МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Курганский государственный университет»

Кафедра информационных технологий
и методики преподавания информатики

ОСНОВЫ МАТЕМАТИЧЕСКОЙ ОБРАБОТКИ ИНФОРМАЦИИ

Методические рекомендации
для студентов направления подготовки 050100.62

Курган 2015

Кафедра: «Информационных технологий
и методики преподавания информатики»

Дисциплины: «Основы математической обработки информации»
(направление 050100.62),
«Компьютерные науки»
(направление 010100.62).

Составили: старший преподаватель О.А. Сидорова;
старший преподаватель Е.Н. Томилова.

Утверждены на заседании кафедры «9» декабря 2013 г.
Рекомендованы методическим советом университета «20» декабря 2013 г.

РАЗДЕЛ 1. ИНФОРМАЦИЯ, ЕЁ СВОЙСТВА И ИЗМЕРЕНИЕ

Цель: изучить основные способы измерения информации.

Оборудование: калькулятор.

Существует несколько подходов к измерению информации.

Первый подход – вероятностный.

Научный подход к оценке сообщений был предложен еще в 1928 году Р. Хартли. Расчетная формула Хартли для равновероятностных событий имеет вид:

$$\mathbf{I = \log_2 N} \text{ или } \mathbf{2^I = N}, \quad (1)$$

где N – количество *равновероятных* событий (число возможных выборов),

I – количество информации. Единицей измерения количества информации является бит.

Пример 1. Сколько бит информации несет сообщение о том, что поезд прибывает на один из 8 путей?
Формула Хартли: $I = \log_2 N$,
где N – число равновероятных исходов события, о котором речь идет в сообщении, (N=8);
I – количество информации в сообщении.
$I = \log_2 8 = 3$(бит).
Ответ: 3 бита.

Вероятность события вычисляется по формуле

$$\mathbf{p = K/N}, \quad (2)$$

где K – величина, показывающая, сколько раз произошло интересующее нас событие;

N – общее число возможных исходов, событий.

С использованием вероятности формула (1) записывается следующим образом:

$$\mathbf{I = \log_2 1/p.} \quad (3)$$

Если вероятность становится меньше, то количество информации увеличивается.

Пример 2. В классе 30 человек. За контрольную работу по математике получено 6 пятерок, 15 четверок, 8 троек и 1 двойка. Сколько бит информации несет сообщение о том, что Иванов получил четверку?
Вероятность интересующего нас события p=15/30. Количество информации в сообщении $I = \log_2(30/15) = \log_2 2 = 1$. Ответ:1 бит.

Общий случай вычисления количества информации в сообщении об одном из N, но уже неравновероятных событий был предложен К. Шенноном в 1948 году.

$$\mathbf{I = -\sum_{i=1}^{N} p_i \log_2 p_i} \qquad (4)$$

где I – количество информации,

p_i – вероятность наступления i-ого события из N-возможных.

Второй подход – алфавитный. При этом подходе количество информации не зависит от содержания, а зависит от мощности алфавита и количества символов в тексте.

Мощность алфавита(A) – количество символов в нем. Объем сообщения измеряется по формуле:

$$\mathbf{V = n \cdot i,} \qquad (5)$$

где n – количество символов в сообщении;

i – информационный объем одного символа, который вычисляется по формуле

$$\mathbf{2^i = A.} \qquad (6)$$

Пример 3. Измерить информационный объем следующей фразы:
О, сколько нам открытий чудных готовит просвещенья дух
Так как фраза набрана компьютерным способом, полагаем, что использовался компьютерный алфавит в кодировке ASCII. Это означает, что информационный объем каждого символа равен 8 бит/символ, т.е. i = = 8 бит/символ. Количество символов в этой фразе – 54, т.е. n=54 символа. Подставляя эти данные в формулу для вычисления информационного объема, имеем: V=54 бит/символ · 8 символов = 432 бита.

Наименьшей единицей измерения количества или объема информации является величина бит. С точки зрения вероятностного подхода 1 бит – это количество информации в сообщении, которое ровно наполовину уменьшает неопределенность о том или ином событии. В алфавитном подходе 1 бит – это минимальный объем, занимаемый 0 или 1 при двоичном кодировании информации.

Так как бит является самой маленькой единицей измерения, его не очень удобно использовать при вычислении объемов даже небольших сообщений. Поэтому используются более крупные единицы:

1 байт = 8 бит

1 Килобайт = 1024 байт = 2^{10} байт

1 Мегабайт = 1024 Килобайт = 2^{20} байт

1 Гигабайт = 1024 Мегабайт = 2^{30} байт

1 Терабайт = 1024 Гигабайт = 2^{40} байт

1 Петабайт = 1024 Терабайт = 2^{50} байт

Упражнения

Базовый уровень

1 Компьютерный алфавит при использовании системы кодировки ASCII имеет мощность 256 символов. Определите информационный вес компьютерного символа в кодировке ASCII.

2 Сообщение с объемом информации 0,25 Кбайт содержит по 128 символов на каждой из 4 страниц. Чему равна мощность использованного алфавита?

3 В школе 4 девятых класса по 16 человек в каждом. Какое количество информации содержится в сообщении «Ученик учится в 9А классе»?

4 Прибор состоит из 128 элементов, размещенных поровну в 4 блоках. Чему равно количество информации в сообщении «Сломался элемент из 3 блока»?

5 Экзамен по информатике оценивается по 15-балльной системе. Возможны следующие оценки в баллах: 2, 6, 7, 8, 9, 11, 13, 15. Чему равно количество информации в сообщении «Абитуриент по информатике получил 9 баллов»?

6 За день первая бригада отремонтировала 4 трактора, вторая – 6 тракторов, третья – 20 и четвертая – 2 (всего в мастерской 4 бригады). Чему равно количество информации в сообщении «Трактор отремонтирован первой бригадой»?

7 Обычный дорожный светофор без дополнительных секций подает 6 видов сигналов. Электронное устройство управления светофором последовательно воспроизводит записанные сигналы. Подряд записано 100 сигналов светофора. Какой объем в байтах занимает эта информация?

8 Автоматическое устройство выполнило перекодировку информационного сообщения на русском языке, которое было записано в 16-битном коде Unicode, в 8-битную кодировку ASCII. При этом объем сообщения уменьшился на 272 бит. Сколько символов в сообщении?

9 Световое табло состоит из лампочек, каждая из которых может находиться в двух состояниях. Какое наименьшее количество лампочек должно находиться на табло, чтобы с его помощью можно было передать 50 различных сигналов?

10 Расположите в порядке возрастания следующие величины: 0,25 Гбайта, 16 Мбайт, 32 Кбайта, 2^{25} байт, 2^{35} бит.

Вариативный уровень

1 В озере разводят карасей и окуней. Подсчитано, что карасей 1500, а окуней - 500. Сколько информации содержится в сообщениях о том, что рыбак поймал карася, окуня, поймал рыбу?

2 В составе поезда 16 вагонов. Среди них есть вагоны купейные и плацкартные. Сообщение о том, что ваш знакомый приезжает в купейном вагоне, несет 3 бита информации. Определите, сколько в поезде купейных вагонов.

3 Добрый экзаменатор никогда не ставит двоек по информатике. По причине своей доброты он заранее определил количество отметок каждого вида и произвольно расставил их абитуриентам. Количество информации, содер-

жащееся в сообщении «Абитуриент Иванов не сдал экзамен на отлично», равно $3-\log_2 7$ бит. Информационный объем сообщения «Абитуриент Сидоров получил четверку» равен двум битам. Найти объем сообщения о получении абитуриентом какой-либо оценки.

4 У скупого рыцаря в сундуке золотые, серебряные и медные монеты. Каждый вечер он извлекает из сундука одну из монет, любуется ею, и кладет обратно в сундук. Информационный объем сообщения «Из сундука извлечена золотая монета» равен трем битам. Количество информации, содержащееся в сообщении «Из сундука извлечена серебряная монета», равно двум битам. Определите информационный объем сообщения о достоинстве вынутой монеты.

5 В некоторой стране автомобильный номер длиной 7 символов составляют по следующему правилу: сначала следует 2 заглавных буквы, затем 4 десятичные цифры и в конце еще одна заглавная буква (задействовано 23 различные буквы). Каждая буква в номере кодируется одинаковым, целым и минимально возможным количеством бит. Каждая цифра в номере кодируется одинаковым, целым и минимально возможным количеством бит. Каждый такой номер в компьютерной программе записывается минимально возможным и одинаковым целым количеством байт. Определите объем памяти, отводимый этой программой для записи 50 номеров.

6 В сейфе банкира Богатеева лежат банкноты достоинством 1, 10 или 100 талеров каждая. Банкир раскрыл свой сейф и наугад вытащил из него одну банкноту. Информационный объем сообщения «Из сейфа взята банкнота достоинством в 10 талеров» равен 3 бита. Количество информации, содержащееся в сообщении «Из сейфа взята банкнота достоинством не в 100 талеров», равно $3-\log_2 5$ бит. Определите информационный объем сообщения о достоинстве наугад вынутой банкноты.

7 Программа защиты данных автоматически генерирует пароль для пользователей. Пароль составляется из 26 латинских букв (строчных и прописных) и цифр от 0 до 9, стоящих в произвольном порядке. Все символы кодируются одинаковым и минимально возможным количеством бит и записываются на диск. Программой было сгенерировано 64 пароля, и они заняли на диске 768 байт памяти. Сколько символов в сгенерированном коде?

8 Информационное сообщение объемом 10 Мбайт передается из пункта А в пункт Б по каналу связи со скоростью передачи данных 2^{21} бит в секунду, а затем из пункта Б в пункт В по каналу связи, обеспечивающему скорость передачи данных 2^{23} бит в секунду. Задержка в пункте Б (время между окончанием приема данных из пункта А и началом передачи в пункт В) составляет 15 секунд. Сколько времени в секундах прошло с момента начала передачи данных из пункта А до их полного получения в пункте В?

9 Электронное письмо объемом 25 Мбайт было отправлено из Москвы в Рязань по каналу связи, обеспечивающему скорость передачи данных 2^{20} бит в секунду, а затем из Рязани в Курск по каналу связи, обеспечивающему скорость передачи данных 2^{22} бит в секунду. Из Москвы в Курск письмо

пришло ровно через 4,5 минуты. Сколько времени в секундах составила задержка письма в Рязани, т.е. время между окончанием приема из Москвы и началом передачи данных в Курск?

10 В школьной базе данных учащиеся получают код длиной 6 символов: первые три символа – заглавные буквы фамилии, имени, отчества (ФИО), следующие три – номер из цифр от 0 до 9. Например, ИАВ009, ПАС123. Каждый такой код в компьютерной программе записывается минимально возможным и одинаковым целым количеством байт (при этом используют посимвольное кодирование, и все символы ФИО кодируются одинаковым и минимально возможным количеством бит, а также все цифры номера кодируются одинаковым и минимально возможным количеством бит). Определите объем памяти, отводимый этой программой для записи кодов 820 учащихся.

Вопросы для самостоятельного изучения

1 Понятие информации в разных науках.
2 Свойства информации.
3 Понятие энтропии.
4 Единицы измерения информации.

РАЗДЕЛ 2. КОДИРОВАНИЕ ИНФОРМАЦИИ

Цель: изучить основные способы кодирования числовой информации.

Оборудование: калькулятор.

Кодирование информации – процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки. Для компьютера такой удобной формой является двоичное кодирование, т.е. представление информации в виде последовательностей сигналов двух видов, обозначаемых 0 и 1.

Недостатком двоичной системы является быстрое нарастание разрядности числа. Поэтому в компьютерной технике помимо двоичной системы, используются восьмеричная и шестнадцатеричная системы.

Таблица 1 – Цифры в системах счисления

Основание системы	Цифровой набор
2	0, 1
8	0, 1, 2, 3, 4, 5, 6, 7
10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(15)

При переводе **целого десятичного числа** в систему с основанием q его необходимо последовательно делить на q до тех пор, пока не останется остаток, меньший или равный (q−1). Число в системе с основанием q записывается как

последовательность остатков от деления, записанных в обратном порядке, начиная с последнего частного.

```
_ 7 5 | 2                                              _ 7 5 | 8
  6   |_ 3 7 | 2                                         7 2 |_ 9 | 8
_ 1 5    2   |_ 1 8 | 2                                    3    8 | 1
  1 4  _ 1 7    1 8 |_ 9 | 2                                    1
    1    1 6      0   8 |_ 4 | 2
           1          1   4 |_ 2 | 2                  _ 7 5 | 16
                          0   2 | 1                     6 4 | 4
                              0                         1 1 (B)
```

Ответ: $75_{10} = 1\ 001\ 011_2 = 113_8 = 4B_{16}$.

При переводе **правильной десятичной дроби** в систему счисления с основанием q необходимо сначала саму дробь, а затем дробные части всех последующих произведений последовательно умножать на q, отделяя после каждого умножения целую часть произведения. Число в новой системе счисления записывается как последовательность полученных целых частей произведения.

Умножение производится до тех пор, пока дробная часть произведения не станет равной нулю или ситуация не перейдет в стадию зацикливания. Рассмотрим перевод на примере перевода дробных чисел 0,25 и 0,15 из десятичной в двоичную систему.

0,	25
	2
0	50
	2
1	00

0,	15	
0	30	
0	60	
1	**20**	период
0	40	период
0	80	период
1	60	период
1	**20**	

Ответ: $0{,}25_{10} = 0{,}01_2$ $\quad 0{,}15_{10} = 0{,}00(1001)_2$

При переводе числа **из системы с основанием q в десятичную** нужно это число представить в виде суммы слагаемых, каждое из которых является произведением цифры числа на основание системы q в степени, соответствующей разряду соответствующей цифры в числе.

Пример 1. *Разряды* $\quad {}^{3\ 2\ 1\ 0\ -1}$

Число $\quad 1\,0\,1\ 1,1_2 = 1{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 1{\cdot}2^0 + 1{\cdot}2^{-1} =$
$= 8 + 0 + 2 + 1 + 0{,}5 = 11{,}5_{10}$

Пример 2. *Разряды* $\quad {}^{2\ 1\ 0\ -1}$

Число $\quad 2\,7\,6,5_8 = 2{\cdot}8^2 + 7{\cdot}8^1 + 6{\cdot}8^0 + 5{\cdot}8^{-1} = 128+56+6+$
$+ 0{,}625 = 190{,}625_{10}$

Пример 3. Разряды $2\ \ 1\ \ 0$

Число $1\ B\ 3_{16} = 1 \cdot 16^2 + 11 \cdot 16^1 + 3 \cdot 16^0 = 256 + 176 + 3 = 435_{10}$

Перевод чисел из двоичной системы счисления в восьмеричную

Каждый разряд восьмеричного числа содержит 3 бита информации. Таким образом, для перевода целого двоичного числа в восьмеричное его нужно разбить на группы по три цифры, справа налево, а затем преобразовать каждую группу в восьмеричную цифру. Если в последней, левой, группе окажется меньше трех цифр, то необходимо ее дополнить слева нулями.

Переведем таким способом двоичное число 101001_2 в восьмеричное:

$101_2 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 5 \qquad 001_2 = 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1$

Следовательно, $101001_2 = 51_8$.

Для перевода дробного двоичного числа (правильной дроби) в восьмеричное необходимо разбить его на триады слева направо и, если в последней, правой, группе окажется меньше трех цифр, дополнить ее справа нулями. Далее необходимо триады заменить на восьмеричные числа.

Пример 4. Преобразуем дробное двоичное число $0{,}110101_2$ *в восьмеричную систему счисления:*

Двоичные триады	*110*	*101*
Восьмеричные цифры	*6*	*5*

Получаем: $0{,}110101_2 = 0{,}65_8$.

Перевод чисел из двоичной системы счисления в шестнадцатеричную

Каждый разряд шестнадцатеричного числа содержит 4 бита информации. Таким образом, для перевода целого двоичного числа в шестнадцатеричное его нужно разбить на группы по четыре цифры (тетрады), начиная справа, и, если в последней левой группе окажется меньше четырех цифр, дополнить ее слева нулями.

Для перевода дробного двоичного числа (правильной дроби) в шестнадцатеричное необходимо разбить его на тетрады слева направо и, если в последней правой группе окажется меньше четырех цифр, то необходимо дополнить ее справа нулями.

Затем надо преобразовать каждую группу в шестнадцатеричную цифру.

Пример 5. Переведем целое двоичное число 101001_2 *в шестнадцатеричное:*

Двоичные тетрады	*0010*	*1001*
Шестнадцатеричные цифры	*2*	*9*

В результате имеем: $101001_2 = 29_{16}$.

Переведем дробное двоичное число $0{,}110101_2$ в шестнадцатеричную систему счисления:

Двоичные тетрады	*1101*	*0100*
Шестнадцатеричные цифры	$13_{10}=D_{16}$	*4*

Получаем: $0{,}110101_2 = 0{,}D4_{16}$.

Для того чтобы преобразовать любое двоичное число в восьмеричную или шестнадцатеричную системы счисления, необходимо произвести преобразования по рассмотренным выше алгоритмам отдельно для его целой и дробной частей.

Перевод чисел из восьмеричной и шестнадцатеричной систем счисления в двоичную

Для перевода чисел из восьмеричной и шестнадцатеричной систем счисления в двоичную необходимо цифры числа преобразовать в группы двоичных цифр. Для перевода из восьмеричной системы в двоичную каждую цифру числа надо преобразовать в группу из трех двоичных цифр (триаду), а при преобразовании шестнадцатеричного числа – в группу из четырех цифр (тетраду).

Пример 6. Преобразуем целое восьмеричное число 47_8 *в двоичную систему счисления:*

Восьмеричные цифры	*4*	*7*
Двоичные триады	*100*	*111*

Получаем: $47_8 = 100111_2$.

Переведем целое шестнадцатеричное число AB_{16} *в двоичную систему счисления:*

Шестнадцатеричные цифры	*A*	*B*
Двоичные тетрады	*1010*	*1011*

В результате имеем: $AB_{16} = 10101011_2$.

Целые числа со знаком обычно занимают в памяти компьютера 1, 2 или 4 байта, при этом самый левый (старший) разряд содержит информацию о знаке числа. Знак «+» кодируется нулем, а «–» – единицей.

Таблица 2 – Диапазоны значений целых чисел со знаком

Формат числа в байтах	Запись с порядком	Обычная запись
1	$-2^7 \dots 2^7-1$	–128 … 127
2	$-2^{15} \dots 2^{15}-1$	–32 768 … 32 767
4	$-2^{31} \dots 2^{31}-1$	–2 147 483 648 … 2 147 483 647

Рассмотрим особенности записи целых чисел со знаком на примере однобайтового формата.

В компьютерной технике применяется три формы записи целого числа со знаком: прямой код, обратный код, дополнительный код. Последние две формы применяются особенно широко, так как позволяют упростить конструкцию арифметико-логического устройства компьютера путем замены разнообразных арифметических операций операцией сложения.

Положительные числа в прямом, обратном и дополнительных кодах изображаются одинаково – двоичными кодами с цифрой 0 в знаковом разряде.

Пример 7. Число $1_{10} = 1_2$. Число положительное, поэтому в знаковом разряде запишем 0. Оставшиеся 7 разрядов необходимо заполнить двоичным кодом числа 1. Недостающие разряды заполняем недостающими нулями слева. В однобайтовом формате во всех трех кодах положительное число 1_2 будет записано следующим образом: 0 0000001.

Пример 8. Число $127_{10} = 1111111_2$. Число положительное, поэтому в знаковом разряде запишем 0. В однобайтовом формате во всех трех кодах положительное число 1111111_2 будет записано следующим образом: 0 1111111.

Отрицательное число в прямом, обратном и дополнительном кодах имеет разные изображения.

1 Прямой код. В знаковый разряд записывается цифра 1, а в разряды цифровой части числа – двоичный код его абсолютной величины.
2 Обратный код получается инвертированием всех цифр абсолютной величины числа. Знаковый разряд не инвертируется.
3 Дополнительный код получается путем прибавления единицы к младшему разряду обратного кода числа.

Пример 9. Записать прямой, обратный и дополнительный коды числа –38. Запишем двоичный код абсолютной величины числа –38. $|-38|_{10} = 38_{10} = 100110_2$. Составим прямой код числа –38. Число отрицательное, следовательно, в знаковый разряд запишется 1. Абсолютная величина в двоичном коде содержит 6 разрядов, следовательно необходимо впереди числа дописать недостающий 0, чтобы заполнить все 7 цифровых разрядов числа. Таким образом, прямой код числа –38 запишется 1 0100110. Обратный код получается инвертированием цифровых разрядов, т.е. заменой 0 на 1, а 1 на 0. Для получения дополнительного кода необходимо прибавить 1 к младшему (крайнему справа) разряду обратного кода числа. Результаты вычисления оформим в виде таблицы 3.

Таблица 3 – Представление отрицательного числа

Число $_{10}$	*Абсолютное значение числа* $_2$	*Прямой код*	*Обратный код*	*Дополнительный код*
–38	*100110*	*1 0100110*	*1 1011001*	*1 1011010*

Арифметические действия над целыми числами

В большинстве компьютеров операция вычитания заменяется сложением уменьшаемого с обратным или дополнительным кодом вычитаемого. Для двоичной системы действия сложения и умножения выполняются в соответствии с таблицами 4 и 5.

Таблица 4 – Сложение

+	0	1
0	0	1
1	1	10

Таблица 5 – Умножение

×	0	1
0	0	0
1	0	1

Рассмотрим примеры вычитания чисел путем сложения их обратных и дополнительных кодов в формате 1 байт.

Пример 10. Вычислить 1 – 38. Заменим вычитание сложением 1+(–38).

1 Переведем в двоичную систему числа 1 и 38.

$$1_{10} = 1_2 \qquad 38_{10} = 100110_2$$

2 Запишем прямой, обратный и дополнительный коды чисел 1 и –38 (таблица 6).

Таблица 6 – Представление чисел 1 и –38

Число	*Прямой код*	*Обратный код*	*Дополнительный код*
1	*0 0000001*	*0 0000001*	*0 0000001*
–38	*1 0100110*	*1 1011001*	*1 1011010*
Результат сложения		*1 1011010*	*1 1011011*

3 Проверим результат сложения:

– в знаковом разряде обратного и дополнительного кодов результата записана 1, что означает, что результат – число отрицательное;

– переведем результат из двоичной системы счисления в десятичную. Для этого сначала получим прямой код результата путем инвертирования цифровых разрядов обратного кода результата 1 0100101, а затем переведем цифровые разряды в десятичное число. $0100101_2 = 1 \cdot 2^5 + 1 \cdot 2^2 + 1 \cdot 2^0 = 32+4+1=37$;

– путем сложения обратных кодов получаем результат –37. Тот же результат получается при выполнении операции вычитания в десятичной системе счисления: 1–38 = –37. Таким образом, действие выполнено верно;

– проверим правильность сложения в дополнительных кодах. Быстрый переход от дополнительного кода к прямому можно выполнить по следующей схеме: сначала инвертировать цифровые разряды дополнительного кода числа, а затем к младшему разряду прибавить 1.

$$1\ 1011011 \rightarrow 1\ 0100100 \rightarrow 1\ 0100101$$

Получили тот же самый результат, что и при сложении в обратном коде. Значит, действие выполнено правильно.

Замечание 1. В случае переполнения разрядной сетки числа в результате сложения обратных кодов единица из разряда переполнения прибавляется к младшему разряду числа.

Замечание 2. В случае переполнения разрядной сетки числа в результате сложения дополнительных кодов единица из разряда переполнения игнорируется.

Пример 11. Выполнить вычитание чисел путем сложения их обратных и дополнительных кодов: –1–38 (см. таблицу 7).

Таблица 7 – Сложение обратных и дополнительных кодов

Число	*Прямой код*	*Обратный код*	*Дополнительный код*
–1	*1 0000001*	*1 1111110*	*1 1111111*
–38	*1 0100110*	*1 1011001*	*1 1011010*
Сложение		*11 1010111* *+1* *Разряд переполнения прибавляется*	*11 1011001* *Разряд переполнения отбрасывается*
Результат		*1 1011000*	*1 1011001*
Проверка	$1\ 0100111_2 = -(1\cdot2^5 + 1\cdot2^2 + 1\cdot2^1 + 1\cdot2^0) = -39$	*Инвертирование цифровых разрядов*	*Инвертирование цифровых разрядов, +1 к младшему разряду*

Деление в любой позиционной системе счисления производится по тем же правилам, как и деление углом в десятичной системе. В двоичной системе деление выполняется проще, чем в других, так как очередная цифра частного может быть только нулем или единицей.

Пример 12. Вычислить 45:5 в двоичной системе счисления. $45_{10} = 101101_2$, $5_{10} = 101_2$

```
_101101 | 101          45:5 = 9
 101    |-----         1001₂ = 1·2³ + 1·2⁰ = 9₁₀
   _101
    101
      0
```

Представление вещественных чисел

Вещественными числами (в отличие от целых) в компьютерной технике называются числа, имеющие дробную часть.

При их написании вместо запятой принято писать точку. Так, например, число 5 – целое, а числа 5.1 и 5.0 – вещественные.

Для удобства отображения чисел, принимающих значения из достаточно широкого диапазона (то есть, как очень маленьких, так и очень больших), используется форма записи чисел с порядком основания системы счисления. Например, десятичное число 1.25 можно в этой форме представить так:

$1.25 \cdot 10^0 = 0.125 \cdot 10^1 = 0.0125 \cdot 10^2 = \ldots$, или так: $12.5 \cdot 10^{-1} = 125.0 \cdot 10^{-2} = 1250.0 \cdot 10^{-3} = \ldots$.

Любое число *N* в системе счисления с основанием *q* можно записать в виде $N = M \cdot q^p$, где *M* называется мантиссой числа, а *p* – порядком. Такой способ записи чисел называется представлением с плавающей точкой.

Если «плавающая» точка расположена в мантиссе перед первой значащей цифрой, то при фиксированном количестве разрядов, отведённых под мантиссу, обеспечивается запись максимального количества значащих цифр числа, то есть максимальная точность представления числа в машине. Из этого следует: мантисса должна быть правильной дробью, первая цифра которой отлична от нуля: $M \in [0.1, 1)$.

Такое, наиболее выгодное для компьютера, представление вещественных чисел называется **нормализованным**. Мантиссу и порядок q-ичного числа принято записывать в системе с основанием q, а само основание – в десятичной системе.

Примеры нормализованного представления:

Десятичная система	Двоичная система
$753.15 = 0.75315 \cdot 10^3$;	$-101.01 = -0.10101 \cdot 2^{11}$ (порядок $11_2 = 3_{10}$)
$-0.000034 = -0.34 \cdot 10^{-4}$;	$-0.000011 = -0.11 \cdot 2^{-100}$ (порядок $-100_2 = -4_{10}$)

Вещественные числа в компьютерах различных типов записываются по-разному. При этом компьютер обычно предоставляет программисту возможность выбора из нескольких числовых форматов наиболее подходящего для конкретной задачи – с использованием четырех, шести, восьми или десяти байтов. Стандарт IEEE 754-1985 определяет четыре формата представления чисел с плавающей запятой (см. таблицу 8).

Таблица 8 – Форматы представления чисел с плавающей запятой

Точность	Размер в битах	Размер смещенного порядка	Размер мантиссы	Примечание
Одинарная	32	8	23	
Двойная	64	11	52	
Одинарная расширенная	43			Редко используемый
Двойная расширенная	79	15	64	Обычно используют 80 бит

Для представления вещественных чисел в памяти компьютера часть разрядов отводится для записи порядка числа, а остальные – для записи мантиссы. Но в этом формате есть один подводный камень – знак может иметь не только число, но и порядок числа также может иметь знак (то есть степень дроби может быть как положительной, так и отрицательной). Чтобы не хранить знак порядка, используется **смещённый порядок**, как показано на рисунке 1.

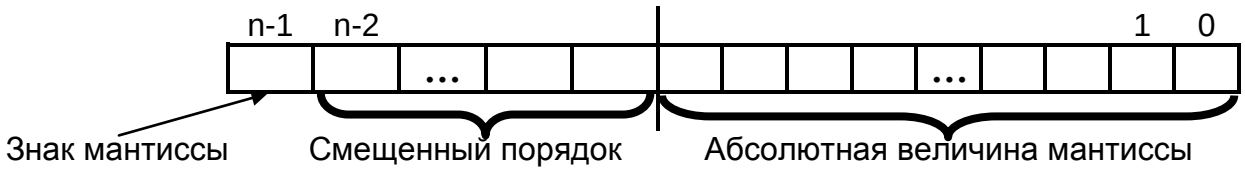

Рисунок 1 – Распределение разрядов при хранении вещественного числа

Если для задания порядка выделено k разрядов, то к истинному порядку (ИП) прибавляют смещение, таким образом, смещённый порядок (СП) определяется по формуле:

$$\mathbf{СП = ИП + 2^{k-1} - 1}, \qquad (7)$$

где k – количество разрядов, выделенных для порядка.

Например, истинный порядок, лежащий в диапазоне –127…+128 представляется смещённым порядком, значения которого меняются в диапазоне 0…255.

Т.е. при ИП = –127, СП = $-127 + 2^{8-1} - 1 = -127 + 128 - 1 = 0$

При ИП = 128, СП = $128 + 2^{8-1} - 1 = 128 + 128 - 1 = 255$

Для представления числа в диапазоне 0…255 требуется 1 байт (8 разрядов), то есть k = 8.

Алгоритм представления вещественного числа в памяти компьютера:

1) перевести число из P-ичной системы в двоичную;
2) представить двоичное число в нормализованной форме;
3) рассчитать смещённый порядок числа;
4) разместить знак, порядок и мантиссу в соответствующие разряды.

Пример 13. Преобразовать число $155{,}125_{10}$ *к* 32*-битному формату.*

1 *Переведем число в двоичную систему счисления:*

$155_{10} = 10011011_2$ $0{,}125_{10} = 0{,}001_2$. *Т.о.* $155{,}125_{10} = 10011011{,}001_2$

2 *Представим двоичное число в нормализованном виде:*

$$10011011{,}001_2 = 0{,}10011011001 \cdot 2^{1000}, \text{ т.к. } 1000_2 = 8_{10}$$

3 Рассчитаем смещенный порядок числа:

ИП = 8*, количество разрядов, выделенных для порядка* $k = 8$.

Подставим в формулу (7) *все имеющиеся данные:*

$$СП = 8 + 2^{8-1} - 1 = 8 + 128 - 1 = 135_{10} = 10000111_2$$

4 Число $155{,}125_{10}$ *положительное, поэтому в самый старший бит в 32-битной последовательности, который отводится для обозначения знака числа, записывается* 0*. Далее пойдут биты порядка. Для этого выделяют* 1 *байт (*8 *бит) и записывают в эти разряды смещенный порядок. Оставшиеся* 23 *бита отводят для мантиссы. Но у нормализованной двоичной мантиссы первый бит всегда равен* 1*. Нет смысла, записывать единицу в отведенные* 23 *бита, поэтому в отведенные* 23 *бита записывают остаток от мантиссы, в нашем случае* 0011011001*. Получаем следующую запись двоичного вещественного числа в* 32*-битном формате:*

$$0\ 10000111\ 00110110010000000000000 = 439B2000_{16}$$

Упражнения

Базовый уровень

1) Переведите числа из десятичной системы в двоичную, восьмеричную и шестнадцатеричную системы счисления:

a) 125; b) 209; c) 88; d) 37,25; e) 206,125; f) 309,6; g) 24,24.

2) Переведите числа из двоичной системы в восьмеричную, десятичную и шестнадцатеричную системы счисления:

a) 1001111111011,0111; b) 1110101011,1011101;

c) 10111001,101100111; d) 1011110011100,11; e) 10111,1111101111.

3) Переведите числа в двоичную систему счисления:

a) 37_8; b) $2A9_{16}$; c) DD_{16}; d) 103_8;

e) $20{,}12_{16}$; f) $30{,}6_8$; g) 124.24_8; h) $103.A_{16}$.

4) Вычислите значение выражения:

a) $256_8 + 101101_2 \cdot (60_8 + 12_{10}) - 1F_{16} = X_{10}$;

b) $1AD_{16} - 100101100_2 : 1010_2 + 217_8 = X_8$;

c) $1010_{10} + (106_{16} - 11011101_2) \cdot 12_8 = X_{16}$;

d) $1011_2 \cdot 1100_2 : 14_8 + (100000_2 - 40_8) = X_2$.

5) Запишите десятичное представление чисел, записанных в обратном коде в однобайтовом формате:

a) 1 1101000; b) 1 0011111; c) 1 0101011; d) 1 1100011; e) 0 1001101;

6) Запишите десятичное представление чисел, записанных в дополнительном коде в однобайтовом формате:

a) 1 1111000; b) 1 0011011; c) 1 1101001; d) 1 1100011; e) 0 1110110.

7) Выполните вычитание чисел путем сложения их обратных (дополнительных) кодов в формате 1 байт:

a) 2–9; b) 9–2; c) 50–25; d) 25–50.

8) Получить шестнадцатеричную форму представления вещественных десятичных чисел в 4-байтовом формате:

a) –125,25; b) 13,125; c) –103,5; d) 25,0625.

Вариативный уровень

1) Определите основание системы счисления:

a) $302_x = 77_{10}$; в) $104_x = 65_8$; c) $212_x = 80_{10}$; d)$305_x = 98_{16}$.

2) Вычислите значение выражения:

a) $256{,}3_8 + 101101{,}01_2 \cdot (60_8 + 12_{10}) – 1F{,}5_{16} = X_{10}$;

b) $1AD{,}8_{16} – 100101100_2 : 1010_2 + 217{,}4_8 = X_8$;

c) $1010{,}7_{10} + (106{,}A_{16} – 11011101{,}01_2) \cdot 12{,}3_8 = X_{16}$;

d) $1011{,}11_2 \cdot 1100{,}1_2 : 14{,}4_8 + (100000{,}101_2 – 40_8) = X_2$.

3) Выполните вычитание чисел путем сложения их обратных (дополнительных) кодов в формате 1 байт:

a) –2–9; b) –50–25; c) –125–50.

4) Получить шестнадцатеричную форму представления вещественных десятичных чисел в 4-байтовом формате:

a) $-125{,}12_{10}$; b) $13{,}15_{10}$; c) –103,35; d) 25,14.

5) По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой с одинарной точностью восстановить само десятичное число:

a) $C9811000_{16}$; b) $C3920000_{16}$; c) 44892000_{16}; d) $589C1000_{16}$.

Вопросы для самостоятельного изучения:

1 Позиционные системы счисления.

2 Непозиционные системы счисления.

3 Стандарты представления вещественных чисел.

4 Нормальная и экспоненциальная форма представления вещественных чисел.

РАЗДЕЛ 3. ШИФРОВАНИЕ

Цель: изучить аффинный метод и метод шифрования, основанный на использовании матричной алгебры.

Оборудование: Microsoft Excel, MathCad.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука).

Криптология – наука о создании и анализе систем безопасности связи. Криптология разделяется на два направления – ***криптографию*** и ***криптоанализ***. Цели этих направлений прямо противоположны.

Криптография – это наука о методах обеспечения секретности и подлинности (идентичности) данных при их передаче по линиям связи или хранении. Криптография занимается поиском и исследованием математических методов преобразования информации.

Криптоанализ – это наука о методах раскрытия или подделки данных.

Рассмотрим два метода шифрования.

Аффинная система подстановок Цезаря

Пусть дано

- исходной алфавит Ао;
- шифрующий алфавит A_1;
- исходный текст;
- $\mathbf{k_1}$ – десятичный коэффициент;
- $\mathbf{k_2}$ – коэффициент сдвига; $\mathbf{0 \le k_1, k_2 \le R-1}$, где **R** – число букв в алфавите**.**

Алгоритм шифрования:

Шаг 1. Заменить каждый символ исходного текста его порядковым номером **i** в алфавите (от 1 до 32).

Шаг 2. Вычислить значение **h** по формуле:

$$\mathbf{h_i = (k_1 \cdot i + k_2) \bmod R,} \qquad (8)$$

Выбранные коэффициенты k_1, k_2 должны обеспечивать однозначное соответствие чисел i и h_i (числа $\mathbf{k_1}$ **и R** должны быть взаимно простыми). При получении $h_i = 0$ нужно выполнить замену $h_i = R$.

Шаг 3. Получение шифртекста путем замены каждого числа h_i соответствующим символом шифртекста алфавита шифрования A_1 размера [1×R].

Пример 1. Исходными данными для шифрования являются:

Исходный текст: <МЕТОД_ШИФРОВАНИЯ>;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_>;

A_1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЛЪШБУЮ>;

R=32; k_1=3; k_2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг1*. Заменяем буквы исходного текста на порядковые номера в алфавите* $\boldsymbol{A_0}$*:*

<12, 6, 18, 14, 5, 32, 24, 9, 20, 16, 14, 3, 1, 13, 9, 31>.

Шаг 2*. Вычисляем соответствующие номера букв шифртекста, которые будем брать в алфавите* $\boldsymbol{A_1}$*:*

$$\mathbf{h_1 = (3 \cdot 12 + 15) \bmod 32 = 51 \bmod 32 = 19}$$
$$\mathbf{h_2 = (3 \cdot 6 + 15) \bmod 32 = 33 \bmod 32 = 1}$$
$$\mathbf{h_3 = (3 \cdot 18 + 15) \bmod 32 = 69 \bmod 32 = 5 \text{ и т.д.}}$$

Получаем: **<19, 1, 5, 25, 30, 15, 23, 10, 11, 31, 25, 24, 18, 22, 10, 12>**

Шаг 3. *Заменяем* h_i *на соответствующие символы алфавита* A_1

Шифртекст: <СОЯГБДИМЧУГЦКПМХ>.

Расшифрование осуществляется путем решения целочисленного уравнения:

$$\mathbf{k_1\, i + k_2 = n\, R + h_i} \qquad (9)$$

При известных целых величинах $\mathbf{k_1}$, $\mathbf{k_2}$, $\mathbf{h_i}$ и **R** величина **i** вычисляется методом перебора **n**. Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.

Но **расшифрование** легче проводить следующим образом: сначала построить таблицу замены, в которой взаимозаменяемые символы располагаются в одном столбце:

S_i – i-ый символ исходного текста;

i – позиция исходного символа в алфавите **A_0;**

h_i – позиция символа шифртекста в алфавите **A_1;**

b_i – i-ый символ шифртекста (см. таблицу 9).

Таблица 9 – Таблица замены для примера 1

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

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки $\mathbf{S_i}$ таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки $\mathbf{b_i}$, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке $\mathbf{b_i}$.

Пример 2. *Расшифруем* **СОЯГБ**. *Ищем символ в последней строке таблицы замены* (**b_i**) (*таблица 9*). *Заменяем его на символ из первой строки* (**S_i**) *этого же столбца. Получаем*

С О Я Г Б

М Е Т О Д

Упражнения

В каждом упражнении выполнить следующее задание:

1 Зашифровать исходный текст.

2 Получить таблицу замены для данных алфавитов.

3 Расшифровать с помощью таблицы замены шифртекст.

1 Исходными данными для шифрования являются:
Исходный текст: <**ИСХОДНАЯ_ИНФОРМАЦИЯ**>; R=32; k_1=5; k_2=10;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ЩКРЬДЫЯТФУЮЕЗСЦГНЛЭ_ЖМЧХПИЪШБАОВ>.
Шифртекст: **ИТКТЮЧТУХТЩГБЧОЩТЮЮГАГУФИЦПЮТЮЧД.**

2 Исходными данными для шифрования являются:
Исходный текст: <**ЗАЩИТА_ИНФОРМАЦИИ**>; R=32; k_1=7; k_2=4;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <КЩРЬДЫЯТФУЮМЧХПИЪШБАОЕЗСЦГНЛЭ_ЖВ>.
Шифртекст: **РНЗЫЯЖКХЬЯЮЖЖКХЬЯЪЭЬМРИАЫЦЮЖРЭ.**

3 Исходными данными для шифрования являются:
Исходный текст: <**МЕТОД_ЗАМЕНЫ**>; R=32; k_1=9; k_2=5;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ХПИЪШБАОЕЗСЦГНЛЭ_ЖВКЩРЬДЫЯТФУЮМЧ>.
Шифртекст: **ЮР_ЧИОШРЮПИЖЯИЕИШАТМЮАН.**

4 Исходными данными для шифрования являются:
Исходный текст: <**КРИПТОГРАФИЯ**>; R=32; k_1=7; k_2=6;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ЛЭ_ЖВКЩХПИЪШБАОЕЗСЦГНРЬДЫЯТФУЮМЧ>.
Шифртекст: **ЖБГЦВЧБКЮБЯЕЛ_КПЦМКБЦСБТВЖБ.**

5 Исходными данными для шифрования являются:
Исходный текст: <**ПОЛИАЛФАВИТНЫЙ**>; R=32; k_1=5; k_2=7;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ЪШБАОЛЭ_ЖВКЩХПИЕЗСЦГНРЬДЫЯТФУЮМЧ>.
Шифртекст: **Г_КХЬБЩНГШЭГБООЪЭНО__ХФЪЖ.**

6 Исходными данными для шифрования являются:
Исходный текст: <**МОНОАЛФАВИТНЫЙ**>; R=32; k_1=5; k_2=6;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ХПИЕЗСЦГЪШБАОЛЭ_ЖВКЩНРЬДЫЯТФУЮМЧ>.
Шифртекст: **ЖРЕМПЕЧСКСА_ВЕДЧСЛБИКЧОСКЦШАРПБЩКК.**

7 Исходными данными для шифрования являются:
Исходный текст: <**ИСХОДНЫЕ_ДАННЫЕ**>; R=32; k_1=7; k_2=6;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <БАОЛЭМЧ_ЖВКЩНХПИЕЗСЦГЪШРЬДЫЯТФУЮ>.
Шифртекст: **ЪНФЫЭЛЭИМХЭЗЪ_ЫНСЯБОЬМТЭТЛИД.**

8 Исходными данными для шифрования являются:
Исходный текст: <**ТЕКСТОВЫЙ_РЕДАКТОР**>; R=32; k_1=9; k_2=5;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ВКЩНХПБАОЛЭМЧ_ЖИЕЗСЦЯТФУЮГЪШРЬДЫ>.
Шифртекст: **Я_ЧЫТБТЪХРТЮЯЩЫ_АЖГУКХЬТЬБЪЕ.**

9 Исходными данными для шифрования являются:
Исходный текст: <**ТЕКСТОВЫЙ_ПРОЦЕССОР**>; R=32; k_1=6; k_2=4;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ОЛЭМЧ_ВКЩНХПБАЖИЕЗГЪШРЬДЫСЦЯТФУЮ>.
Шифртекст: **УЪЗДЖКЕДВЯЗЭЗЭВОКАНЯЕФС_ЗДЭЧЩКУЗ_ЗВ.**

10 Исходными данными для шифрования являются:
Исходный текст: <**ИНФОРМАЦИОННАЯ_БЕЗОПАСНОСТЬ**>; R=32; k_1=5; k_2=4;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ОЛЭМЧ_ВКЩНХПБАЖИЕЗГЪШРЬДЫСЦЯТФУЮ>.
Шифртекст: **ЭЫФЪНЕЫФГЩМПЩОЕФХМФЛЦЛКНЧЧНЕМЦЕЧЕЕ.**

Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании ***матричной алгебры***. Зашифрование k-го блока исходной информации, представленного в виде вектора $B_k=||b_i||$, осуществляется путем перемножения матрицы-ключа $A=||a_{ij}||$ и вектора $B_к$. В результате перемножения получается блок шифртекста в виде вектора $C_k=||c_i||$, где элементы вектора $C_к$ определяются по формуле:

$$c_i = \sum_j a_{ij} b_j. \qquad (10)$$

Расшифрование информации осуществляется путем последовательного перемножения векторов $C_к$ и матрицы A^{-1}, обратной матрице A.

Пример 3. Шифрование информации с использованием алгебры матриц.
Пусть необходимо зашифровать и расшифровать исходный текст <**ЗАБАВА**> *с помощью матрицы-ключа A*:

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1. *Заменить каждый символ исходного текста его порядковым номером i в алфавите* (от 1 до 32):

<8, 1, 2, 1, 3, 1>.

Шаг 2. *Умножить матрицу* A *на векторы* B_1={8, 1, 2} и B_2={1, 3, 1}:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} \qquad C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}$$

Шаг 3. *Зашифрованное слово записывается в виде последовательности чисел* <28, 35, 67, 21, 26, 38>.

Расшифрование текста осуществляется следующим образом:

Пример 4. Расшифруем <28, 35, 67, 21, 26, 38>.

Шаг 1*. Вычисляется определитель* |A |= –115.

Шаг 2*. Определяется присоединенная матрица* A, *каждый элемент которой является алгебраическим дополнением элемента* a_{ij} *матрицы* A, *т.е. каждый элемент вычисляется следующим образом*: $(-1)^{i+j}$ *умноженное на определитель матрицы, у которой вычеркнуты строка и столбец, в которой стоит элемент. Получаем:*

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

Шаг 3*. Получается транспонированная матрица* A^T *путем перестановки строк и столбцов:*

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

Шаг 4*. Вычисляется обратная матрица* A^{-1} *по формуле*:

$$\mathbf{A^{-1}} = \frac{\mathbf{1}}{\mathbf{|A|}}\mathbf{A^T} \qquad (11)$$

В результате вычислений обратная матрица имеет вид:

$$A^{-1} = \begin{vmatrix} 17/115 & 52/115 & -48/115 \\ -3/115 & -43/115 & 22/115 \\ -15/115 & 15/115 & -5/115 \end{vmatrix}$$

Шаг 5. *Определяются векторы* B_1 и B_2: $B_1=A^{-1}C_1$; $B_2 = A^{-1}C_2$.

$$B_1 = \begin{vmatrix} 17/115 & 52/115 & -48/115 \\ -3/115 & -43/115 & 22/115 \\ -15/115 & 15/115 & -5/115 \end{vmatrix} \bullet \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} \qquad B_2 = \begin{vmatrix} 17/115 & 52/115 & -48/115 \\ -3/115 & -43/115 & 22/115 \\ -15/115 & 15/115 & -5/115 \end{vmatrix} \bullet \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}$$

Шаг 6*. Последовательность чисел зашифрованного слова* <8, 1, 2, 1, 3, 1> *заменяется символами, в результате чего получается исходное слово* <**ЗАБАВА**>.

Упражнения

1 Зашифровать исходный текст <МАТРИЧНАЯ_АЛГЕБРА> с помощью матрицы-ключа A:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
41, 77, 67, 108, 207, 207, 177, 327, 289, 162, 312, 266, 130, 246, 226, 86, 172, 143

2 Зашифровать исходный текст <БЕЗОПАСНОСТЬ_ИНФОРМАЦИИ> с помощью матрицы-ключа A:

$$A = \begin{vmatrix} 5 & 1 & 3 \\ 9 & 6 & 2 \\ 4 & 7 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
55, 97, 126, 118, 199, 287, 122, 246, 264, 54, 159, 230, 155, 279, 124

3 Зашифровать исходный текст <ТРАНСПОРТИРОВКА> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
135, 256, 278, 160, 289, 266, 46, 91, 244, 116, 218, 213, 211, 394, 415

4 Зашифровать исходный текст <СОВЕРШЕННО_СЕКРЕТНО> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 5 & 1 & 3 \\ 9 & 6 & 2 \\ 4 & 7 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
118, 199, 287, 122, 246, 264, 54, 159, 230, 155, 279, 124

5 Зашифровать исходный текст <ОБЪЕКТИВНАЯ_ОЦЕНКА> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
93, 174, 191, 84, 162, 154, 70, 134, 175

6 Зашифровать исходный текст <КОЛИЧЕСТВО_ИНФОРМАЦИИ> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 5 & 1 & 3 \\ 9 & 6 & 2 \\ 4 & 7 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
212, 375, 351, 139, 258, 282, 76, 267, 253

7 Зашифровать исходный текст <ЗАЩИТА_ИНФОРМАЦИИ> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
129, 244, 287, 107, 208, 162, 70, 134, 175

8 Зашифровать исходный текст <МАТРИЦА_КЛЮЧ> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 5 & 1 & 3 \\ 9 & 6 & 2 \\ 4 & 7 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
118, 254, 262, 161, 342, 397, 240, 361, 427, 126, 218, 194, 103, 261, 194

9 Зашифровать исходный текст <ВЕРОЯТНОСТЬ_ПОЯВЛЕНИЯ> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
104, 191, 252, 127, 237, 277, 85, 161, 131, 6, 12, 42

10 Зашифровать исходный текст <РЕЗУЛЬТАТ_ИССЛЕДОВАНИЯ> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:
60, 112, 102, 64, 127, 166, 126, 238, 283, 211, 394, 415

Вопросы для самостоятельного изучения:

1 Основные понятия информационной безопасности.
2 Случайные угрозы.
3 Преднамеренные угрозы.
4 Основные понятия шифрования.
5 Понятие криптосистемы.
6 Понятия и методы криптоанализа.
7 Симметричные методы шифрования.
8 Ассиметричные методы шифрования.
9 Электронная цифровая подпись.

РАЗДЕЛ 4. МОДЕЛИРОВАНИЕ

Цель: изучить этапы моделирования, отработать навыки разработки различных видов моделей и их реализации в среде Microsoft Excel.

Оборудование: Microsoft Excel.

Основные этапы компьютерного моделирования

1 Постановка задачи.
2 Разработка модели.
3 Компьютерный эксперимент.
4 Анализ результатов моделирования.

Этап 1. Постановка задачи

Этап постановки задачи характеризуется тремя основными стадиями: описание задачи, определение целей моделирования и формализация задачи.

Задача формулируется на обычном языке. Главное – определить объект моделирования и понять, что собой должен представлять результат.

При этом нужно ответить на следующие вопросы:

1) что дано по условия задачи?
2) что требуется найти?
3) какие данные допустимы?
4) какие результаты и в каком виде должны быть получены, а какие нет?

По характеру постановки задачи можно разделить на две основные группы:

- «Что будет, если?» (цель моделирования в этом случае – исследовать изменение характеристик объекта при воздействии на него).
- «Как сделать, чтобы?» (цель моделирования в этом случае – какое произвести воздействие, чтобы параметры объекта удовлетворяли заданному условию?).

Формализацию проводят в виде поиска ответов на вопросы, уточняющие общее описание задачи.

Этап 2. Разработка модели

При построении модели сначала определяется вид модели:

1) ***математическая модель***. При построении данной модели выполняется формальная (математическая) постановка задачи, т.е. представление ее в виде уравнений, соотношений, ограничений и т.п.;
2) ***информационная модель***. При построении данной модели выясняются свойства, состояния, действия и другие характеристики элементарных объектов в любой форме: устно, в виде схем, таблиц. Формируется представление об элементарных объектах, составляющих исходный объект, т.е. информационная модель. Модели должны отражать наиболее существенные признаки, свойства, состояния и отношения объектов предметного мира. Именно они дают полную информацию об объекте;
3) ***компьютерная модель***. Это модель, реализованная средствами программной среды. От выбора программной среды зависит алгоритм построения компьютерной модели, а также форма его представления. В среде программирования – это программа, записанная на языке программирования, в прикладных средах – это последовательность технологических приемов, приводящая к решению задачи.

Помимо этих моделей используются и другие виды моделей.

Этап 3. Компьютерный эксперимент

На данном этапе происходит тестирование модели.

Тест – набор исходных данных, позволяющие определить правильность построения модели. При подборе тестов следует предусмотреть:

1) проверку основных частных случаев;
2) проверку основных типов недопустимых данных;
3) проверку пограничных условий, т.е. тех, которые лежат на границе допустимых и недопустимых значений.

Этап 4. Анализ результатов моделирования

Конечная цель моделирования – принятие решения, которое должно быть выработано на основе всестороннего анализа результатов моделирования. Этот этап решающий: либо продолжается исследование, либо заканчивается. Возможно, известен ожидаемый результат, тогда необходимо сравнить полученный и ожидаемый результаты. В случае совпадения можно принять решение.

Основой для выработки решения служат результаты тестирования и экспериментов. Если результаты не соответствуют целям поставленной задачи, значит, были допущены ошибки на предыдущих этапах. Это может быть слишком упрощенное построение информационной модели, либо неудачный выбор метода или среды моделирования, либо нарушение технологических приемов при построении модели. Если такие ошибки выявлены, то требуется корректировка модели, т.е. возврат к одному из предыдущих этапов. Процесс повторяется до тех пор, пока результаты эксперимента не будут отвечать целям моделирования.

Пример 1. ***Обои и комната***

I этап. Постановка задачи

Описание задачи*. В магазине продаются обои. Известны наименование, длина и ширина рулона. Для удобства обслуживания надо составить таблицу, которая позволит определить необходимое количество рулонов для оклейки любой комнаты.*

Цель моделирования*. Помочь покупателям быстро определять необходимое количество рулонов обоев.*

Формализация задачи. *Формализуем задачу в виде поиска ответов на вопросы (таблица 10).*

Таблица 10 – Формализация задачи

Уточняющий вопрос	***Ответ***
Что моделируется?	*Система, состоящая из двух объектов: комнаты и обоев*
Форма комнаты?	*Прямоугольная*
Что известно о комнате?	*Размеры комнаты задаются высотой (h), длиной (a) и шириной (b)*

Продолжение таблицы 10

Как учитывается неоклеиваемая поверхность?	*15% площади стен комнаты занимают окна и двери. Можно рассчитать процент неоклеиваемой поверхности. Для этого надо знать размеры и количество окон и дверей*
Что известно об обоях?	*Наименования, длина и ширина рулона*
Какая часть рулона уходит на обрезки?	*10% площади рулона*
Надо ли покупать рулоны «про запас»?	*Да, желательно 1 рулон*
Можно ли купить часть рулона?	*Нет. Количество рулонов должно быть целым*
Что надо определить?	*Необходимое количество рулонов обоев*

II этап. Разработка модели
Информационная модель *представлена в таблице 11.*

Таблица 11 – Информационная модель

Объект	*Параметры*	
	название	*значения*
Обои	*Наименование образцов* *Длина рулона (L)* *Ширина рулона (d)* *Обрезки (Обр)* *Площадь рулона ($S_р$)*	*Исходные данные* *Исходные данные* *Исходные данные* *Рекомендуется 10%* *Расчетные данные*
Комната	*Высота (h)* *Длина (a)* *Ширина (b)* *Неоклеиваемая поверхность (НП)* *Площадь стен ($S_{ком}$)*	*Исходные данные* *Исходные данные* *Исходные данные* *Рекомендуется 15%* *Расчетные данные*
Система	*Количество рулонов (N)*	*Результаты*

Дополним информационную модель в табличной форме математической моделью.
При расчете фактической площади рулона, которая пойдет на оклейку помещения, надо отбросить обрезки. Формула имеет вид:

$$\mathbf{S_р = (1–Обр)×L×d}. \qquad (12)$$

В прямоугольной комнате две стены площадью ah, и две стены площадью bh. При расчете фактической площади стен учитывается неоклеиваемая площадь окон и дверей

$$S_{ком} = 2\cdot(a+b)\cdot h\cdot(1–НП). \quad (13)$$

Количество рулонов, необходимых для оклейки комнаты, вычисляется по формуле

$$N = \frac{S_{ком}}{S_р} + 1 \quad (14)$$

Необходимо учесть, что количество рулонов должно быть целым числом, но не меньшим, чем значение T.

Примечание. Значения, указанные в исходных данных в процентах – Обр и НП – используются в расчетных формулах в виде числа, получаемого делением процентного значения на 100. При выполнении расчетов в электронных таблицах делить на 100 не надо, так как тип данных ***Процент*** воспринимается средой именно как число.

Компьютерная модель

Для моделирования выберем среду электронной таблицы. В этой среде информационная и математическая модели объединяются в таблицу, которая содержит три области: исходные данные; промежуточные расчеты; результаты.

Заполним по образцу, представленному на рисунке 2, расчетную таблицу.

	A	B	C	D	E
1	Обои и комната				
2					
3	**Исходные данные**				
4	**Комната**				
5	Высота (h)	2,6			
6	Длина (a)	5			
7	Ширина (b)	3			
8	Неоклеиваемая поверхность	15%			
9	Площадь стен	Формула 1			
10					
11	**Обои**				
12	**Обрезки**	**10%**		**Промежуточные расчеты**	**Результаты**
13	Наименования	Длина	Ширина	Площадь рулона	Количество рулонов
14	Образец 1	10,5	0,5	Формула 2	Формула 3
15	Образец 2	10,5	0,6	Заполнить вниз	Заполнить вниз
16	Образец 3	10,5	0,7		
17	Образец 4	13	0,5		
18	Образец 5	13	0,6		
19	Образец 6	13	0,7		

Рисунок 2 – Расчетная таблица «Обои и комната»

Введем формулы в расчетные ячейки.

Ячейка	**Формула**
B9	=2 ·B6+b7) ·B5 ·(1-B8)
D14	= ·(1-B12) ·B14 ·C14
E14	=ЦЕЛОЕ(B9/D14)+1

Примечание. Функция ЦЕЛОЕ() округляет до ближайшего целого числа, меньшего, чем заданное. Но поскольку количество рулонов нельзя округлять в меньшую сторону, то к значению функции прибавляем 1 для округления в большую сторону и получаем 1 запасной рулон.

III этап. Компьютерный эксперимент

План эксперимента

Тестирование. *Провести тестовый расчет компьютерной модели по данным, приведенным в таблице.*

Эксперимент 1. *Провести расчет количества рулонов обоев для помещений вашей квартиры.*

Эксперимент 2. *Изменить данные некоторых образцов обоев и проследить за пересчетом результатов.*

Эксперимент 3. *Добавить строки с образцами и дополнить модель расчетом по новым образцам.*

Проведение исследования

1 Введите в таблицу тестовые данные, как показано на рисунке 3 и сравните результаты тестового расчета с результатами, приведенными на рисунке 3.

9	Площадь стен	35,36

14	Образец 1	10,5	0,5	4,725	9
15	Образец 2	10,5	0,6	5,67	8
16	Образец 3	10,5	0,7	6,615	7
17	Образец 4	13	0,5	5,85	8
18	Образец 5	13	0,6	7,02	7
19	Образец 6	13	0,7	8,19	6

Рисунок 3 – Тестовые данные

2 Поочередно введите размеры комнат вашей квартиры и результаты расчетов скопируйте в текстовый редактор.

3 Составьте отчет.

4 Проведите другие виды расчетов согласно плану.

IV этап. Анализ результатов

По данным таблицы можно определить количество рулонов каждого образца обоев для любой комнаты.

Упражнения

1 Компьютерный магазин. Магазин компьютерных аксессуаров продает товары, указанные в прайс-листе. Стоимость указана в долларах. Если стоимость товара превышает некоторую сумму, покупателю предоставляется скидка. Составить таблицу-шаблон, позволяющую рассчитать стоимость произвольной покупки. В расчете указать текущий курс доллара.

2 Сберкасса. За два часа до обеденного перерыва 40 бабушек встали в очередь за пенсией. Кассирша обслуживает клиента в среднем за одну минуту.

Первая бабушка «мучила» кассиршу вопросами 9 мин 15 с. Каждая следующая бабушка, частично «мотая на ус» ответы, адресованные предыдущим бабушкам, «мучает» кассиршу на 10 с меньше. Построить модель ситуации и исследовать ее.

3 Нерадивый ученик. Ученик учит стихотворение из 40 строк. Чтобы запомнить первую строчку, ему понадобилось всего 1 мин. На каждую следующую он тратит на 10% времени больше. Стихотворение держится в памяти нерадивого ученика не дольше трех часов, а до школы бежать 15 минут. Как организовать заучивание стихотворения?

4 Расчет кривой падения электрика. Электрик Петров приставил к стене лестницу и, поднявшись вверх, остановился на одной из ступенек. В это время концы лестницы начали скользить вдоль стены и пола. Провести исследование, по какой кривой будет падать вниз электрик.

5 Дачник и собака. От железнодорожной станции по направлению к дачному поселку движется пешеход. Одновременно с ним в том же направлении бежит собака. Поскольку собака бежит быстрее, то, добежав до дома и радостно известив о приближении хозяина, она разворачивается и бежит к человеку, а от него обратно к дому. Какой суммарный путь пробежит собака за время, пока человек дойдет до дома?

6 Буратино и папа Карло. У папы Карло было накоплено 20 золотых, когда Буратино поступил на работу в кукольный театр Карабаса Барабаса. Еженедельно Буратино приносит зарплату 5 золотых, а папа Карло тратит половину (50%) имеющегося на начало недели богатства. Постройте модель изменения капитала в течение нескольких недель. Исследуйте модель и ответьте как изменяется капитал, если увеличить (уменьшить) начальный капитал папы Карло; как изменяется капитал, если увеличить (уменьшить) зарплату Буратино; как изменяется капитал, если увеличить (уменьшить) процент еженедельной траты капитала.

7 График тренировки. Начав тренировки, спортсмен в первый день пробежал 10 км. Каждый следующий день он пробегал на 10% больше предыдущего. Построить таблицу 12.

Таблица 12 – График тренировок

Номер дня п/п	Пробег за день	Суммарный пробег

По таблице определить:

- суммарный пробег за 7 дней;
- через сколько дней спортсмен будет пробегать в день более 20 км;
- через сколько дней суммарный пробег превысит 100 км.

8 Аквариум. Мальчик решил почистить аквариум. Начал с переселения рыб в банку. Семейство рыб, проживающих в аквариуме, составляло 40 штук. Первую рыбку он поймал быстро затратив 5 с, и еще 2 с потратил на пере-

кладывание в банку. Но чем меньше становилось в воде рыбок, тем труднее было их поймать. На каждую следующую рыбку он затрачивал времени больше на 5%, чем на предыдущую. Сколько времени он затратит на переселение рыбок?

9 Награда. Шахматы были изобретены в Индии. Индусский царь Шерам решил наградить изобретателя шахмат, вызвал его к себе и сказал, что исполнит любую его просьбу. Изобретатель удивил царя беспримерной скромностью просьбы:

– Прикажи выдать мне за первую клетку шахматной доски 1 пшеничное зерно, за вторую – 2, за каждую следующую в два раза больше, чем за предыдущую.

Сколько килограммов зерен было выдано изобретателю, если 1 зерно весит 0,05 г?

10 Концентрация раствора. В магазине продается 70% раствор уксусной эссенции. Для домашних нужд обычно используется раствор меньшей концентрации и в разных количествах. Примеры приведены в таблице 13.

Таблица 13 – Концентрация раствора уксусной эссенции

Маринование овощей	1,5 л 0,4-0,6% раствора в 3 л банку
Маринование грибов	100 мл 9% раствора на 1 л банку
Компрессы при высокой температуре	50 мл 3,5% раствора на 1 компресс
Удаление ржавчины	20 мл 50% раствора

Составьте таблицу, по которой можно определить, как изменяется исходная концентрация при добавлении 1, 2, 3 и т.д. частей воды. По таблице определите, сколько надо взять частей воды на 1 часть уксусной эссенции, чтобы получить нужное количество раствора требуемой концентрации, а также подберите вес исходной части раствора (и воды), чтобы получить требуемое количество разбавленного раствора. Исходными данными являются:

- исходная концентрация раствора;
- вес 1 части раствора исходной концентрации (и 1 части воды).

Вопросы для самостоятельного изучения:

1 Понятие модели.
2 Виды классификации моделей.
3 Виды моделей.
4 Инструменты моделирования.

РАЗДЕЛ 5. ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ

Цель: научиться вычислять простейшие статистические показатели по результатам выборки с использование MS Excel.

Оборудование: Microsoft Excel.

Случайная величина – это величина, которая принимает в результате опыта одно из множества значений, причём появление того или иного значения этой величины до её измерения нельзя точно предсказать.

Для задания случайной величины недостаточно перечислить все ее возможные значения, необходимо указать их вероятности. Соответствие между возможными значениями случайной величины и их вероятностями называют **законом распределения** дискретной случайной величины.

При табличном задании закона распределения в первой строке таблицы записываются возможные значения случайной величины, а во второй – соответствующие значениям вероятности (см. таблицу 14).

Таблица 14 – Распределение случайной величины

X	x_1	x_2	…	x_n
p	p_1	p_2	…	p_n

Такая таблица называется **рядом распределения** дискретной случайной величины X.

Для наглядности строят различные графики статистического распределения, и в частности, полигон и гистограмму. Для построения **полигона** частот в прямоугольной системе координат по оси абсцисс OX будем откладывать значения случайной величины x_i, i=1, 2, …, *n*, а по оси ординат OY – соответствующие им вероятности p_i. Полученные точки соединяются отрезками прямых (рисунок 4).

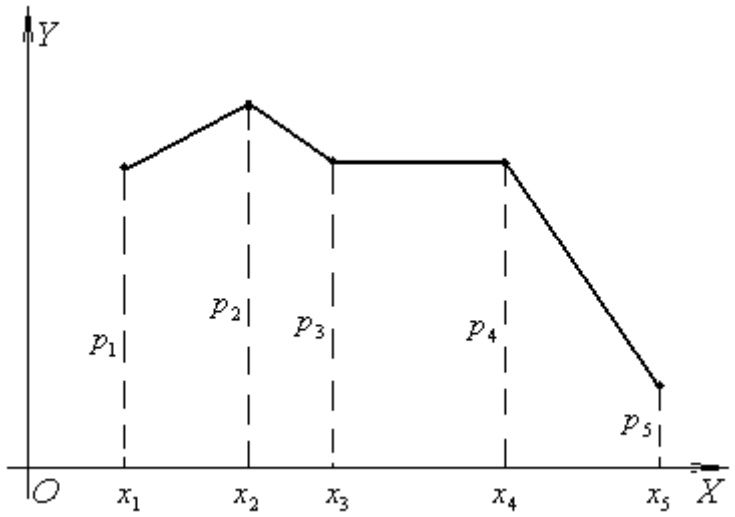

Рисунок 4 – Пример полигона частот

В случае непрерывного признака целесообразно строить **гистограмму,** для чего интервал, в котором заключены все наблюдаемые значения признака, разбивают на несколько частичных интервалов длиной h_i (i=1, 2, ..., n) и находят для каждого частичного интервала m_i – сумму частот варианта, попавших в i-ый интервал. В прямоугольной системе координат построим прямоугольники

с основаниями h_i и высотами (m_i / h_i). Полученная таким образом фигура называется **гистограммой** выборки.

Гистограммой относительных частот называют ступенчатую фигуру, состоящую из прямоугольников, основаниями которых служат частичные интервалы длиною h_i, а высотами являются плотности относительных частот, вычисляемые по формуле (15):

$$\mathbf{h(x_i) = m_i / (n \cdot h_i).} \qquad (15)$$

Пример 1. Построить гистограмму относительных частот для выборки объемом 50, данные для которой приведены в таблице 15.

Таблица 15 – Данные для построения гистограммы

Номер интервала	Границы интервала $x_i - x_{i+1}$	Сумма частот вариант интервала m_i	Плотность относительной частоты m_i / (nh_i)
1	3 - 7	5	
2	7 - 12	10	
3	12 - 17	20	
4	17 - 21	8	
5	21 - 28	7	

Найдем плотность m_i / (nh_i) *относительной частоты для каждого интервала и заполним последний столбец таблицы*:

$m_1 / (nh_1) = 5 / (50 \cdot 4) = 0{,}025$ $\quad$ $m_2 /(nh_2) = 10 / (50 \cdot 5) = 0{,}04$

$m_3 / (nh_3) = 20 / (50 \cdot 5) = 0{,}08$ $\quad$ $m_4 /(nh_4) = 8 / (50 \cdot 4) = 0{,}04$

$m_5 / (nh_5) = 7 / (50 \cdot 7) = 0{,}02$

Построим, как показано на рисунке 5, на оси абсцисс заданные интервалы и проведем над этими интервалами отрезки, параллельные оси абсцисс и находящиеся на расстояниях, равных соответствующим плотностям относительной частоты m_i / (nh_i)

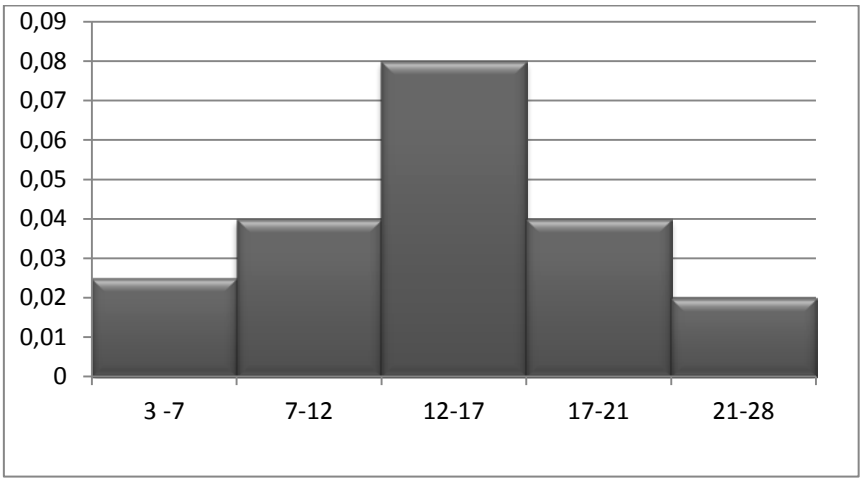

Рисунок 5 – Гистограмма

Математическое ожидание M_x случайной величины x вычисляется по формуле:

$$\boldsymbol{M_x = \sum_{i=1}^{n} p_i x_i} \qquad (16)$$

Математическое ожидание дискретной случай ной величины приближенно равно среднему арифметическому всех её возможных значений.

Модой называют количественное значение исследуемого признака, наиболее часто встречающееся в выборке. К примеру, в последовательности значений признаков 1, 2, 5, 2, 4, 2, 6, 7, 2 модой является значение 2, так как оно встречается чаще других значений – четыре раза.

Моду находят согласно следующим правилам:

1) в том случае, когда все значения в выборке встречаются одинаково часто, принято считать, что этот выборочный ряд не имеет моды. Например: 5, 5, 6, 6, 7, 7 – в этой выборке моды нет;
2) когда два соседних (смежных) значения имеют одинаковую частоту и их частота больше частот любых других значений, мода вычисляется как среднее арифметическое этих двух значений. Например, в выборке 1, 2, 2, 2, 5, 5, 5, 6 частоты рядом расположенных значений 2 и 5 совпадают и равняются 3. Эта частота больше, чем частота других значений 1 и 6 (у которых она равна 1). Следовательно, модой этого ряда будет величина 3,5;
3) если два несмежных (не соседних) значения в выборке имеют равные частоты, которые больше частот любого другого значения, то выделяют две моды. Например, в ряду 10, 11, 11, 11, 12, 13, 14, 14, 14, 17 модами являются значения 11 и 14. В таком случае говорят, что выборка является бимодальной.

Могут существовать и так называемые мультимодальные распределения, имеющие более двух вершин (мод).

Медианой называется значение изучаемого признака, которое делит выборку, упорядоченную по величине данного признака, пополам. Справа и слева от медианы в упорядоченном ряду остается по одинаковому количеству признаков. Например, для выборки 2, 3, 4, 4, 5, 6, 8, 7, 9 медианой будет значение 5, так как слева и справа от него остается по четыре показателя. Если ряд включает в себя четное число признаков, то медианой будет среднее, взятое как полусумма величин двух центральных значений ряда. Для следующего ряда 0, 1, 1, 2, 3, 4, 5, 5, 6, 7 медиана будет равна 3,5.

Выборочное среднее определяется при помощи следующей формулы:

$$\boldsymbol{\bar{X} = \frac{x_1 + x_2 + \cdots + x_n}{n} = \frac{1}{n}\sum_{i=1}^{n} x_i,} \qquad (17)$$

где $\bar{X}$ – выборочная средняя величина или среднее арифметическое значение по выборке;

n – количество испытуемых в выборке или частных показателей, на основе которых вычисляется средняя величина;

x_i – частные значения показателей у отдельных испытуемых. Всего таких показателей n, поэтому индекс i данной переменной принимает значения от 1 до n.

Разброс (иногда эту величину называют размахом) выборки обозначается буквой R. Это самый простой показатель, который можно получить для выборки – разность между максимальной и минимальной величинами данного конкретного вариационного ряда:

$$\mathbf{R= x_{max} - x_{min}.} \qquad (18)$$

Понятно, что чем сильнее варьирует измеряемый признак, тем больше величина R, и наоборот. Однако может случиться так, что у двух выборочных рядов и средние, и размах совпадают, однако характер варьирования этих рядов будет различный. Например, даны две выборки:

X = 10 15 20 25 30 35 40 45 50 X = 30 R = 40

Y = 10 28 28 30 30 30 32 32 50 Y= 30 R = 40

При равенстве средних и разбросов для этих двух выборочных рядов характер их варьирования различен. Для того чтобы более четко представлять характер варьирования выборок, следует обратиться к их распределениям.

Дисперсия – это среднее арифметическое квадратов отклонений значений переменной от её среднего значения.

Дисперсия как статистическая величина характеризует, насколько частные значения отклоняются от средней величины в данной выборке. Чем больше дисперсия, тем больше отклонения или разброс данных.

$$\boldsymbol{D}_x = \frac{\mathbf{1}}{\boldsymbol{n}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}}(\boldsymbol{x_i} - \bar{\boldsymbol{X}})^{\mathbf{2}}, \qquad (19)$$

где D_x – выборочная дисперсия, или просто дисперсия;

выражение в скобках – выражение, означающее, что для всех x, от первого до последнего в данной выборке, необходимо вычислить разности между частными и средними значениями, возвести эти разности в квадрат и просуммировать;

n – количество испытуемых в выборке или первичных значений, по которым вычисляется дисперсия.

Однако сама дисперсия как характеристика отклонения от среднего часто неудобна для интерпретации. Для того, чтобы приблизить размерность дисперсии к размерности измеряемого признака, применяют операцию извлечения квадратного корня из дисперсии. Полученную величину называют **стандартным отклонением**.

$$S_x = \sqrt{D_x}. \quad (20)$$

Метод вторичной статистической обработки, посредством которого выясняется связь или прямая зависимость между двумя рядами экспериментальных данных, носит название метод корреляций. Он показывает, каким образом одно явление влияет на другое или связано с ним в своей динамике. Подобного рода зависимости существуют, к примеру, между величинами, находящимися в причинно-следственных связях друг с другом. Если выясняется, что два явления статистически достоверно коррелируют друг с другом и если при этом есть уверенность в том, что одно из них может выступать в качестве причины другого явления, то отсюда определенно следует вывод о наличии между ними причинно-следственной зависимости.

Когда повышение уровня одной переменной сопровождается повышением уровня другой, то речь идёт о положительной корреляции. Если же рост одной переменной происходит при снижении уровня другой, то говорят об отрицательной корреляции. При отсутствии связи переменных говорят о нулевой корреляцией.

Упражнение

В своей рабочей книге создайте новый лист и переименуйте его, дав название «Статистика».

Заполните на листе «Статистика» данные балльно-рейтинговой системы успеваемости, как показано в таблице 16.

Таблица 16 – Данные балльно-рейтинговой системы успеваемости по дисциплине ОМОИ для групп П-10112, М-10212, М-10312

№ студента	П-10112	М-10212	М-10312
1	34,5	54	35
2	14,5	54,5	38
3	41	56,5	52,5
4	52	49	32,5
5	44	46	38
6	2	52,5	56
7	45,5	0	54
8	53,5	55	33,5
9	31	46	8,5
10	60	43	40
11	6	42,5	35,5
12	39	58,5	9,5
13	64	28,5	44,5
14	53,5	55	58
15	26,5	42	59
16	62	52,5	58

Продолжение таблицы 16

17		53,5	4
18		31,5	
19		53	

Используя встроенные статистические функции MS EXCEL, для каждой группы вычислите МОДУ, МЕДИАНУ, СРЕДНЕЕ, ДИСПЕРСИЮ, РАЗМАХ, СТАНДАРТНОЕ ОТКЛОНЕНИЕ, СКОС. Объясните значение каждого полученного показателя.

Постройте полигон для данных таблицы 16.

Определите длины интервалов, вычислите сумму частот вариант интервала, заполните таблицу 15 и постройте гистограмму.

На этот же лист введите данные из таблицы 17.

Используя функцию КОРРЕЛ, выясните, коррелируют ли данные выполнения контрольной работы с общим результатом по дисциплине для каждой группы.

Таблица 17 – Результаты выполнения контрольной работы по каждой группе

№ студента	П-10112	М-10212	М-10312
1	7	6	7
2	0	6	5
3	6	7	7
4	7	7	8
5	5	7	6
6	0	6	8
7	7	0	7
8	8	9	0
9	2	7	0
10	8	9	7
11	5	8	6
12	6	9	0
13	4	3	9
14	0	8	10
15	6	8	10
16	7	8	7
17		9	0
18		0	
19		9	

Вопросы для самостоятельного изучения:

1 Возможные виды гистограмм распределения.

2 Практический смысл основных статистических характеристик.

3 Возможности пакета Statistica.

ЗАДАНИЯ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

Указания по выполнению контрольной работы.

1 Работа должна быть выполнена в указанные преподавателем сроки.
2 Работа оформляется на листах формата А4. Все задания могут быть оформлены в печатном или рукописном виде.
3 Контрольная работа должна содержать титульный лист, включающий название дисциплины, номер варианта, фамилию, инициалы и номер группы исполнителя.
4 Задания контрольной работы оцениваются следующим образом:
   - задания № 1, № 2, № 3, № 6 – по 1 баллу;
   - задания № 4, № 5, № 7, № 8, – по 2 балла;
   - задание № 9 – 3 балла;
   - задание № 10 – 5 баллов.
5 За несвоевременную сдачу работы будут начисляться штрафные баллы.

Вариант 1

1 Найдите основание системы: $\mathbf{312_x = 54_{10}}$.
2 Вычислите: $\mathbf{A4_{16} + 35_8 = X_{10}}$.
3 Выполните переводы: $\mathbf{100011_2 \rightarrow X_{16}, X_{10}, X_8}$.
4 В некоторой стране автомобильный номер состоит из 7 символов. В качестве символов используют 18 различных букв и десятичные цифры в любом порядке. Каждый такой номер в компьютерной программе записывается минимально возможным и одинаковым целым количеством байтов, при этом используют посимвольное кодирование и все символы кодируются одинаковым и минимально возможным количеством битов. Определите объем памяти, отводимый этой программой для записи 60 номеров.
5 В корзине лежат 32 клубка красной и черной шерсти. Среди них 4 клубка красной шерсти. Сколько информации несет сообщение, что достали клубок красной шерсти? Сколько информации несет сообщение, что достали клубок шерсти любой окраски?
6 Выполните перевод $\mathbf{13{,}13_{10} \rightarrow X_2}$.
7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **27 – 45**.
8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-123{,}125_{10}}$ в формате с плавающей точкой с одинарной точностью.
9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{C9811300_{16}}$ записать число в нормализованном виде в двоичной системе счисления.
10 Аффинная система подстановок Цезаря. Исходными данными для шифрования являются:

Исходный текст: <**ФЕДЕРАЛЬНЫЙ_ЗАКОН**>; R=32; k_1=5; k_2=3;
A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;
A_1 = <ЪШБАОЛЭ_ЖВКЩХПИЕЗСЦГНРЬДЫЯТФУЮМЧ>.
Задание:

а) зашифровать исходный текст;
б) получить таблицу замены для данных алфавитов;
в) расшифровать с помощью таблицы замены:

НЖМПЯЪНДАВЪБДЕДУЪМВБХЪКЖП_ДАЖДУЕ.

Вариант 2

1 Найдите основание системы: $\mathbf{116_x = 62_{10}}$.

2 Вычислите: $\mathbf{3B_{16} + 1010_2 = X_{10}}$.

3 Выполните переводы: $\mathbf{34_8 \rightarrow X_{16}}$, $\mathbf{X_{10}}$, $\mathbf{X_2}$.

4 Для регистрации на сайте некоторой страны пользователю требуется придумать пароль. Длина пароля – ровно 11 символов. В качестве символов используются десятичные цифры и 12 различных букв местного алфавита, причём все буквы используются в двух начертаниях: как строчные, так и заглавные (регистр букв имеет значение). Под хранение каждого такого пароля на компьютере отводится минимально возможное и одинаковое целое количество байтов, при этом используется посимвольное кодирование и все символы кодируются одинаковым и минимально возможным количеством бит. Определите объём памяти, который занимает хранение 60 паролей.

5 Пусть имеется строка текста, содержащая 1000 букв. Буквы встречаются в тексте: «о» – 90 раз, «р» – 40 раз, «ф» – 2 раза, «а» – 200 раз. Какое количество информации несет буква в строке?

6 Выполните перевод $\mathbf{12{,}12_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **31 – 34**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{124{,}125_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{CC811700_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Метод матричной алгебры. Зашифровать исходный текст <**СЛОЖНАЯ_ЗАЩИТА**> с помощью матрицы-ключа A:

$$A = \begin{vmatrix} 1 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:

148, 276, 275, 122, 232, 258, 100, 191, 151, 121, 220, 236, 102, 204, 187.

Вариант 3

1 Найдите основание системы $\mathbf{130_x = 70_{10}}$.

2 Вычислите: $\mathbf{2B_{16} + 23_8 = X_{10}}$.

3 Выполните переводы: $\mathbf{D4_{16} \rightarrow X_2}$, $\mathbf{X_{10}}$, $\mathbf{X_8}$.

4 В классе 30 человек. За контрольную работу по математике получено 6 пятёрок, 15 четвёрок, 8 троек и 1 двойка. Какое количество информации в сообщении о том, что Иванов получил оценку?

5 В велокроссе участвуют 119 спортсменов. Специальное устройство регистрирует прохождение каждым из участников промежуточного финиша, записывая его номер с использованием минимально возможного количества бит, одинакового для каждого спортсмена. Каков информационный объем сообщения, записанного устройством, после того как промежуточный финиш прошли 70 велосипедистов?

6 Выполните перевод $\mathbf{23{,}23_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **23 – 52**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-215{,}25_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{C3A14300_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Аффинная система подстановок Цезаря. Исходными данными для шифрования являются:

Исходный текст: <**ФЕДЕРАЛЬНЫЙ_ЗАКОН**>; R=32; k_1=5; k_2=7;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;

A_1 = <БАОЛЭМЧ_ЖВКЩНХПИЕЗСЦГЪШРЬДЫЯТФУЮ>.

Задание:

а) зашифровать исходный текст;

б) получить таблицу замены для данных алфавитов;

в) расшифровать с помощью таблицы замены:

НЕПНШЧОЭБНЮНЪЧПЩЛЦБХЧЦ_КНШОЩГЦЦ.

Вариант 4

1 Найдите основание системы $\mathbf{101_x = 50_{10}}$.

2 Вычислите: $\mathbf{12_{16} + 1000011_2 = X_{10}}$.

3 Выполните переводы: $\mathbf{DD_{16} \rightarrow X_2}$, $\mathbf{X_{10}}$, $\mathbf{X_8}$.

4 В непрозрачном мешочке хранятся 10 белых, 20 красных, 30 синих и 40 зеленых шариков. Какое количество информации будет содержать зрительное сообщение о цвете вынутого шарика?

5 Обычный дорожный светофор способен выдавать 6 видов сигналов. Электронное устройство управления светофором фиксирует эти сигналы с помощью минимально возможного количества бит. Всего зафиксировано 540 сигналов. Какой объем памяти займет эта информация?

6 Выполните перевод $\mathbf{17{,}17_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **19 – 38**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-104{,}5_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой **$C93E2500_{16}$** записать число в нормализованном виде в двоичной системе счисления.

10 Метод матричной алгебры. Зашифровать исходный текст <**ТЕХНОЛОГИЯ_ЗАЩИТЫ**> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 3 & 1 & 5 \\ 6 & 2 & 9 \\ 4 & 7 & 8 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:

83 153 162 39 77 144 148 280 298 215 411 448 37 74 55.

Вариант 5

1 Найдите основание системы **$121_x = 36_{10}$**.

2 Вычислите: **$AC_{16} + 1101011_2 = X_8$**.

3 Выполните переводы: **$D4_{16} \rightarrow X_2, X_{10}, X_8$**.

4 В коробке лежат кубики: 10 красных, 8 зеленых, 5 желтых, 12 синих. Какое количество информации содержит сообщение о том, что из коробки вынули один кубик?

5 При регистрации в компьютерной системе, используемой при проведении командной олимпиады, каждому ученику выдается уникальный идентификатор – целое число от 1 до 1000. Для хранения каждого идентификатора ученика используется одинаковое и минимально возможное количество бит. В каждой команде участвует 3 ученика. Идентификатор команды состоит из последовательно записанных идентификаторов учеников. Для записи каждого идентификатора команды система использует одинаковое и минимально возможное количество байт. Сколько байт должна отвести система для записи идентификаторов 20 команд?

6 Выполните перевод **$35{,}35_{10} \rightarrow X_2$**.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **23 – 50**.

8 Получить шестнадцатеричную форму внутреннего представления числа **$312{,}25_{10}$** в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой **$C9B52500_{16}$** записать число в нормализованном виде в двоичной системе счисления.

10 Аффинная система подстановок Цезаря. Исходными данными для шифрования являются:

Исходный текст: <**НАЦИОНАЛЬНЫЕ_СТАНДАРТЫ**>; R=32; k_1=9; k_2=5;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;

A_1 = <ЭМЧ_ЖВКЩНХПИЕЗСЦГЪШРЬДЫЯТФУЮБАОЛ>.

Задание:

а) зашифровать исходный текст;

б) получить таблицу замены для данных алфавитов;
в) расшифровать с помощью таблицы замены:

ЩНБЖНПЗЗЯБТОЕЯРГЭБАТЯРТ.

Вариант 6

1 Найдите основание системы: $\mathbf{312_x = 82_{10}}$.
2 Вычислите: $\mathbf{AA_{16} + 27_8 = X_{10}}$.
3 Выполните переводы: $\mathbf{101011_2 \rightarrow X_{16}, X_{10}, X_8}$.
4 Какое количество информации будет содержать зрительное сообщение о цвете вынутого шарика, если в непрозрачном мешочке находится 50 белых, 25 красных, 25 синих шариков?
5 При регистрации в компьютерной системе каждому пользователю выдается пароль, состоящий из 10 символов и содержащий только символы №, $, @, ^. &, %. Каждый такой пароль в системе записывается минимально возможным и одинаковым целым количеством байт (при этом используют посимвольное кодирование и все символы кодируются одинаковым и минимально возможным количеством бит). Определите объем памяти, отводимый системой для записи 65 паролей.
6 Выполните перевод $\mathbf{16{,}16_{10} \rightarrow X_2}$.
7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **34 – 45**.
8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-302{,}125_{10}}$ в формате с плавающей точкой с одинарной точностью.
9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{C3A1B500_{16}}$ записать число в нормализованном виде в двоичной системе счисления.
10 Метод матричной алгебры. Зашифровать исходный текст <**ПРОВОДНИК**> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 5 & 3 & 1 \\ 9 & 6 & 2 \\ 8 & 4 & 7 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:

184 339 318 120 230 264 124 234 235 106 194 239 63 117 96.

Вариант 7

1 Найдите основание системы: $\mathbf{117_x = 97_{10}}$.
2 Вычислите: $\mathbf{AC_{16} + 45_8 = X_{10}}$.
3 Выполните переводы: $\mathbf{76_8 \rightarrow X_{16}, X_{10}, X_2}$.
4 В некоторой стране автомобильный номер длиной 6 символов составляют из заглавных букв (задействовано 17 различных букв) и десятичных цифр в любом порядке. Каждый такой номер в компьютерной программе записывается минимально возможным и одинаковым целым количеством байт (при этом используют посимвольное кодирование и все символы ко-

дируются одинаковым и минимально возможным количеством бит). Определите объем памяти, отводимый этой программой для записи 40 номеров.

5 В мешке Деда Мороза четыре вида конфет, все они одинаковые по форме и весу, но с разной начинкой:
   а) конфет первого вида – 16;
   б) конфет второго вида – 8;
   в) конфет третьего вида – 8;
   г) конфет четвертого вида – 32.

   Сколько бит содержится в информации «Дед Мороз достал конфету»?

6 Выполните перевод $\mathbf{18{,}19_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **18 – 59**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{272{,}0625_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{C5020D00_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Аффинная система подстановок Цезаря. Исходными данными для шифрования являются:

   Исходный текст: <**МЕХАНИЗМ_РЕАЛИЗАЦИИ**>; R=32; k_1=7; k_2=8;

   A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;

   A_1 = <НХПИЕЗСЦГЪШРЬДЫЯТФУЮБАОЛЭМЧ_ЖВКЩ>.

   Задание:

   a) зашифровать исходный текст;
   b) получить таблицу замены для данных алфавитов;
   c) расшифровать с помощью таблицы замены:

   ТЛЪИЛЫ__ПЕФЦЛФЫБСЩЫХССЦЫБИЪЛСЗ_ЪЖ.

Вариант 8

1 Найдите основание системы $\mathbf{120_x = 63_{10}}$.

2 Вычислите: : $\mathbf{AB_{16} + 32_8 = X_{10}}$.

3 Выполните переводы: $\mathbf{8F_{16} \rightarrow X_2}$, $\mathbf{X_{10}}$, $\mathbf{X_8}$.

4 В княжестве есть только черные, белые и серые автомобили. Белых автомобилей 18. Сообщение о том, что в аварию попал черный автомобиль, несет 7 бит информации. Сообщение о том, что в аварию попал не серый автомобиль, несет 5 бит информации. Сколько автомобилей в княжестве?

5 В велокроссе участвуют 69 спортсменов. Специальное устройство регистрирует прохождение каждым из участников промежуточного финиша, записывая его номер с использованием минимально возможного количества бит, одинакового для каждого спортсмена. Каков информационный объем сообщения, записанного устройством, после того как промежуточный финиш прошли 30 велосипедистов?

6 Выполните перевод $\mathbf{51{,}13_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **25 – 44**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-297{,}25_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{C1CAF500_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Метод матричной алгебры. Зашифровать исходный текст <**БОЛЬШОЕ_КОЛИЧЕСТВО**> с помощью матрицы-ключа A:

$$A = \begin{vmatrix} 8 & 1 & 5 \\ 6 & 9 & 2 \\ 4 & 7 & 3 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:

255 204 177 173 226 183 161 138 111 248 186 124.

Вариант 9

1 Найдите основание системы $\mathbf{121_x = 49_{10}}$.

2 Вычислите: : $\mathbf{E2_{16} + 1011011_2 = X_{10}}$.

3 Выполните переводы: $\mathbf{C3_{16} \rightarrow X_2}$, $\mathbf{X_{10}}$, $\mathbf{X_8}$.

4 В коробке находятся кубики трех цветов: красного, желтого и зеленого, причем желтых в два раза больше красных, а зеленых на 6 больше, чем желтых. Сообщение о том, что из коробки случайно вытащили желтый кубик, содержало 2 бита информации. Сколько в коробке зеленых кубиков?

5 Для регистрации на сайте некоторой страны пользователю требуется придумать пароль. Длина пароля – ровно 14 символов. В качестве символов используются десятичные цифры и 12 различных букв местного алфавита, причём все буквы используются в двух начертаниях: как строчные, так и прописные. Под хранение каждого такого пароля на компьютере отводится минимально возможное и одинаковое целое количество байтов, при этом используется посимвольное кодирование и все символы кодируются одинаковым минимально возможным количеством битов. Определите объем памяти, который занимает хранение 50 паролей.

6 Выполните перевод $\mathbf{44{,}15_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **45 – 56**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{197{,}25_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{7C27A100_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Аффинная система подстановок Цезаря. Исходными данными для шифрования являются:

Исходный текст: <**СИСТЕМЫ_ХРАНЕНИЯ _ИНФОРМАЦИИ**>;

R=32; k_1=9; k_2=2;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ_>;

A_1 = <ЗСЦГЪШРЬДЫЯТФУЮБАОЛЭМЧ_ЖВКЩНХПИЕ>.

Задание:

а) зашифровать исходный текст;

б) получить таблицу замены для данных алфавитов;

в) расшифровать с помощью таблицы замены:

ЮЕНФУЖ_ГЕЕЭЕОЕГСЛСЕЭУЖ_СЮЯ__МУЛ.

Вариант 10

1 Найдите основание системы $\mathbf{231_x = 45_{10}}$.

2 Вычислите: $\mathbf{37_8 + 1100011_2 = X_{16}}$.

3 Выполните переводы: $\mathbf{5F_{16} \rightarrow X_2, X_{10}, X_8}$.

4 Студенты группы изучают один из трех языков: английский, немецкий или французский, причем 12 студентов не учат английский. Сообщение, что случайно выбранный студент Петров изучает английский, несет $\log_2 3$ бит информации, а что Иванов изучает французский – 1 бит. Сколько студентов изучают немецкий язык?

5 При регистрации в компьютерной системе, используемой при проведении командной олимпиады, каждому ученику выдается уникальный идентификатор – целое число от 1 до 500. Для хранения каждого идентификатора ученика используется одинаковое и минимально возможное количество бит. В каждой команде участвует 3 ученика. Идентификатор команды состоит из последовательно записанных идентификаторов учеников. Для записи каждого идентификатора команды система использует одинаковое и минимально возможное количество байт. Сколько байт должна отвести система для записи идентификаторов 30 команд?

6 Выполните перевод $\mathbf{27{,}27_{10} \rightarrow X_2}$.

7 Выполните вычитание путем сложения в однобайтовом формате в обратном и дополнительном кодах **37 – 54**.

8 Получить шестнадцатеричную форму внутреннего представления числа $\mathbf{-234{,}125_{10}}$ в формате с плавающей точкой с одинарной точностью.

9 По шестнадцатеричной форме внутреннего представления числа в форме с плавающей точкой $\mathbf{79CA5700_{16}}$ записать число в нормализованном виде в двоичной системе счисления.

10 Метод матричной алгебры. Зашифровать исходный текст: <**ОФИЦИАЛЬНЫЙ_ДИЛЕР**> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 8 & 3 & 5 \\ 2 & 6 & 9 \\ 7 & 4 & 1 \end{vmatrix}$$

Расшифровать, используя эту же матрицу-ключ:

145 133 136 274 272 239.

Список литературы

1 Вентцель Е. С., Овчаров Л. А. Задачи и упражнения по теории вероятностей : учебное пособие. М. : Кнорус, 2014. 496 с.
2 Гмурман В. Е. Теория вероятностей и математическая статистика : учеб. пособие для вузов. 9-е изд., стер. М. : Высш. шк., 2003. 479 с. : ил.
3 Информатика 7-9 класс. Базовый курс. Теория / под ред. Н. В. Макаровой. СПб. : Питер, 2003. 368 с. : ил.
4 Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов. 4-е изд., стереотип. Горячая линия-Телеком, 2011. 146 с.
5 Матвеев Л. А. Компьютерная поддержка решений : учебник. СПб. : Специальная литература, 1998. 472 с. : ил.
6 Никифорова Т. А. Теоретические основы информатики (часть 1) : методические рекомендации для проведения лабораторных работ. Курган : Изд-во Курганского гос. ун-та, 2009.
7 Никифорова Т.А. Теоретические основы информатики (часть 2) : методические рекомендации для проведения лабораторных работ. Курган : Изд-во Курганского гос. ун-та, 2009.
8 Новик Л. В. Обработка статистических данных с помощью электронных таблиц. URL: http://festival.1september.ru/articles/213989/ (дата обращения: 9.11.2014).
9 Поршнев С. В. Вычислительная математика: курс лекций : учебное пособие для студентов вузов. СПб : БХВ – Петербург, 2004. 304 с.
10 Сингх С. Книга шифров: тайная история шифров и их расшифровки / пер. с англ. А. Галыгина. М. : АСТ: Астрель, 2007. 447 с. : ил.
11 Тетюшева С. Г., Февралева Н. А. MICROSOFT EXCEL : методические рекомендации для проведения лабораторных работ. Курган : Изд. Курганского гос. ун-та, 2002.
12 Фаддеев М. А. Элементарная обработка результатов эксперимента : учебное пособие. СПб.; М.; Краснодар : Лань, 2008. 117 с.
13 Шауцукова Л. З. Информатика : учеб. пособие для 10-11 кл. общеобразоват. учреждений. М. : Просвещение, 2000. 416 с. : ил.
14 Шеннон Р. Имитационное моделирование систем – искусство и наука. М. : Мир, 1978.

Сидорова Оксана Аркадьевна
Томилова Елена Николаевна

ОСНОВЫ МАТЕМАТИЧЕСКОЙ ОБРАБОТКИ ИНФОРМАЦИИ

Методические рекомендации
для студентов направления подготовки 050100.62

Редактор Е. А. Могутова

Подписано в печать 26.03.15	Формат 60x84 1/16	Бумага 65 г/м^2
Печать цифровая	Усл. печ.л. 3,0	Уч.-изд. л. 3,0
Заказ 81	Тираж 25	Не для продажи

РИЦ Курганского государственного университета.
640000, г. Курган, ул. Советская, 63/4.
Курганский государственный университет.