиииинзсяд_неыж_окОэус_языил_овирчдв_астюув_м_яет |
| 4 | олоосахаопвГкЭеывор_ламтйылявтуньныу___т7__анхопдрРикктуи__февмдосмол_з_игуже__сь |
| 5 | Оо_1___моото5тптеоинс9нунчмдцн2пдпутдют6ю_юнтеао4аеа_чнвп7мимо__и_8игитунеа3оро_о |
| 6 | лн_в_Оотеиомоддвы___ызон_смл__ьчп_жниыутоайаонб_иткедироьда_д_летлутйючлччсбсоляи |
| 7 | _SI49EAAPE2R_SS_G53VCMLD8IE_UOA6S_IIA_1TSACTM7ATM |
| 8 | _TRTSS_AA_IUAAE_VDARRLTPEE3_IAESAD4ERNPOCI2TOAMP_V1_MTIOEI_I_U_R |
| 9 | eeu21_L__D_r2Kiagnbth35r_rlidn3ielrdel_4_eeeaee_4nbsoeiEt5rdism_ri6de_erL_s7e_dst |

ЭБГТУ ВГТ

**Задание 5. Дешифрировать сообщение (метод гаммирования)**

Номер варианта выбирается по предпоследней цифре зачетной книжки.

Таблица 6

| Вар | Гамма | Шифрограмма |
|---|---|---|
| 0 | 7 25 3 4 11 | ИЧСБЮЗЭЖПШИЧПБЮЗ |
| 1 | 1 5 32 7 | ЦЦжЙИЙеГВЛрВЛ |
| 2 | 6 12 22 5 3 | ДЬУЙЬДЭУЙРЧЯТЩЬ |
| 3 | 34 12 25 5 31 | бИЬОЯжЮЩЙЧиЗЩБ |
| 4 | 4 32 5 25 | ЗоБЛМхБЩУаФТМх |
| 5 | 14 2 17 25 34 | ДЙПОуЖЙНФзЛЕСХиО |
| 6 | 41 2 7 27 33 | еЗБЫфъДВЦппВ |
| 7 | 18 1 2 5 7 | ЯДБЛГЙРРЕЧНУВЖЙВД |
| 8 | 32 33 35 34 | оузсмълуомвзжйс |
| 9 | 3 2 5 35 | ММЧнПИНрППАжМТАзЙМЗ |

**Задание 6. Извлечь из контейнера текст, скрытый методом стеганографии**

Номер варианта выбирается по последней цифре зачетной книжки.

Таблица 7

| Вариант 0 | Вариант 1 | Вариант 2 | Вариант 3 |
|---|---|---|---|
| 11100011 | 01111001 | 00000101 | 10111111 |
| 01100111 | 10001001 | 11010001 | 00000001 |
| 10011110 | 01010110 | 10110010 | 11111000 |
| 11100101 | 00101101 | 00100011 | 11110011 |
| 01101101 | 11100110 | 01111100 | 01110100 |
| 01111100 | 00011111 | 10011101 | 01001010 |
| 10011010 | 11010101 | 11010011 | 11111111 |
| 10010011 | 00111001 | 00000011 | 10000110 |
| 11010101 | 10100111 | 10010101 | 00101101 |
| 00100111 | 10110011 | 00101011 | 10111101 |
| 11100101 | 00001011 | 11111111 | 11000111 |
| 11100000 | 00011000 | 01100100 | 11110110 |
| 10110011 | 00100010 | 00011110 | 11011001 |
| 01000010 | 01101000 | 10101100 | 11101101 |
| 00001000 | 11010010 | 00111010 | 10001011 |
| 01100010 | 11110000 | 11001100 | 10100010 |
| 01011001 | 10110001 | 00101011 | 01000101 |
| 00110001 | 00000001 | 10000011 | 11111011 |
| 01111001 | 11111001 | 10000101 | 00001001 |
| 11100011 | 01000110 | 00010101 | 11010100 |

СПбГУТИ

| | | | |
|---|---|---|---|
| 00001100 | 00011011 | 10111110 | 10110001 |
| 10010000 | 10111010 | 10101000 | 00010000 |
| 10100111 | 11111110 | 10111110 | 10011101 |
| 11101000 | 00111101 | 11100011 | 10001010 |

| **Вариант 4** | **Вариант 5** | **Вариант 6** | **Вариант 7** |
|---|---|---|---|
| 11100011 | 01111001 | 00000101 | 10111111 |
| 01100111 | 10001001 | 11010001 | 00000001 |
| 10011111 | 01010111 | 10110011 | 11111001 |
| 11100100 | 00101100 | 00100010 | 11110010 |
| 01101100 | 11100111 | 01111101 | 01110101 |
| 01111101 | 00011110 | 10011100 | 01001010 |
| 10011010 | 11010101 | 11010011 | 11111111 |
| 10010010 | 00111001 | 00000011 | 10000111 |
| 11010101 | 10100111 | 10010101 | 00101101 |
| 00100111 | 10110011 | 00101011 | 10111101 |
| 11100100 | 00001010 | 11111110 | 11000110 |
| 11100001 | 00011000 | 01100101 | 11110111 |
| 10110010 | 00100011 | 00011110 | 11011000 |
| 01000010 | 01101001 | 10101100 | 11101100 |
| 00001001 | 11010011 | 00111011 | 10001011 |
| 01100011 | 11110000 | 11001101 | 10100011 |
| 01011001 | 10110001 | 00101011 | 01000101 |
| 00110001 | 00000001 | 10000011 | 11111011 |
| 01111001 | 11111001 | 10000101 | 00001001 |
| 11100010 | 01000110 | 00010100 | 11010100 |
| 00001100 | 00011010 | 10111110 | 10110001 |
| 10010000 | 10111010 | 10101000 | 00010000 |
| 10100110 | 11111110 | 10111111 | 10011101 |
| 11101001 | 00111101 | 11100011 | 10001010 |

ЭБС ГГТУ им

| Вариант 8 | Вариант 9 | Вариант10 |
|---|---|---|
| 11100011 | 01111001 | 00000101 |
| 01100111 | 10001001 | 11010001 |
| 10011111 | 01010111 | 10110011 |
| 11100100 | 00101100 | 00100010 |
| 01101101 | 11100111 | 01111101 |
| 01111100 | 00011110 | 10011100 |
| 10011011 | 11010101 | 11010011 |
| 10010010 | 00111000 | 00000010 |
| 11010101 | 10100111 | 10010101 |
| 00100111 | 10110011 | 00101011 |
| 11100101 | 00001011 | 11111111 |
| 11100000 | 00011000 | 01100100 |
| 10110011 | 00100011 | 00011111 |
| 01000010 | 01101001 | 10101101 |
| 00001000 | 11010011 | 00111011 |
| 01100010 | 11110000 | 11001100 |
| 01011001 | 10110001 | 00101011 |
| 00110001 | 00000001 | 10000011 |
| 01111000 | 11111000 | 10000100 |
| 11100011 | 01000111 | 00010100 |
| 00001100 | 00011010 | 10111111 |
| 10010000 | 10111010 | 10101001 |
| 10100111 | 11111111 | 10111110 |
| 11101000 | 00111100 | 11100011 |

ЭБС ПГТИ

## Методические указания

### 1. Общие понятия и определения

Информация наряду с материей и энергией является первичным понятием нашего материального мира. Дать строгое исчерпывающее определение этому термину через другие, более простые понятия, сложно. Это понятие остается одним из самых дискуссионных в науке. Тем не менее, существует несколько определений понятия «информация». Приведем одно из них.

**Информация** — это совокупность каких-либо сведений, данных, передаваемых устно (в форме речи), письменно (в виде текста, таблиц, рисунков, чертежей, схем, условных обозначений) либо другим способом (например, с помощью звуковых или световых сигналов, электрических и нервных импульсов, запахов, вкусовых ощущений, перепадов давления или температуры и т. д.).

Теоретические и практические вопросы, относящиеся к информации, изучает информатика.

**Информатика** — наука, изучающая структуру и свойства информации, а также вопросы, связанные с ее сбором, хранением, поиском, передачей, преобразованием, распространением и использованием в различных сферах человеческой деятельности.

Еще одно определение информатики.

Информатика — это область человеческой деятельности, связанная с процессами преобразования информации с помощью компьютеров.

Современная информатика коренным образом изменяет не только сферу материального производства, но и сферу духовной жизни.

Эффективным инструментом обработки большого объема информации является электронная вычислительная машина (**ЭВМ**).

Одним из основных факторов ускорения научно-технического прогресса является широкое использование **новых информационных технологий**, под которыми понимается **совокупность методов и средств** сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления на базе вычислительной и коммуникационной техники и широкого применения математических методов.

Различают две формы представления информации — **непрерывную (аналоговую)** и **прерывистую (цифровую, дискретную).** Непрерывная форма характеризует процесс, который не имеет перерывов и теоретически может изменяться в любой момент времени и на любую величину (например, речь человека, музыкальное произведение). Цифровой сигнал может изменяться лишь в определенные моменты времени и принимать лишь заранее обусловленные значения (например, только значения напряжений 0 и 3,5 В). Моменты возможного изменения уровня цифрового сигнала задает тактовый генератор конкретного цифрового устройства.

ЭБС ПГУТИ

Для преобразования аналогового сигнала в цифровой сигнал требуется провести дискретизацию непрерывного сигнала во времени, квантование по уровню, а затем кодирование отобранных значений.

**Дискретизация** — замена непрерывного (аналогового) сигнала последовательностью отдельных во времени отсчетов этого сигнала. Наиболее распространена равномерная дискретизация, в основе которой лежит **теорема Котельникова**.

На рисунке схематично показан процесс преобразования аналогового сигнала в цифровой сигнал. Цифровой сигнал в данном случае может принимать лишь пять различных уровней. Естественно, что качество такого преобразования невысокое. Из рисунка видно, что изменение цифрового сигнала возможно лишь в некоторые моменты времени (в данном случае этих моментов одиннадцать).

После такого преобразования непрерывный сигнал представляют

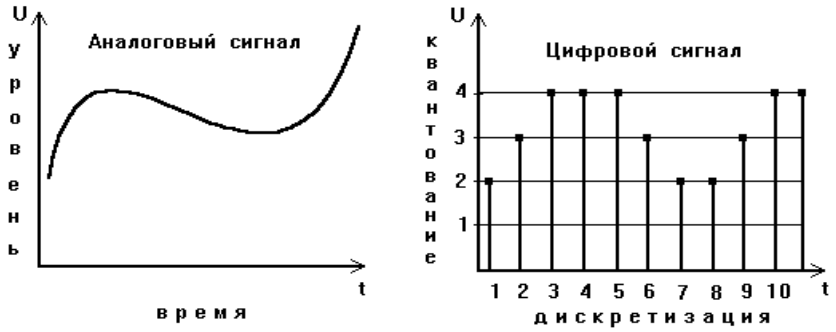



Рис. 1.1

последовательностью чисел. Показанный на рисунке непрерывный сигнал заменяется числами 2-3-4-4-4-3-2-2-3-4-4. Десятичная система счисления в рассматриваемом примере использована лишь для большей наглядности. Фактически аналоговый сигнал преобразуют в последовательность единиц и нулей. Результаты данного преобразования можно представить таблицей:

Табл. 1.1.

| Время | Десятичные числа | Двоичные числа |
|---|---|---|
| $t_1$ | 2 | 0010 |
| $t_2$ | 3 | 0011 |
| $t_3$ | 4 | 0100 |
| $t_4$ | 4 | 0100 |
| $t_5$ | 4 | 0100 |
| $t_6$ | 3 | 0011 |
| $t_7$ | 2 | 0010 |
| $t_8$ | 2 | 0010 |
| $t_9$ | 3 | 0011 |
| $t_{10}$ | 4 | 0100 |
| $t_{11}$ | 4 | 0100 |

В данном случае цифровые сигналы представлены четырьмя разрядами двоичных чисел. Очевидно, что, чем больше разрядов у двоичных чисел (а значит, тем больше число уровней квантования) и чем чаще во времени осуществляются отсчеты (выборки), тем точнее будет преобразован непрерывный сигнал в цифровой.

Первое представление об аналоговом и цифровом способах хранения и распространения информации можно получить, рассматривая два способа записи звуковых сигналов: аналоговую и цифровую аудиозаписи.

При аналоговой аудиозаписи непрерывный электрический сигнал, формируемый источником звука на выходе микрофона, с помощью магнитной головки наносится на движущуюся магнитную ленту. Недостатком аналогового способа обработки информации является то, что копия бывает всегда хуже оригинала.

При цифровой аудиозаписи используется **процесс выборки,** заключающийся в периодическом измерении уровня (громкости) аналогового звукового сигнала (например, поступающего с выхода микрофона) и превращении полученного значения в последовательность двоичных чисел. Для преобразования аналогового сигнала в цифровой используется специальный конвертор, называемый **аналогово-цифровой преобразователь (АЦП).** Сигнал на выходе АЦП представляет собой последовательность двоичных чисел, которая может быть записана на лазерный диск или обработана компьютером. Обратная конверсия цифрового сигнала в непрерывный сигнал осуществляется с помощью цифроаналогового преобразователя (ЦАП).

Качество аналогово-цифрового преобразования характеризует параметр, называемый разрешением. **Разрешение** — это количество уровней квантования, используемых для замены непрерывного аналогового сигнала цифровым сигналом. Восьмиразрядная выборка позволяет получить только 256 различных уровней квантования цифрового сигнала, а шестнадцатиразрядная выборка — 65 536 уровней.

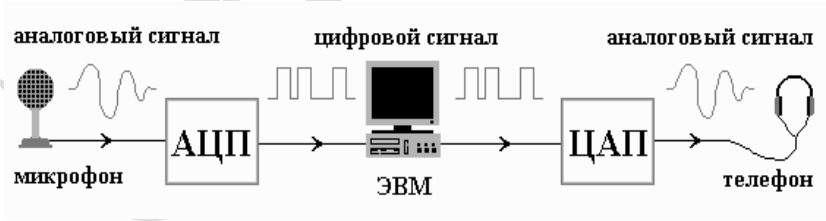



Рис.1.2

Еще один показатель качества трансформации непрерывного сигнала в цифровой сигнал — это частота дискретизации — количество преобразований аналог-цифра (выборок), производимое устройством в одну секунду. Этот показатель измеряют килогерцами (килогерц — тысяча выборок в секунду). Типичное значение частоты дискретизации современных лазерных (оптических) аудиодисков — 44,1 кГц.

Имеется тенденция перехода к единому цифровому представлению всех видов информации. Глобальная сеть Интернет претендует на то, чтобы объединить все средства вещания и коммуникации, компьютерные, телефонные, радио- и видеосети, связав их в единое «киберпространство».

С позиции каждого отдельного человека количество информации, содержащееся в каком-либо сообщении, — субъективная величина.

Объективная количественная мера информации может быть введена на основе вероятностной трактовки информационного обмена.

Этот способ измерения количества информации впервые предложил в 1948 г. **К. Шеннон**. В соответствии с идеями К. Шеннона, информация — это сведения, уменьшающие неопределенность (энтропию), существовавшую до их получения.

Наименьшей единицей информации является **бит** (от англ. **bi**nary digi**t** — двоичный разряд). Сообщение о том, что произошло одно из двух возможных равновероятных событий, дает получателю один бит информации.

Один бит информации получает человек, когда он узнает, опаздывает с прибытием нужный ему поезд или нет, был ночью мороз или нет, присутствует на лекции студент Иванов или нет и т. д.

Более крупная единица информации — **байт** — равна 8 бит. Проверка присутствия или отсутствия на лекции 24 студентов дает лектору три байта информации. Еще более крупная единица информации — 1 Кбайт — равна 1024 байтам. Далее — 1 Мбайт равен 1024 Кбайтам, 1 Гбайт равен 1024 Мбайтам, 1 Тбайт равен 1024 Гбайтам, а 1 Пбайт равен 1024 Тбайт.

Перечисленные единицы измерения информации произносятся так:

Кбайт — килобайт, Мбайт — мегабайт, Гбайт — гигабайт, Тбайт — терабайт, Пбайт — петабайт.

ЭБ ПГУТИ

## 2. Системы счисления

Все фантастические возможности вычислительной техники (ВТ) реализуются путем создания разнообразных комбинаций сигналов высокого и низкого уровней, которые условились называть «единицами» и «нулями». Под **системой счисления** (СС) понимается способ представления любого числа с помощью алфавита символов, называемых цифрами.


СС называется **позиционной**, если одна и та же цифра имеет различное значение, которое определяется ее местом в числе.

Десятичная СС является позиционной. На рисунке слева значение цифры 9 изменяется в зависимости от ее положения в числе. Первая слева девятка делает вклад в общее значение десятичного числа 900 единиц, вторая — 90, а третья — 9 единиц.

Римская СС является **непозиционной**. Значение цифры X в числе XXI остается неизменным при вариации ее положения в числе.

Количество различных цифр, употребляемых в позиционной СС, называется **основанием** СС. В десятичной СС используется десять цифр: 0, 1, 2, ..., 9; в двоичной СС — две цифры: 0 и 1; в восьмеричной СС — восемь цифр: 0, 1, 2, ..., 7. В СС с основанием $Q$ используются цифры от 0 до $Q - 1$.

В общем случае в позиционной СС с основанием $Q$ любое число $x$ может быть представлено в виде **полинома**:

$$x = a_n \cdot Q^n + a_{n-1} \cdot Q^{n-1} + \ldots + a_1 \cdot Q^1 + a_0 \cdot Q^0 + a_{-1} \cdot Q^{-1} + a_{-2} \cdot Q^{-2} + \ldots a_{-m} \cdot Q^{-m}$$

целая часть — дробная часть

В этом полиноме в качестве коэффициентов $a_i$ могут стоять любые цифры, используемые в данной СС.

Принято представлять числа в виде последовательности входящих в полином соответствующих цифр (коэффициентов):

$$x = a_n\, a_{n-1} \ldots a_1\, a_0\, ,\, a_{-1}\, a_{-2} \ldots a_{-m}$$

Запятая отделяет целую часть числа от дробной части. В ВТ чаще всего для отделения целой части числа от дробной части используют **точку**. Позиции цифр, отсчитываемые от точки, называют **разрядами**. В позиционной СС вес каждого разряда отличается от веса (вклада) соседнего разряда в число раз, равное основанию СС. В десятичной СС цифры 1-го справа разряда — единицы, 2-го — десятки, 3-го — сотни и т. д.

ЭБС ПГУТИ

В ВТ применяют позиционные СС с недесятичным основанием: двоичную, восьмеричную и шестнадцатеричную системы. Для обозначения используемой СС **числа заключают в скобки и индексом указывают основание СС:**

$(15)_{10}$; $(1011)_2$; $(735)_8$; $(1EA9F)_{16}$.

Чаще всего скобки опускают и оставляют только индекс:

$15_{10}$; $1011_2$; $735_8$; $1EA9F_{16}$.

Есть еще один способ обозначения СС: при помощи латинских букв, добавляемых после числа. Например,

15D; 1011B; 735Q; 1EA9FH.

Установлено, что, чем больше основание СС, тем компактнее запись числа. Так двоичное изображение числа требует примерно в 3,3 раза большего количества цифр, чем его десятичное представление.

Несмотря на то, что десятичная СС имеет широкое распространение, цифровые ЭВМ строятся на двоичных (цифровых) элементах, так как реализовать элементы с десятью четко различимыми состояниями сложно. В другой системе счисления могут работать приборы декатрон и трохотрон. Декатрон — газоразрядная счетная лампа — многоэлектродный газоразрядный прибор тлеющего разряда для индикации числа импульсов в десятичной СС.

Указанные устройства не нашли применения для построения средств ВТ. Историческое развитие вычислительной техники сложилось таким образом, что цифровые ЭВМ строятся на базе двоичных цифровых устройств (триггеров, регистров, счетчиков, логических элементов и т. п.).

Шестнадцатеричная и восьмеричная СС используются при составлении программ на языке машинных кодов для более короткой и удобной записи двоичных кодов — команд, данных, адресов и операндов. Перевод из двоичной СС в шестнадцатеричную и восьмеричную СС (и обратно) осуществляется достаточно просто.

Задача перевода из одной системы счисления в другую часто встречается при программировании и особенно часто при программировании на языке Ассемблера. Например, при определении адреса ячейки памяти, для получения двоичного или шестнадцатеричного эквивалента десятичного числа. Отдельные стандартные процедуры языков программирования Паскаль, Бейсик, HTML и Си требуют задания параметров в шестнадцатеричной системе счисления. Для непосредственного редактирования данных, записанных на жесткий диск, также необходимо умение работать с шестнадцатеричными числами. Отыскать неисправность в ЭВМ практически невозможно без представлений о двоичной системе счисления. Без знания двоичной СС невозможно понять принципы архивации, криптографии и стеганографии. Без знания двоичной СС и булевой алгебры невозможно представить, как происходит слияние объектов в векторных графических редакторах.

В табл. 2.1 приведены числа, представленные в различных СС.

ЭБС ПГУТИ

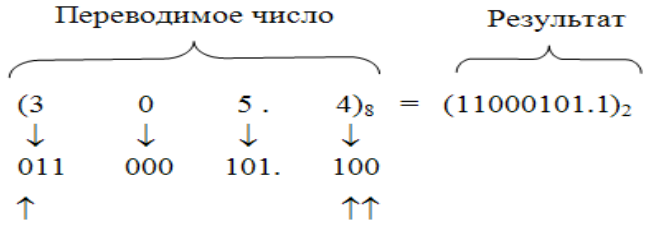
Таблица 2.1

| Системы счисления | | | |
|---|---|---|---|
| **Десятичная** | **Двоичная** | **Восьмеричная** | **Шестнадцатер.** |
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 2 | 10 | 2 | 2 |
| 3 | 11 | 3 | 3 |
| 4 | 100 | 4 | 4 |
| 5 | 101 | 5 | 5 |
| 6 | 110 | 6 | 6 |
| 7 | 111 | 7 | 7 |
| 8 | 1000 | 10 | 8 |
| 9 | 1001 | 11 | 9 |
| 10 | 1010 | 12 | A |
| 11 | 1011 | 13 | B |
| 12 | 1100 | 14 | C |
| 13 | 1101 | 15 | D |
| 14 | 1110 | 16 | E |
| 15 | 1111 | 17 | F |
| 16 | 10000 | 20 | 10 |
| 17 | 10001 | 21 | 11 |

Рассмотрим **правило** перехода из восьмеричной СС в двоичную СС.

Для перевода **восьмеричного** числа в **двоичную** СС достаточно заменить каждую цифру восьмеричного числа соответствующим трехразрядным двоичным числом. Затем необходимо удалить крайние нули слева, а при наличии дробной части — и крайние нули справа.

**Пример 1**. Перевести число 305.4Q из восьмеричной СС в двоичную СС.
*Решение.*



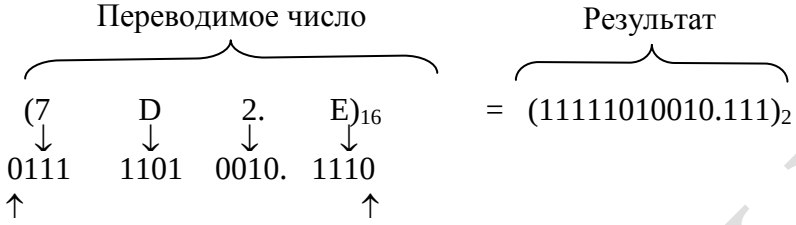

Отмеченные символами «↑» нули следует отбросить. Заметим, что двоичные числа взяты из табл. 1.

Еще одно правило перевода чисел:

Для перехода от **шестнадцатеричной** СС к **двоичной** СС каждая цифра шестнадцатеричного числа заменяется соответствующим четырехразрядным двоичным числом. У двоичного числа удаляются лидирующие нули (крайние слева), а если имеется дробная часть, то и крайние правые нули.

**Пример 2**. Перевести число 7D2.EH из шестнадцатеричной СС в двоичную СС.

*Решение.*



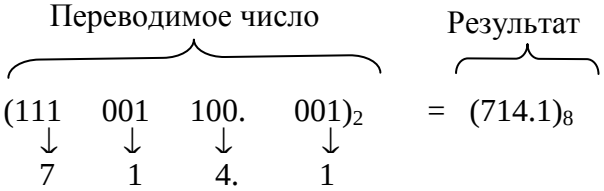

Отмеченные крайние нули следует отбросить.

Рассмотрим еще одно правило:

Для перехода от **двоичной** СС к **восьмеричной** (или ***шестнадцатеричной)*** СС поступают следующим образом: двигаясь от точки сначала влево, а затем вправо, разбивают двоичное число на группы по три *(четыре)* разряда, дополняя при необходимости нулями крайнюю правую группу. Затем каждую группу из трех *(четырех)* двоичных разрядов заменяют соответствующей восьмеричной *(шестнадцатеричной)* цифрой.

**Пример 3.** Перевести число 111001100.001B из двоичной СС в восьмеричную СС.

*Решение.*




ЭБ ПГУТИ

**Пример 4.** Перевести число 10111110001.001B из двоичной СС в шестнадцатеричную СС.

*Решение.*

Переводимое число — Результат

$(0101\ 1111\ 0001.\ 0010)_2 = (5F1.2)_{16}$

5 F 1. 2

Для перевода **двоичного** числа в **десятичную** СС следует представить число в виде полинома, подставить в него известные коэффициенты и вычислить сумму.

**Пример 5.** Перевести число 11011.11B из двоичной СС в десятичную СС.

*Решение.*

$$(11011.11)_2 = 1\cdot2^4 + 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 + 1\cdot2^{-1} + 1\cdot2^{-2} =$$
$$= 16 + 8 + 0 + 2 + 1 + 0.5 + 0.25 = (27.75)_{10}.$$

**Пример 6.** Перевести шестнадцатеричное число 2E5.AH в десятичную СС.

*Решение.*

$$(2E5.A)_{16} = 2\cdot16^2 + 14\cdot16^1 + 5\cdot16^0 + 10\cdot16^{-1} = (741.625)_{10}.$$

Перевод целых чисел из **десятичной** СС в **двоичную**, **восьмеричную** или **шестнадцатеричную** СС удобно делать с помощью следующего правила:

Для перевода **целого** числа из *S*-системы счисления в *W*-систему счисления нужно последовательно делить это число, а затем получаемые частные на основание *W* новой СС до тех пор, пока частное не станет меньше *W*.

**Пример 7.** Перевести целое десятичное число 37D в двоичную СС:

*Решение.*

```
  37 | 2
  36   18 | 2
   1   18   9 | 2
       0    8   4 | 2
            1   4   2 | 2
                0   2   1   ← СЗР
                    0
МЗР →
```

Результат перевода: $(37)_{10} = (100101)_2$.

При переводе наиболее частой ошибкой является неверная запись результата. Запись двоичного числа следует начинать со старшего значащего разряда (СЗР), а заканчивать записью младшего значащего разряда (МЗР). Следует помнить, что при делении первым получается значение МЗР.

> Для перевода **правильной дроби** из *S*-системы счисления в СС с основанием W нужно умножить исходную дробь и дробные части получающихся произведений на основание W, представленное в старой *S*-системе. Целые части получающихся произведений дают последовательность цифр, которая является представлением дроби в W-системе счисления.

Напомним, что **правильной** называется дробь, числитель которой меньше знаменателя.

**Пример 8.** Перевести правильную десятичную дробь 0.1875D в двоичную СС.

*Решение.*

```
      0.1875
      x    2
0 ←  0.3750
      x    2
0 ←  0.7500
      x    2
1 ←  1.5000
      x    2
1 ←  1.0000
```

Запишем результат перевода: 0.1875D = 0.0011B.

Обычно перевод дробей из одной СС в другую производят приближенно. При переводе неправильной дроби переводят отдельно целую и дробную части, руководствуясь соответствующими правилами.

**Пример 9.** Перевести десятичное число 9.625D в двоичную СС.

*Решение.*

Вначале переведем целую часть десятичного числа в двоичную СС: 9D = 1001B.

Затем переведем правильную дробь: 0.625D = 0.101B.

Окончательный ответ: 9.625D = 1001.101B.

ЭБС ПГУТИ

## 3. Арифметические основы работы ЭВМ

Правила выполнения арифметических действий над двоичными числами задаются таблицами сложения, вычитания и умножения.

Таблица 3.1

| Сложение | Вычитание | Умножение |
|---|---|---|
| 0 + 0 = 0 | 0 – 0 = 0 | 0 □ 0 = 0 |
| 0 + 1 = 1 | 1 – 0 = 1 | 0 □ 1 = 0 |
| 1 + 0 = 1 | 1 – 1 = 0 | 1 □ 0 = 0 |
| 1 + 1 = 10 | 10 – 1 = 1 | 1 □ 1 = 1 |

Правила арифметики во всех позиционных СС аналогичны. В двоичной СС арифметическое сложение происходит по правилу сложения по модулю два с учетом переноса единицы в старший разряд (см. табл. 3.1).

**Пример 1.** Выполнить операцию арифметического сложения в двоичной системе счисления.

*Решение.*

$$\begin{array}{r} \cdot \\ 13 \\ +\ 7 \\ \hline 20 \end{array}_{10} \rightarrow \begin{array}{r} \cdot\ \cdot\ \cdot\ \cdot \\ 01101 \\ +\ 00111 \\ \hline 10100 \end{array}_{2}$$

Точками показаны переносы.

В устройствах, реализующих операцию арифметического сложения двоичных чисел, операнды представляют числами определенной разрядности (одинаковой для обоих операндов). При этом неиспользуемые старшие разряды заполняются нулями. Также заполняются нулями младшие разряды дробной части вещественного числа (справа от точки).

Следует заметить, что в реальных ЭВМ чаще всего используются 32-, 64-, 128-разрядные сетки (машинные слова). Однако для учебных целей при рассмотрении правил выполнения арифметических операций не будем обращать внимание на разрядность операндов (т. е. будем использовать разрядность, отличающуюся от разрядности реальных ЭВМ).

**Пример 2**. Выполнить операцию арифметического сложения двух вещественных чисел в двоичной системе счисления.

*Решение.*

$$\begin{array}{r} \cdot \\ 55{,}25 \\ +\ 19{,}5 \\ \hline 74{,}75 \end{array}_{10} \rightarrow \begin{array}{r} \cdot\ \cdot\ \cdot\ \cdot \\ 0110111.01 \\ +\ 0010011.10 \\ \hline 1001010.11 \end{array}_{2}$$

Результаты сложения двух чисел показаны на рисунке слева. При сложении вещественных чисел в общем случае перенос осуществляется и из дробной части числа в целую часть.

Рассмотрим правило умножения многоразрядных двоичных чисел.

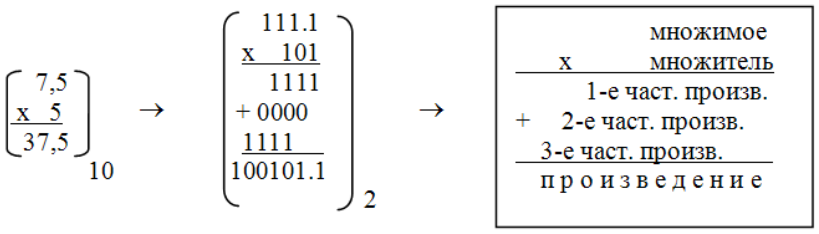
Умножение двоичных многоразрядных чисел производится путем образования частичных произведений и последующего их суммирования. Каждое частичное произведение равно нулю, если в соответствующем разряде множителя стоит 0, или равно множимому, сдвинутому на соответствующее число разрядов влево, если в разряде множителя стоит 1.

ЭБ ПГУТИ

Таким образом, **операция умножения** многоразрядных двоичных чисел внутри ЭВМ **сводится к операции сдвига и сложения**. Положение точки, отделяющей целую часть от дробной части, определяется так же, как и при умножении десятичных чисел.

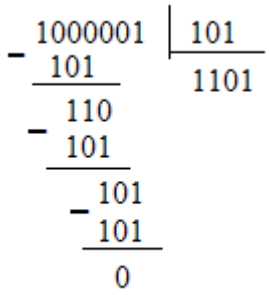
**Пример 3.** Перемножить в двоичной СС числа 7,5D и 5D.

*Решение.*




В рассмотренном примере второй разряд множителя равен нулю, поэтому второе частичное произведение также равно нулю.

**Пример 4.** Выполнить деление в двоичной СС десятичного числа 65D на число 5D.




Полученный результат 1101B = 13D свидетельствует о верности выполненной операции деления.

В ВТ, с целью упрощения реализации арифметических операций, применяют специальные коды. За счет этого облегчается определение знака результата операции, а операция вычитания чисел сводится к арифметическому сложению. В результате упрощаются устройства, выполняющие арифметические операции.

В ВТ применяют прямой, обратный и дополнительный коды.

**Прямой** двоичный код $P_{пр}(x)$ — это такое представление двоичного числа $x$, при котором знак «+» кодируется нулем в старшем разряде числа, а знак «–» — единицей. При этом старший разряд называется **знаковым.**

Например, числа +5D и –5D, представленные в прямом четырехразрядном коде, выглядят так: +5D = 0'101B; –5D = 1'101B. Здесь апострофом условно (для удобства определения знака) отделены знаковые разряды.

**Обратный код** $P_{обр}(x)$ получается из прямого кода по следующему правилу:

$$P_{обр}(x) = \begin{cases} 0'\,P_{пр}(x), & \text{при } x \geq 0 \\ \overline{1'\,P_{пр}(x)}, & \text{при } x \leq 0. \end{cases}$$

Из приведенного выражения видно, что обратный код для положительных чисел совпадает с прямым кодом. Чтобы представить отрицательное двоичное число в обратном коде, нужно поставить в знаковом разряде 1, во всех значащих разрядах заменить 1 на 0, а 0 на 1. Такая операция называется инверсией и обозначается горизонтальной чертой над инвертируемым выражением.

**Пример 5**. Получить обратный код для числа $x$ = –11D.

*Решение.*

$$P_{пр}(x) = (1'1011)_2$$
$$P_{обр}(x) = (1'0100)_2.$$

Считается, что здесь числа представлены пятью разрядами. Из рассмотренного примера видно, что обратный код для положительных чисел совпадает с прямым, а для отрицательных чисел получается инверсией (переворотом) всех разрядов, кроме знакового разряда.

**Дополнительный код** $P_{доп}(x)$ образуется следующим образом:

$$P_{доп}(x) = \begin{cases} 0'\, P_{пр}(x), & \text{при } x \geq 0 \\ \overline{1'\, P_{пр}(x)} + 1, & \text{при } x < 0. \end{cases}$$

Из выражения видно, что дополнительный код положительного числа совпадает с прямым кодом, а для отрицательного числа получается инверсией всех значащих разрядов и добавлением единицы к младшему разряду результата.

Дополнительный код отрицательного числа может быть получен из обратного кода путем прибавления 1 к младшему разряду обратного кода (естественно, с учетом переносов между разрядами).

**Пример 6.** Получить дополнительный код для числа $x$ = –13D.

*Решение.*

$P_{пр}(x) = (1'1101)_2$ прямой код

$P_{обр}(x) = (1'0010)_2$ обратный код

$P_{доп}(x) = (1'0011)_2$ дополнительный код.

В табл. 2 представлены прямые, обратные и дополнительные коды чисел в диапазоне от –7D до +7D.

ЭБС ПГУТИ

Таблица 3.2

| **Десятичное число *x*** | $P_{пр}(x)$ | $P_{обр}(x)$ | $P_{доп}(x)$ |
|---|---|---|---|
| 0 | 0'000 | 0'000 | 0'000 |
| 1 | 0'001 | 0'001 | 0'001 |
| 2 | 0'010 | 0'010 | 0'010 |
| 3 | 0'011 | 0'011 | 0'011 |
| 4 | 0'100 | 0'100 | 0'100 |
| 5 | 0'101 | 0'101 | 0'101 |
| 6 | 0'110 | 0'110 | 0'110 |
| 7 | 0'111 | 0'111 | 0'111 |
| -0 | 1'000 | 1'111 | — |
| -1 | 1'001 | 1'110 | 1'111 |
| -2 | 1'010 | 1'101 | 1'110 |
| -3 | 1'011 | 1'100 | 1'101 |
| -4 | 1'100 | 1'011 | 1'100 |
| -5 | 1'101 | 1'010 | 1'011 |
| -6 | 1'110 | 1'001 | 1'010 |
| -7 | 1'111 | 1'000 | 1'001 |

Рассмотрим правило сложения двоичных чисел в дополнительном коде.

При алгебраическом сложении двоичных чисел положительные слагаемые представляют в прямом коде, а отрицательные числа (слагаемые) — в дополнительном коде и производят арифметическое суммирование этих кодов, включая разряды знаков, которые при этом рассматривают как старшие разряды. При возникновении переноса из разряда знака единицу переноса отбрасывают. В результате получают алгебраическую сумму в прямом коде, если эта сумма положительная, и в дополнительном коде, — если сумма отрицательная.

Напомним, что алгебраическое сложение — это сложение, в котором могут участвовать как положительные, так и отрицательные числа.

**Пример 7**. Выполнить алгебраическое сложение с использованием дополнительного кода для чисел $x_1$ = 7D и $x_2$ = –3D.

*Решение.*

Необходимо найти сумму: $y = x_1 + x_2$.

Учитывая, что $x_1 > 0$, это число нужно представить в прямом коде, а так как $x_2 < 0$, то число $x_2$ нужно перевести в дополнительный код.

$P(y) = P_{пр}(x_1) + P_{доп}(x_2)$.

$P_{пр}(x_1)$ = 0'111B

$P_{пр}(x_2)$ = 1'011B

$P_{обр}(x_2)$ = 1'100B

$P_{доп}(x_2)$ = 1'101B.

$$P(y) = \left[\begin{array}{r} \cdots \\ 0'111 \\ +\ 1'101 \\ \hline 0'100 \end{array}\right]_2$$

Так как результат положителен (в знаковом разряде $P(y)$ — 0), значит, он представлен в прямом коде $P_{пр}(y)$ =0'100B. После перевода двоичного числа в десятичную СС получим ответ: $y$ = +4D.

**Пример 8**.

Выполнить алгебраическое сложение чисел $x_1$ = 8D и $x_2$ = –13D с использованием дополнительного кода.

*Решение*

Необходимо найти сумму: $y = x_1 + x_2$.

Число $x_1$ нужно представить в прямом коде, а $x_2$ — в дополнительном коде.

$P(y) = P_{пр}(x_1) + P_{доп}(x_2)$.

$P_{пр}(x_1)$ = 0'1000B

$P_{пр}(x_2)$ = 1'1101B

$P_{обр}(x_2)$ = 1'0010B

$P_{доп}(x_2)$ = 1'0011B.

$$P(y) = \begin{pmatrix} 0'1000 \\ +\ 1'0011 \\ \hline 1'1011 \end{pmatrix}_2$$

В знаковом разряде стоит единица, и, значит, результат получен в дополнительном коде. Для перехода от дополнительного кода

$$P_{доп}(y) = 1'1011B$$

к прямому коду $P_{пр}(y)$ необходимо выполнить следующие преобразования:

$$P_{обр}(y) = P_{доп}(y) - 1 = 1'1011B - 1 = 1'1010B,$$

$$\overline{\quad} \qquad \overline{\quad}$$

$$P_{пр}(y) = P_{обр}(y) = 1'1010B = 1'0101B.$$

Переходя от двоичной СС к десятичной СС, получим ответ: $y$ = –5D.

**Пример 9**. Выполнить алгебраическое сложение с использованием дополнительного кода для чисел $x_1$ = – 6D и $x_2$ = –17D.

*Решение*

Необходимо найти сумму: $y = x_1 + x_2$.

Числа $x_1$ и $x_2$ нужно представить в дополнительном коде.

$P(y) = P_{доп}(x_1) + P_{доп}(x_2)$.

$P_{пр}(x_1)$ = 1'00110B

$P_{обр}(x_1)$ = 1'11001B

$P_{доп}(x_1)$ = 1'11010B

$P_{пр}(x_2)$ = 1'10001B

$P_{обр}(x_2)$ = 1'01110B

$P_{доп}(x_2)$ = 1'01111B.

$$P(y) = \begin{pmatrix} 1'11010 \\ +\ 1'01111 \\ \hline 1'01001 \end{pmatrix}_2$$

В знаковом разряде стоит единица, и, значит, результат получен в дополнительном коде. Для перехода от дополнительного кода Рдоп(у) = 1'01001B к прямому коду Рпр(у) необходимо выполнить следующие преобразования:

Робр(у) = Рдоп(у) – 1 = 1'01001B – 1 = 1'01000B,

Рпр(y) = Робр(y) = 1'01000B = 1'10111B.

Переходя от двоичной СС к десятичной СС, получим ответ: y = –23D.

## 4. Форматы представления чисел в ЭВМ

При проведении математических расчетов числа в ЭВМ могут быть представлены с помощью естественной и нормальной форм записи.

Примером записи в естественной форме может служить вещественное число 173,856. Для записи такого числа машинное слово (операнд) делится на два фиксированных поля (на две части). Первое поле отводится для записи целой части числа, второе — для записи дробной части числа. Старший разряд предназначается для указания знака числа. Числами нумеруются разряды машинного слова (справа – налево).

В вычислительной технике принято отделять целую часть числа от дробной части точкой. Так как положение точки между целой и дробной частью числа четко определено, то такое представление чисел называют представлением с фиксированной точкой.

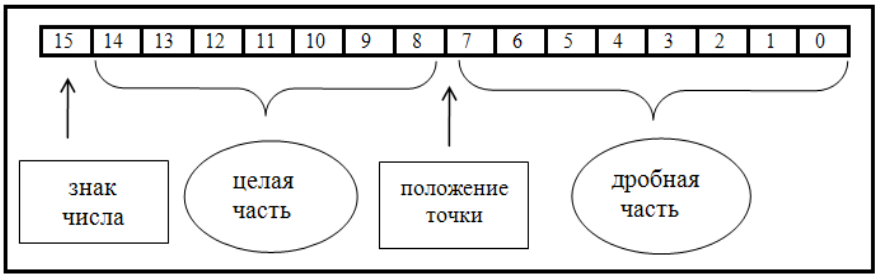



Рис. 4.1.

Недостатком формы с фиксированной точкой является малый диапазон представления (изменения) чисел. В современных ЭВМ в этой форме записывают только целые числа. При записи целых чисел отпадает необходимость отводить поле для записи дробной части числа (см. следующий рисунок).

Разряд кода числа, в котором размещается знак, называется знаковым разрядом. Знаковый разряд размещается в старшем разряде машинного слова. Знак положительного числа кодируется двоичной цифрой 0, а знак отрицательного числа – цифрой 1.

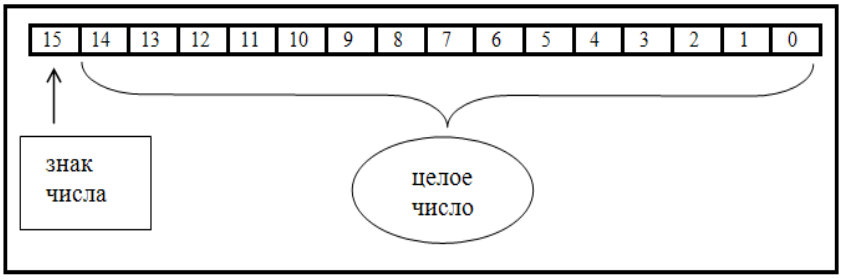



Рис. 4.2.

Нормальная форма записи числа n имеет следующий вид:

$$n = m \cdot d^{\,p},$$

где $m$ — мантисса числа; $p$ — порядок; $d$ — основание системы счисления.

Приведем пример записи числа в нормальной форме:

$$n = 1.541 \cdot 10^{2}.$$

Порядок $p$ указывает местоположение в числе точки, отделяющей целую часть числа от дробной части. В зависимости от значения порядка p точка перемещается (плавает) по мантиссе. Такая форма представления чисел называется формой с плавающей точкой.

Следующий рисунок иллюстрирует форму числа с плавающей точкой на примере 32-х разрядного машинного слова.

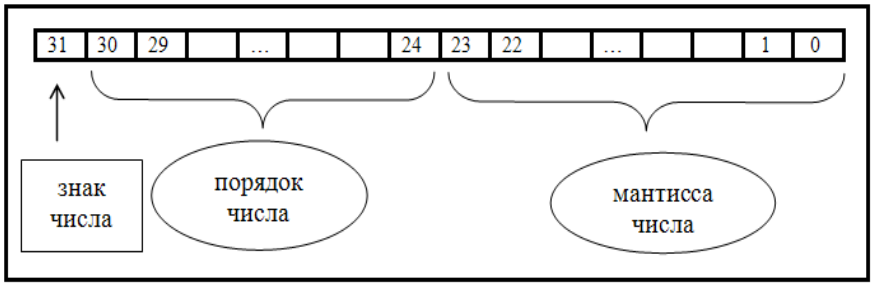



Рис. 4.3.

Например, пусть $m$ = 0.3, $d$ = 10, а порядок p будем брать разным:

$0.3 \cdot 10^{-1} = 0.03;\quad 0.3 \cdot 10^{-2} = 0.003;\quad 0.3 \cdot 10^{2} = 30;\quad 0.3 \cdot 10^{3} = 300.$

Из приведенного примера видно, что благодаря изменению порядка точка перемещается (плавает) по мантиссе. При этом если порядок отрицательный, точка смещается по мантиссе влево, а если положительный, то -вправо.

В нормальной форме машинное слово делится на два поля. В одном поле записывается мантисса числа, а во втором — указывается порядок числа.

Диапазон представления чисел с плавающей точкой значительно больше диапазона представления чисел с фиксированной точкой. Однако быстродействие ЭВМ при обработке чисел с плавающей точкой гораздо ниже, чем при обработке чисел с фиксированной точкой. Этим объясняется одновременное существование двух форм чисел.

Последовательность нескольких битов или байтов называют полем данных [7].

Биты в поле нумеруются справа налево, начиная с нулевого разряда. В ЭВМ могут обрабатываться поля постоянной и переменной длины.

Перечислим поля постоянной длины:

полуслово — 1 байт;

слово — 2 байта;

двойное слово — 4 байта;

расширенное слово — 8 байт.

ЭБС ПГУТИ

Числа с фиксированной точкой чаще всего имеют формат слова и полуслова, числа с плавающей точкой — формат двойного и расширенного слова.

Поля переменной длины могут иметь любой размер от 0 до 256 байт. При этом поле должно состоять из целого числа байтов.

**Пример 1.** Записать число -19310 = -110000012 в формате слова со знаком и фиксированной точкой.

*Решение.*

| | Знак числа | Абсолютная величина числа | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N разряда | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Число | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |

Для чисел с плавающей точкой под знак и порядок отводится восемь старших бит числа. Для представления как положительного так и отрицательного порядков применяют смещенный порядок. При этом машинный порядок Мр представляют со смещением на 64 разряда по отношению к фактическому порядку: Мр = Р + 64. Таким образом при машинном порядке равном нулю (0000000 В) фактический порядок равен -64, а при максимальном машинном порядке 1111111 В = 127D, фактический порядок равен +63D.

**Пример 2.** Записать число -19310 = -110000012 = -0.11000001*28 в формате двойное слово и плавающей точкой.

*Решение.*

Здесь мантисса = -0.11000001, фактический порядок =10002 .

Машинный порядок: Мр = 10000002 + 10002 = 10010002.

| | Знак числ | Порядок 8D = 1000B | | | | | | | Мантисса 0.11000001 B | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N разряда | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | … | 1 | 0 |
| Число | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | | 0 | 0 |

Двоично-десятичные числа могут быть представлены в ЭВМ полями переменной длины в так называемых упакованном и распакованном форматах.

Двоично-десятичная система счисления получила большое распространение в современных ЭВМ ввиду легкости перевода в десятичную систему счисления и обратно. Она используется при решении задач учетно-статистического характера. В этой системе счисления все десятичные цифры отдельно кодируются четырьмя двоичными цифрами (тетрадами) и в таком виде записываются последовательно друг за другом.

**Пример 3.** Записать десятичное число 9703 в двоично-десятичной системе счисления.

*Решение.*

| | | | |
|---|---|---|---|
| 1001 | 0111 | 0000 | 0011 |

В упакованном формате для каждой десятичной цифры отводится по 4 двоичных разряда (полубайта), при этом знак числа кодируется в крайнем правом полубайте числа (1100 — знак "+" и 1101 — знак "-").

Структура поля двоично-десятичного упакованного формата:

| | | | | |
|---|---|---|---|---|
| Цф | Цф | ... | Цф | Знак |

Здесь и далее: Цф — цифра, Знак — знак числа

Упакованный формат используется обычно в ЭВМ при выполнении операций сложения и вычитания двоично-десятичных чисел.

В распакованном формате для каждой десятичной цифры отводится по целому байту, при этом старшие полубайты (зоны) каждого байта (кроме самого младшего) заполняются кодом 0011 (в соответствии с ASCII-кодом), а в младших (левых) полубайтах обычным образом кодируются десятичные цифры. Старший полубайт (зона) самого младшего (правого) байта используется для указания кода знака числа.

Структура поля распакованного формата:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Зона | Цф | Зона | Цф | ... | Зона | Цф | Знак | Цф |

Распакованный формат используется при вводе-выводе информации в ЭВМ, а также при выполнении операций умножения и деления двоично-десятичных чисел.

**Пример 4.** Представить число -193D в упакованном и распакованном форматах.

*Решение.*

В упакованном формате:

| | | | |
|---|---|---|---|
| 0001 | 1001 | 0011 | 1101 |

В распакованном формате:

| | | | | | |
|---|---|---|---|---|---|
| 0011 | 0001 | 0011 | 1001 | 1101 | 0011 |

ЭБС ПГУТИ

# 5. Криптографические и стеганографические методы защиты информации

Рассмотрим классические шифры, которые в настоящее время представляют лишь исторический интерес, однако позволяют понять основные идеи криптографии.

## 5.1. Шифр Цезаря

**Пример 1.** Требуется расшифровать криптограмму:
КГУВЙЗРРСПЦХГРНЦЕЖЦОСРЗФПСХУВХ
*Решение.*
Составим таблицу замен, в которой алфавит криптограммы циклически смещен по отношению букв алфавита открытого текста на три позиции:

Табл. 5.1.1.

| А | Б | В | Г | Д | Е | Ё | Ж | З | … |
|---|---|---|---|---|---|---|---|---|---|
| Г | Д | Е | Ё | Ж | З | И | Й | К | … |

В результате дешифрации получено:
ЗАРЯЖЕННОМУ ТАНКУ В ДУЛО НЕ СМОТРЯТ

## 5.2. Шифр атбаш

**Пример 2.**
Требуется расшифровать криптограмму:
ФЯШЫДХНРРЮЁЯБЁЦХНАНРНЛЫЛЭЪОЪСЗМРЪЬРЛОРЭЪСГЭДЖЪ

*Решение.*
Составим таблицу замен, в которой первая буква алфавита открытого текста заменяется на последнюю букву алфавита криптограммы, вторая буква заменяется на предпоследнюю и т.д. Таблица замен состоит из двух строк, причем в нижней строке записаны те же символы, что и в верхней строки, но начиная с конца.

Табл. 5.2.1.

| А | Б | В | Г | Д | Е | Ё | Ж | З | … |
|---|---|---|---|---|---|---|---|---|---|
| Я | Ю | Э | Ь | Ы | Ъ | Щ | Ш | Ч | … |

В результате дешифрации получено:

КАЖДЫЙ СООБЩАЮЩИЙСЯ СОСУД УВЕРЕН ЧТО ЕГО УРОВЕНЬ ВЫШЕ

## 5.3. Квадрат Полибия

**Пример 3.** Требуется расшифровать криптограмму:
41 34 12 11 51 56 63 15 36 43 22 12 11 15 34 35 16 36 13 34 25 26 34 41 42 24

ЭБС ПГУТИ

*Решение.*

Составим таблицу замен:

Табл. 5.3.1.

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

Для расшифрования числа 41 нужно найти букву, которая находится на пересечении строки 4 и столбца 1. Из таблицы видно, что этим символом является буква «С». Аналогично происходит дешифрация остальных символов. В результате получен текст:

СОБАЧЬЯ ДРУЖБА ДО ПЕРВОЙ КОСТИ

### 5.4. Метод перестановок

**Пример 4.** Требуется расшифровать криптограмму:

ДКАГЧЬОВА_РУААКОЕБЗЕРЕ_ДСОХТЕСЕ_Т_ЛУ

Известно, что при шифровании использованы матрица 6x6, ключ записи 352146 и ключ считывания 425316.

*Решение.*

Правило дешифрирования криптограммы, полученной методом перестановок, формулируется так.

Чтобы дешифровать криптограмму, полученную с помощью матрицы *n x n*, нужно криптограмму разбить на группы символов по *n* символов в каждой группе. Крайнюю левую группу записать сверху - вниз в столбец, номер которого совпадает с первой цифрой ключа считывания. Вторую группу символов записать в столбец, номер которого совпадает со второй цифрой ключа считывания и т.д. Открытый текст считывать из матрицы по строкам в соответствии с цифрами ключа записи.

Разобьем шифрограмму на группы по 6 символов:

ДКАГЧЬ ОВА_РУ ААКОЕБ ЗЕРЕ_Д СОХТЕС Е_Т_ЛУ

Затем первую группу символов запишем в столбец 4 матрицы 6x6 (рис. 5.4.1), так как первая цифра ключа считывания – 4 (см. рисунок а). Вторую группу из 6 символов запишем в столбец 2 (см. рисунок б), третью группу символов – в столбец 5 (см. рисунок в), пропустив две фазы заполнения матрицы, изобразим полностью заполненную матрицу (см. рисунок г).

ОБС ПГУТИ

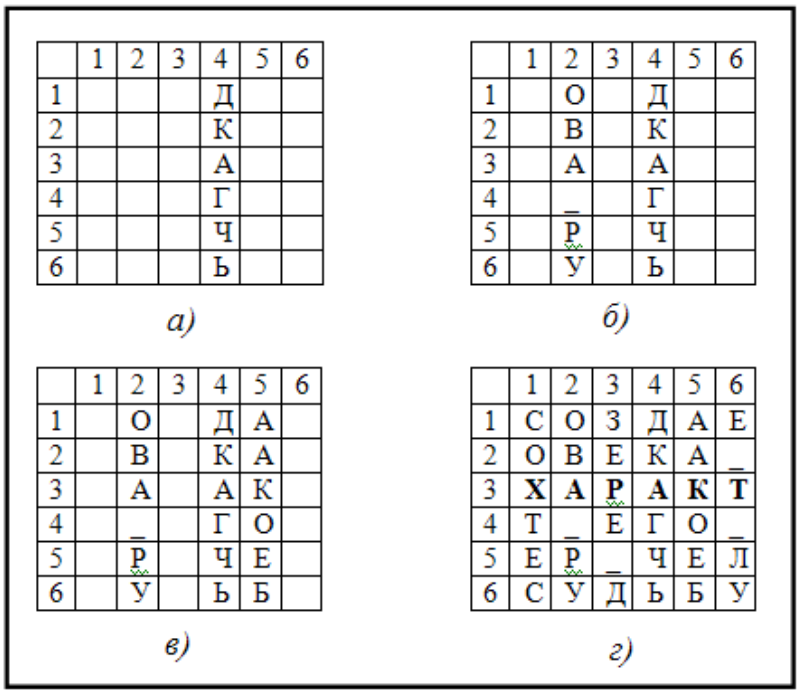



Рис. 5.4.1. Последовательность заполнения матрицы

Считывание открытого текста в соответствии с ключом записи начинаем со строки 3, затем используем строку 5 и т.д. В результате дешифрования получаем открытый текст:

ХАРАКТЕР ЧЕЛОВЕКА СОЗДАЕТ ЕГО СУДЬБУ

**5.5. Метод гаммирования**

**Пример 5.** Требуется расшифровать криптограмму:

ьбгЛ

Известно, что гамма равна:

61 36 32 11

*Решение*

При шифровании методом гаммирования вначале символы открытого текста преобразуют в числа. Затем к числам открытого текста прибавляют секретную гамму (псевдослучайную числовую последовательность). На приемной стороне эту гамму вычитают из криптограммы и получают открытый текст. Добавление гаммы к открытому тексту на передаче и вычитание гаммы на приеме часто осуществляют поразрядно (так называемый поточный шифр). Процедуру добавления гаммы удобно реализовать с помощью двоичных чисел. При этом на каждый бит открытого текста накладывается бит секретной гаммы.

Генератор гаммы выдает псевдослучайную последовательность битов: $\gamma 1$, $\gamma 2$, $\gamma 3,\ldots$, $\gamma n$. Потоки битов гаммы и открытого текста $p1$, $p2$, $p3,\ldots$, $pn$ поразрядно подвергаются логической операции Исключающее ИЛИ. В результате получается поток битов криптограммы:

$$c_i = p_i \oplus \gamma_i.$$

При расшифровании на приемной стороне операция Исключающее ИЛИ выполняется над битами криптограммы и тем же самым потоком гаммы:

$$p_i = c_i \oplus \gamma_i.$$

Благодаря особенностям логической операции Исключающее ИЛИ на приемной стороне операция вычитания заменяется данной логической операцией. Сказанное иллюстрируется примером.

Предположим, что открытый текст P = 10011001, а гамма G = 11001110. В результате шифрования криптограмма C будет иметь следующий вид:

Таблица 5.5.1.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| P | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| G | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| C | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |

На приемной стороне повторно выполняется логическая операция Исключающее ИЛИ:

Таблица 5.5.2.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| C | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| G | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| P | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

Из этих таблиц видно, что переданный и принятый байты P одинаковые.

В таблице 5.5.3. показаны этапы дешифрации рассматриваемого примера.

Следует иметь ввиду, что, если заданная гамма короче текста, то гамму нужно циклически повторить необходимое число раз. Переход от символьной криптограммы к ее записи в виде десятичных чисел осуществляется с помощью таблицы CP-1251 (см. Приложение 1).

Таблица 5.5.3.

| Криптограмма | ь | б | г | Л |
|---|---|---|---|---|
| Криптограмма (десятичная) | 252 | 225 | 227 | 203 |
| Криптограмма (двоичная) | 11111100 | 11100001 | 11100011 | 11001011 |
| Гамма (десятичная) | 61 | 36 | 32 | 11 |
| Гамма (двоичная) | 00111101 | 00100100 | 00100000 | 00001011 |
| Текст (двоичный) | 11000001 | 11000101 | 11000011 | 11000000 |
| Текст (десятичный) | 193 | 197 | 195 | 192 |
| Текст | Б | Е | Г | А |

В результате дешифрования получаем открытый текст:

БЕГА

ЭБС ПГУТИ

### 5.6.Стеганографический метод сокрытия информации

**Пример 6.**

Требуется извлечь сообщение, скрытое в данных (табл. 7 , вариант 10.)

*Решение*

Стеганографические методы защиты информации ориентированы на скрытую передачу информации. В качестве переносчиков информации (контейнеров) могут выступать различные объекты: текстовые документы, рисунки, фотографии, звуковые файлы и т.п.

Стеганография — это наука, изучающая такие методы организации передачи (и хранения) секретных сообщений, которые скрывают сам факт передачи информации.

Криптография превращает открытый текст в нечитаемый набор символов (шифрограмму). Шифрограмма передается по открытому каналу связи, и защита информации держится на сложности подбора секретного ключа. Факт передачи криптограммы не скрывается от противника.

Стеганография нацелена на сокрытие факта передачи информации. Сообщение (его называют вложением) помещают (внедряют) в контейнер, вид которого практически не изменяется от сделанного внедрения.

При сокрытии сообщений методами цифровой стеганографии часто используют информацию, запрятанную в последнем (наименьшем) значащем бите LSB (Last Significant Bits). В отечественных публикациях для его обозначения используют аббревиатуру НЗБ (наименьший значащий бит). При цифровом представлении графики и звука последний бит контейнера является малозначимым, часто изменяющимся по случайному закону. Шумы, возникающие при аналого-цифровом преобразовании звука и изображения (шумы квантования), случайным образом изменяют последний бит каждого отсчета.

Во всех вариантах задания 6 заданы двадцать четыре восьмиразрядных слова. Однако скрытая информация содержится только в последних битах каждого слова. Нужно записать последние биты этих слов в виде последовательности из 24-х битов. Полученную последовательность битов нужно разделить на три байта. Для варианта 10 получим:

11101010_11101110_11001101

Затем каждый байт следует перевести из двоичной системы счисления в десятичную СС:

234 _238 _ 205

Наконец, с помощью таблицы СР-1251 нужно определить скрытый в данных текст:

коН

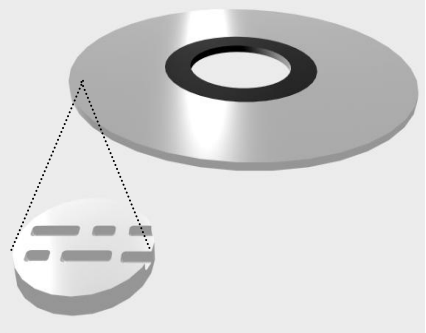
ЭБ ГГТУ ГИ

## Приложение 1

**Таблица CP-1251**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **пробел** | 32 | **!** | 33 | **"** | 34 | **#** | 35 | **$** | 36 |
| **%** | 37 | **&** | 38 | **'** | 39 | **(** | 40 | **)** | 41 |
| ***** | 42 | **+** | 43 | **,** | 44 | **-** | 45 | **.** | 46 |
| **/** | 47 | **0** | 48 | **1** | 49 | **2** | 50 | **3** | 51 |
| **4** | 52 | **5** | 53 | **6** | 54 | **7** | 55 | **8** | 56 |
| **9** | 57 | **:** | 58 | **;** | 59 | **<** | 60 | **=** | 61 |
| **>** | 62 | **?** | 63 | **@** | 64 | **A** | 65 | **B** | 66 |
| **C** | 67 | **D** | 68 | **E** | 69 | **F** | 70 | **G** | 71 |
| **H** | 72 | **I** | 73 | **J** | 74 | **K** | 75 | **L** | 76 |
| **M** | 77 | **N** | 78 | **O** | 79 | **P** | 80 | **Q** | 81 |
| **R** | 82 | **S** | 83 | **T** | 84 | **U** | 85 | **V** | 86 |
| **W** | 87 | **X** | 88 | **Y** | 89 | **Z** | 90 | **[** | 91 |
| **** | 92 | **]** | 93 | **^** | 94 | **_** | 95 | **`** | 96 |
| **a** | 97 | **b** | 98 | **c** | 99 | **d** | 100 | **e** | 101 |
| **f** | 102 | **g** | 103 | **h** | 104 | **i** | 105 | **j** | 106 |
| **k** | 107 | **l** | 108 | **m** | 109 | **n** | 110 | **o** | 111 |
| **p** | 112 | **q** | 113 | **r** | 114 | **s** | 115 | **t** | 116 |
| **u** | 117 | **v** | 118 | **w** | 119 | **x** | 120 | **y** | 121 |
| **z** | 122 | **А** | 192 | **Б** | 193 | **В** | 194 | **Г** | 195 |
| Д | 196 | **Е** | 197 | **Ж** | 198 | **З** | 199 | **И** | 200 |
| **Й** | 201 | **К** | 202 | **Л** | 203 | **М** | 204 | **Н** | 205 |
| **О** | 206 | **П** | 207 | **Р** | 208 | **С** | 209 | **Т** | 210 |
| **У** | 211 | **Ф** | 212 | **Х** | 213 | **Ц** | 214 | **Ч** | 215 |
| **Ш** | 216 | **Щ** | 217 | **Ъ** | 218 | **Ы** | 219 | **Ь** | 220 |
| **Э** | 221 | **Ю** | 222 | **Я** | 223 | **а** | 224 | **б** | 225 |
| **в** | 226 | **г** | 227 | **д** | 228 | **е** | 229 | **ж** | 230 |
| **з** | 231 | **и** | 232 | **й** | 233 | **к** | 234 | **л** | 235 |
| **м** | 236 | **н** | 237 | **о** | 238 | **п** | 239 | **р** | 240 |
| **с** | 241 | **т** | 242 | **у** | 243 | **ф** | 244 | **х** | 245 |
| **ц** | 246 | **ч** | 247 | **ш** | 248 | **щ** | 249 | **ъ** | 250 |
| **ы** | 251 | **ь** | 252 | **э** | 253 | **ю** | 254 | **я** | 255 |

ЭБС ГГТУ им



ЭБС ПГУТИ