Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный технический колледж»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по выполнению практических работ

по учебной дисциплине

«ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ»

для студентов специальности

09.02.06 Сетевое и системное администрирование

Квалификация: Сетевой и системный администратор

Челябинск, 2023

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации по выполнению практических работ по учебной дисциплине «Основы теории информации» предназначены для студентов специальности 09.02.06 Сетевое и системное администрирование, квалификация – Сетевой и системный администратор (перечень ТОП-50).

Практические занятия являются важным элементом учебной дисциплины. В процессе выполнения практических работ обучающиеся систематизируют и закрепляют полученные теоретические знания, развивают интеллектуальные и профессиональные умения, формируют элементы общих и профессиональных компетенций.

Программой учебной дисциплины «Основы теории информации» предусмотрено выполнение 17 практических работ, направленных **на формирование *элементов следующих компетенций*:**

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 9 Использовать информационные технологии в профессиональной деятельности.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

***умений*:**

– применять закон аддитивности информации;

– применять теорему Котельникова;

– использовать формулу Шеннона.

обобщение, систематизацию, углубление и закрепление *знаний*:

– виды и формы представления информации;

– методы и средства определения количества информации;

– принципы кодирования и декодирования информации;

– способы передачи цифровой информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

– методы криптографической защиты информации;

– способы генерации ключей.

Описание каждой практической работы содержит номер, название и цель работы, формируемые в процессе выполнения работы умения и элементы компетенций, изложение необходимого теоретического материала (при необходимости примеры выполнения заданий), варианты заданий, описание алгоритма выполнения работы и контрольные вопросы (с целью выявить и устранить недочеты в освоении материала).

Для получения дополнительной, более подробной информации по основным вопросам учебной дисциплины в конце методических рекомендаций приведен перечень информационных источников.

Отчеты студентов по практическим работам должны содержать номер, название и цель работы, выполненные задания и их результаты, ответы на контрольные вопросы и выводы по проделанной работе.

Титульный лист должен быть оформлен в соответствии с приложением 1.

Отчет должен быть оформлен в соответствии с приложением 2 (если практическая работа выполнялась на ПК), и с приложением 3 (если расчеты проводились в тетради).

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

№	Наименование работы	Количество часов
1.	Способы хранения обработки и передачи информации	2
2.	Измерение количества информации	2
3.	Применение теоремы Шеннона	2
4.	Применение теоремы отчетов	2
5.	Определение пропускной способности канала	2
6.	Поиск энтропии случайных величин	2
7.	Расчет вероятностей	2
8.	Энтропийное кодирование	2
9.	Составление закона распределения вероятностей	2
10.	Практическое применение различных алгоритмов сжатия. Сравнение и анализ архиваторов	2
11.	Кодирование по алгоритму Хаффмана	2
12.	Таблично-символьное кодирование	2
13.	Цифровое кодирование	2
14.	Аналоговое кодирование	2
15.	Практическое применение криптографии. Изучение и сравнительный анализ методов шифрования.	2
16.	Криптография с симметричным ключом, с открытым ключом.	2
17.	Шифрование с использованием перестановок. Шифрование с использованием замен	2
Всего часов		**34**

Практическая работа №1

Название практической работы: Способы хранения обработки и передачи информации

Цель работы: сформировать умения систематизировать и упорядочивать документы на ПК, организовывать их размещение, хранение, обработку, поиск и передачу файлов

знания (актуализация)**:**

– виды и формы представления информации;
– методы и средства определения количества информации.

умения:

– применять закон аддитивности информации.

элементы компетенций и личностных результатов:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 9 Использовать информационные технологии в профессиональной деятельности

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Информационные процессы невозможны без средств передачи и представления информации, поскольку зачастую информация требуется в месте, территориально удаленном от источника ее возникновения, и должна быть представлена в виде символов, образов и сигналов, пригодных для восприятия потребителем. Современные средства связи способны передавать информацию в любой форме: телефонные, телевизионные, телеграфные сообщения, массивы данных, печатные материалы, фотографии и т. д. В соответствии со спецификой передаваемых сообщений организуется канал передачи информации — совокупность технических средств, обеспечивающих передачу сигналов от источника к потребителю. Основная характеристика канала передачи — скорость передачи информации, а ее предельно допустимое

значение называют емкостью канала, которая ограничивается шириной полосы канала и шумом. Канал связи соединяет передатчик и приемник с помощью линии связи, которая может быть проводной, кабельной, радио, микроволновой, оптической или спутниковой. Примерами линий связи являются телефонные и вычислительные сети, сети телевизионного и радиовещания, мобильной связи, спутниковые технологии передачи данных. Основное достоинство передачи информации в цифровой форме заключается в возможности использования кодированных сигналов, обеспечения защиты информации и наилучшего способа приема. Для представления переданной или хранимой информации потребителю используются процессы воспроизведения и отображения.

Ход работы:

Перед началом работы необходимо ознакомиться с техникой безопасности при работе на компьютере и правилами поведения в компьютерном классе.

1. Включите ПК и загрузите ОС, введите свой пароль и логин.

2. Создайте портфолио группы, заранее заготовить фотографии одногруппников.

3. Создать общую папку на сервере под именем **Портфолио группы,** в которую поместите фотографии одногруппников.

4. Создать папку под именем **Практика ОТИ.**

5. Набрать в одном из текстовых редакторов текст из 10 предложений на тему «Моя профессия».

6. Вставить в набранный текст рисунок.

7. Сохранить текст в папке **Практика ОТИ\ Практика 1** под именем **Моя профессия**.

8. Создать титульный лист с общей фотографией и названием группы: специальность и номер группы.

9. Оформить лист на себя: записать данные: дата рождения, номер школы, хобби, вставить свою фотографию.

10. Сохранить данные в папку **Практика ОТИ\ Практика 1**под своей фамилией.

11. Открыть свою электронную почту.

12. Отправить, набранную информацию по электронной почте своему одногруппнику.

13. Получить информацию по электронной почте.

14. Добавить информацию одногруппника в свой документ и сохранить под фамилиями (своя и одногруппника).

15. Отправить, набранную информацию по электронной почте другому одногруппнику.

16. В результате получится файл, в котором содержится вся информация о группе. Полученный файл сохраните под именем **Моя группа**

17. Ответьте на контрольные вопросы:

– Как происходит сбор и хранение данных?

– Как происходит передача данных?

– Из каких технологических процессов состоит процесс обработки информации?

– Как осуществляется вывод данных?

18. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 2).

Практическая работа №2

Название практической работы: Измерение количества информации

Цель работы: научиться измерять информацию различными методами, использовать правила перевода информации из одних единиц измерения в другие.

знания (актуализация)**:**

– виды и формы представления информации;

– методы и средства определения количества информации.

умения:

– применять закон аддитивности информации.

элементы компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Информативность сообщения зависит от многих причин.

Существует несколько подходов к вопросу информативности сообщения: *субъективный (содержательный, объективный (алфавитный) и вероятностный.*

Содержательный подход:

Научный подход к оценке сообщений был предложен еще в 1928 году Р. Хартли.

Пусть в некотором сообщении содержатся сведения о том, что произошло одно из N равновероятных событий. Тогда количество информации, заключенное в этом сообщении, - I бит и число N связаны формулой:

$$2^I = N \quad (1)$$

где I – количество информации или информативность события (в битах);

N – число равновероятных событий (число возможных выборов).

Следовательно, *информативность события равна*

$$I = \log_2 N \qquad (2)$$

Пример №1: При угадывании целого числа в диапазоне от 1 до N было получено 8 бит информации. Чему равно N?

Решение: Для того чтобы найти число, достаточно решить уравнение $N=2^I$, где I = 8. Поскольку $2^8 = 256$, то N = 256. Следовательно, при угадывании любого целого числа в диапазоне от 1 до 256 получаем 8 бит информации.

Объективный подход:

Информация рассматривается как последовательность символов, знаков.

Количество символов в сообщении называется *длиной сообщения*. Основой любого языка является алфавит.

Алфавит – это набор знаков (символов), в котором определен их порядок.

Есть алфавит, который можно назвать достаточным. Это алфавит мощностью 256 символов. Алфавит из 256 символов используется для представления текстов в компьютере. Поскольку $256=2^8$, то один символ этого алфавита «весит» 8 бит.8 бит информации присвоили свое название – байт.

Если один символ алфавита несет 1 байт информации, то надо просто сосчитать число символов, полученное значение даст информационный объем текста в байтах.

Для вычисления объема информации V используют формулу:

$$V = K \cdot I \qquad (3)$$

где I –информационный вес одного символа и находится по формуле (1), где N – мощность алфавита (количество символов);

K – количество символов в сообщении (тексте).

Пример №2: Племя “Обезьяны” пишет письма, пользуясь 32-символьным алфавитом. Племя “Слоны” пользуется 64-символьным алфавитом. Вожди племен обменялись письмами. Письмо племени “Обезьяны” содержало 90 символов, а письмо племени “Слоны” – 80 символов. Сравните объем информации, содержащейся в письмах.

Решение: Мощность алфавита племени “Обезьяны” равна 32, информационный вес одного символа алфавита $I = \log_2 32 = 5$ бит. Количество

информации в тексте, состоящем из 90 символов, равно V= 90*5 = 450 бит = 56,25 байт.

В любой системе единиц измерения существуют основные единицы и производные от них. Для измерения больших объемов информации используются производные от байта единицы:

1 килобайт = 1 Кб = 2^{10} байт = 1024 байта; 1 мегабайт = 1 Мб = 2^{10} Кб = 1024 Кб

1 гигабайт = 1 Гб = 2^{10} Мб = 1024 Мб = 1048576 Кб = 1073741824 байт

1 Терабайт = 1024 Гбайт; 1 Петабайт = 1024 Терабайт; 1 экзабайт = 1024 Пбайт

1 зеттабайт = 1024 экзабайт; 1 йоттабайт = 1024 зеттабайт

Ход работы:

1. Выполните перевод единиц измерения информации:

а). 5 Кбайт = __ байт = __ бит;

б). __ Кбайт = __ байт = 12288 бит;

в). __ Кбайт = __ байт = 213 бит;

г). __Гбайт = 1536 Мбайт = __ Кбайт;

д). 512 Кбайт = __ байт = __ бит;

е). 4Гбайт 5Кбайт 8000 бит = ___Мбайт;

ж). 2 Кбайт 8008 бит = ___ байт;

з). 2^{33} бит = ___ Гбайт.

2. Используя содержательный подход к измерению информации, решите задачи:

а). Определите количество информации, полученное при отгадывании числа из интервала от 0 до 31;

б). Сообщение о том, что Иванов живет на 12 этаже несет 4 бита информации. Определите количество этажей в доме.

в). Шарик находится в одном из 64 ящичков. Посчитайте сообщения о том, где находится шарик;

г). Определите количество бит информации в сообщении о том, что на светофоре горит зеленый свет;

д). Определите количество информации, полученной вторым игроком при игре в крестики-нолики на поле 8х8, после первого хода первого игрока, играющего крестиками;

е). Вы бросаете два кубика с нанесенными на гранях цифрами от 1 до 6. Определите, сколько бит информации несет сообщение, что на одном кубике выпала тройка, а на другом – пятерка.

3. Используя алфавитный подход к измерению информации, решите задачи:

а). Сообщение, записанное буквами 64-х символьного алфавита, содержит 20 символов. Определите, какой объем информации оно несет. Результат перевести в байты;

б). Информационное сообщение объемом 1,5 Кбайта содержит 3072 символа. Определите количество символов, содержащихся в алфавите, при помощи которого было записано это сообщение;

в). Подсчитайте количество килобайт информации в тексте, если текст состоит из 600 символов, а мощность используемого алфавита – 128 символов;

г). Для записи текста использовался 256-символьный алфавит. Каждая страница содержит 30 строк по 70 символов в строке. Определите объем информации, содержащейся в 5 страницах текста;

д). Лазерный принтер печатает со скоростью в среднем 7 Кбит в секунду. Сколько времени понадобится для распечатки 12-ти страничного документа, если известно, что на одной странице в среднем по 45 строк, в строке 60 символов (1 символ – 1 байт). Результат округлите до целой части;

е). Имеется 2 текста на разных языках. Первый текст использует 32-символьный алфавит и содержит 200 символов, второй – 16-символьный алфавит и содержит 250 символов. Определите, какой из текстов содержит большее количество информации и на сколько бит;

ж). Определите количество символов в сообщении, записанном с помощью 16-символьного алфавита, если объем этого сообщения составил 1/16 Мб;

з). Для записи сообщения использовался 64-символьный алфавит. Каждая страница содержит 30 строк. Все сообщение содержит 8775 байтов информации и занимает 6 страниц. Определите количество символов в строке.

4. Решите задачи на измерение информации:

а). Считая, что каждый символ кодируется одним байтом, оцените информационный объем следующего предложения: «HTML – это язык гипертекстовой разметки документа»;

б). Разведчик А. Белов должен передать сообщение: «Место встречи изменить нельзя. Юстас» Пеленгатор определяет место передачи, если она

длится не менее 2 минут. С какой скоростью (бит/с) должен передавать радиограмму разведчик?

в). Сколько различных комбинаций можно построить, используя четыре двоичных разряда?

5. Решите уравнение: 16^x бит=128 Кбайта.

6. Ответьте на контрольные вопросы:

– Перечислите подходы к измерению информации;

– Запишите формулу вычисления объема информации.

7. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №3

Название практической работы: Применение теоремы Шеннона

Цель работы: научиться измерять информацию, используя вероятностный подход, применять данный метод при решении задач.

знания (актуализация)**:**

– методы и средства определения количества информации.

умения:

– использовать формулу Шеннона.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

В жизни же мы сталкиваемся не только с равновероятными событиями, но и событиями, которые имеют разную вероятность реализации.

Например:

1. Когда сообщают прогноз погоды, то сведения о том, что будет дождь, более вероятно летом, а сообщение о снеге - зимой.

2. Если на озере живет 500 уток и 100 гусей, то вероятность подстрелить на охоте утку больше, чем вероятность подстрелить гуся.

3. Если в мешке лежат 10 белых шаров и 3 черных, то вероятность достать черный шар меньше, чем вероятность вытаскивания белого.

4. Если одна из сторон кубика будет более тяжелой, то вероятность выпадения этой стороны будет меньше, чем других сторон.

Как вычислить количество информации в сообщении о таком событии?

Для этого необходимо использовать следующую формулу, предложенную в 1948 г. американским математиком и инженером Клодом Шенноном:

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

где I - количество информации;

N - количество возможных событий;

p_i - вероятность i-го события (p = K/N, K – величина, показывающая, сколько раз произошло интересующее нас событие).

Этот подход к определению количества информации называется *вероятностным*.

Для событий с равной вероятностью (p_i=1/N) количество информации рассчитывается по формуле:

$$I = -\sum_{i=1}^{N} \frac{1}{N} \log_2 \frac{1}{N} = \log_2 N \qquad (2)$$

Количественная зависимость между вероятностью события (p) и количеством информации в сообщении о нем (i) выражается формулой:

$$I = \log_2(1/p) \qquad (3)$$

Пример№1: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.

Решение:

Т.к. количество шариков различных цветов неодинаково, то вероятности зрительных сообщений о цвете вынутого из мешочка шарика также различаются и равны количеству шариков данного цвета, деленному на общее количество шариков:

$p_б$= 0,1; $p_к$= 0,2; $p_с$ = 0,3; $p_з$ = 0,4.

События неравновероятны, поэтому для определения количества информации, содержащегося в сообщении о цвете шарика воспользуемся формулой(4)

I = - (0,1·$\log_2$0,1 + 0,2·$\log_2$0,2 + 0,3·$\log_2$0,3 + 0,4·$\log_2$0,4) бит ≈ 1,85 бита

Количество информации, содержащееся в символе, которое определяется частотой его появления, равно: $\log_2$ (1/p_i), бит и определяется по формуле (1),

где p_i – вероятность (относительная частота) знака номер i данного алфавита из N знаков.

Ход работы:

1. Решите задачи, используя вероятностный подход к измерению информации:

а). В коробке 5 синих и 15 красных шариков. Определите количество информации в сообщении о том, что из коробки достали синий шарик;

б). 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. Определите количество зеленых кубиков;

в). 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?

г). В колоде содержится 32 карты. Из колоды случайным образом вытянули туза, потом его положили обратно и перетасовали колоду. После этого из колоды опять вытянули этого же туза. Какое количество бит информации в сумме содержат эти два сообщения?

д). В составе 16 вагонов, среди которых К – купейные, П – плацкартные и СВ – спальные. Сообщение о том, что ваш друг приезжает в СВ несет 3 бита информации. Определите, сколько в поезде вагонов СВ;

е). Ученики группы, состоящего из 21 человека, изучают немецкий или французский языки. Сообщение о том, что ученик А изучает немецкий язык, несет $\log_2 3$ бит информации. Сколько человек изучают французский язык?

ж). В ящике лежат перчатки (белые и черные). Среди них – две пары черных. Сообщение о том, что из ящика достали пару черных перчаток, несет 4 бита информации. Сколько пар былых перчаток было в ящике?

з). В корзине лежат белые и черные шары. Среди них 18 черных шаров. Сообщение о том, что из корзины достали белый шар, несет 2 бита информации. Определите количество шаров в корзине;

и). В ведерке у рыбака караси и щуки. Щук в ведерке 3. Зрительное сообщение о том, что из ведра достали карася, несет 1 бит информации. Сколько всего рыб поймал рыбак?

к). На автобусной остановке останавливаются два маршрута автобусов: № 5 и № 7. Ученику дано задание: определить, сколько информации содержит сообщение о том, что к остановке подошел автобус № 5, и сколько информации в сообщении о том, что подошел автобус № 7. Ученик провел исследование. В течение всего рабочего дня он подсчитал, что к остановке автобусы подходили 100 раз. Из них — 25 раз подходил автобус № 5 и 75 раз подходил автобус № 7. Сделав предположение, что с такой же частотой автобусы ходят и в другие дни, ученик вычислил вероятность появления на остановке автобуса № 5: p5= …, и вероятность появления автобуса № 7: p7 = ...

л). В ящике лежат 36 красных и несколько зеленых яблок. Сообщение «Из ящика достали зеленое яблоко» несет 2 бита информации. Сколько яблок в ящике?

м). В концертном зале 270 девушек и несколько юношей. Сообщение «Первым из зала выйдет юноша» содержит 4 бита информации. Сколько юношей в зале.

2. Ответьте на контрольные вопросы:

– Приведите примеры событий с разной вероятностью реализации;

– Как вычислить количество информации в сообщении о таких событиях?

3. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №4

Название практической работы: Применение теоремы отчетов

Цель работы: научиться синтезировать сигналы по дискретным отсчетам в соответствии с теоремой Котельникова.

знания (актуализация)**:**

– методы и средства определения количества информации;

– способы передачи цифровой информации.

умения:

– применять теорему Котельникова.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Переход от аналогового сигнала к дискретному для реализации ЦОС осуществляется операцией дискретизации. *Временная дискретизация*– представление непрерывного сигнала $x(t)$ в виде последовательности выборок отдельных значений сигнала, взятых в дискретные моменты времени. Если интервалы T между соседними выборками одинаковы, дискретизацию называют *равномерной*.

При этом д*искретные сигналы* описываются решетчатыми функциями вида

$$x(nT) = \sum_{n=-\infty}^{\infty} x(t)\delta(nT - t). \qquad (1)$$

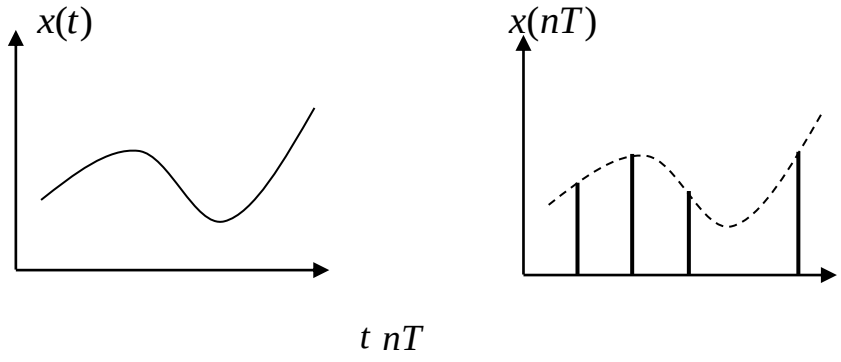


Рисунок 1.

Чем меньше шаг дискретизации, тем ближе дискретный процесс к непрерывному, т.е. при $T \to 0$ $x(nT) \to x(t)$.

Особое внимание при переходе от аналоговых сигналов к дискретным следует уделить тому, чтоб не потерять их некоторые параметры, т.е. сохранить их информативность.

Одним из фундаментальных положений теоретической радиотехники, устанавливающим возможность сколь угодно точного восстановления мгновенных значений сигнала с ограниченным спектром исходя из отсчетных значений, взятых через равные промежутки времени, является теорема Котельникова.

Согласно теореме Котельникова (1933г.), если спектральная плотность $X(\omega)$ сигнала $x(t)$ финитна, т.е. существует такое значение $\omega = \omega_в$, что $|X(\omega)| = 0$ при $\omega > \omega_в$, то такой сигнал можно точно восстановить (интерполировать) по его значениям (отсчетам), взятым в моменты $t_n = n\Delta t$, где $n =$ ..., -2, -1, 0, 1, 2,..., а $\Delta t = \pi / \omega_в = 1/2 f_в$:

$$x(t) = \sum_{n=-\infty}^{\infty} x(n\Delta t)\frac{\sin\omega_в(t - n\Delta t)}{\omega_в(t - n\Delta t)} \qquad (2)$$

.

Для восстановления аналогового сигнала по его дискретным значениям используется восстанавливающий фильтр. При использовании фильтра, построенного методом прямоугольного весового окна в результате резкого обрезания краев его ИХ возникают пульсации Гиббса. Для увеличения качества восстановления аналогового сигнала применяют весовое взвешивание ИХ

фильтра. Среди наиболее широко известных весовых функций различают следующие:

- Прямоугольную $w_k = 1,\ 0 \le k \le N-1$;
- Хэмминг $w_k = 0.54 - 0.46\cos\frac{2\pi k}{N-1}$;
- Ханна $w_k = \frac{1}{2}\left(-\cos\left(\frac{2\pi k}{N-1}\right)+1\right)$;
- Блэкмана $w_k = 0.42 - 0.5\cos\left(\frac{2\pi k}{N-1}\right)$

Пример 1

Пусть на вход аналогово-цифрового преобразователя поступает гармонический сигнал с частотой f (период $T = 1/f$).частоты исходного сигнала

Проведем дискретизацию входного аналогового сигнала с периодом дискретизации $T_д$ меньшим половины периода входного сигнала T (рисунок 2).

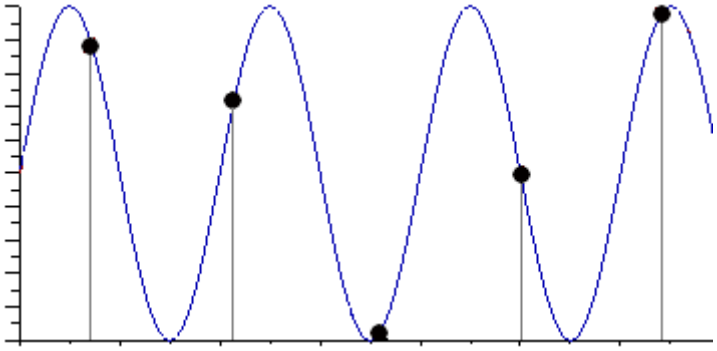


Рисунок 2

Очевидно, что дискретные отсчеты сигнала однозначно не отображают форму исходного сигнала, в частности по получившимся точкам можно построить гармонический сигнал с периодом $T_{искаж.}$, отличающимся от периода исходного сигнала T. Период $T_{искаж}$ больше периода исходного сигнала T, соответственно частота меньше, частоты исходного сигнала f (рисунок 3).

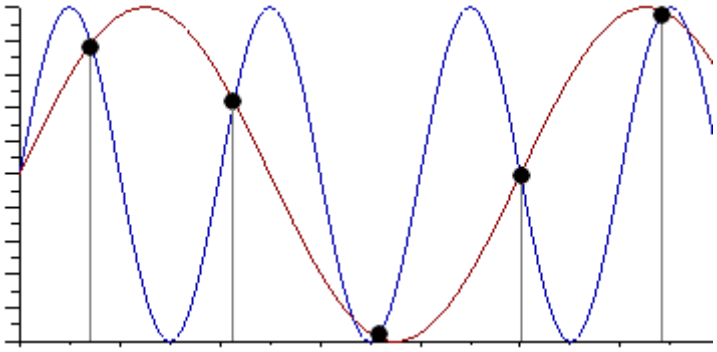


Рисунок 3

Данный эффект называется стробоскопическим эффектом или алиасингом. Он заключается в появлении ложной низкочастотной составляющей при дискретизации сигнала с частотой меньшей удвоенной частоты исходного сигнала (или с периодом большим половины периода исходного сигнала), отсутствующей в исходном сигнале.

Пример 2

Уменьшим период дискретизации до половины периода исходного аналогового сигнала (частоту дискретизации увеличим до удвоенной частоты исходного сигнала). В данной ситуации возникает неопределенность начальной фазы и амплитуды сигнала, при этом частота исходного сигнала не искажается. В крайнем случае мы можем получить отсчеты сигнала равные нулю (рисунок 3).

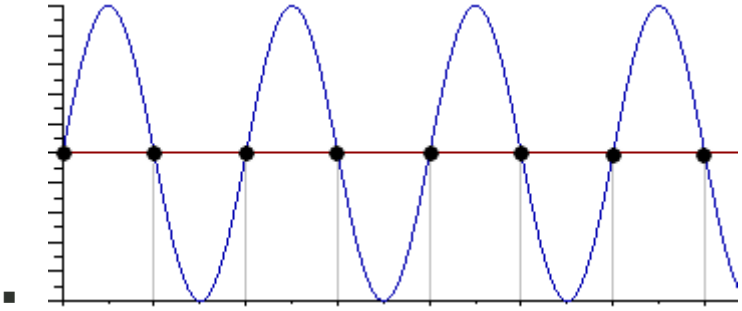


Рисунок 4

Пример 3

Продолжим уменьшение периода дискретизации. Если период дискретизации меньше половины периода исходного сигнала, то очевидно, что через получившиеся после оцифровки точки можно построить только один гармонический сигнал, соответствующий исходному, без искажения начальной фазы, амплитуды и частоты (рисунок 5). Данное утверждение теоретически обосновано, и мы его примем без доказательства.

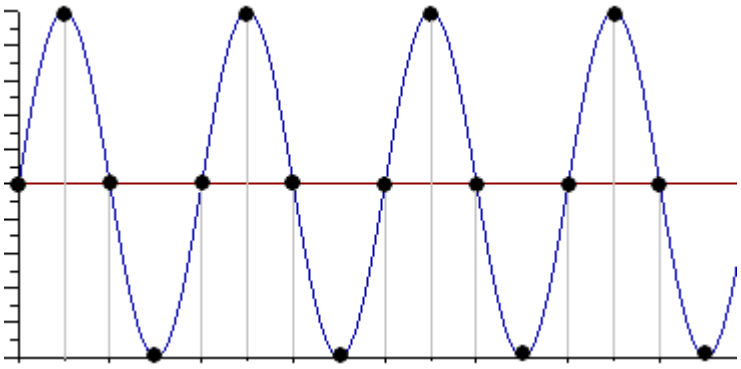


Рисунок 5

Таким образом, для адекватного восстановления гармонического сигнала по дискретным отсчетам, частота дискретизации должна быть не меньше

половины частоты сигнала. Частота равная половине частоты дискретизации называется частотой Найквиста $f_N = f_Д/2$.

Данное утверждение можно обобщить следующим образом:

Аналоговый сигнал с ограниченным спектром может быть восстановлен однозначно и без искажений по своим дискретным отсчетам, взятым с частотой большей удвоенной максимальной частоты в своем спектре.

$$fд > 2 \cdot F_{max} \quad \textbf{(1)}$$

Данное утверждение известно как **теорема Котельникова** (в западной литературе **теорема Найквиста-Шеннона**) или теорема отсчетов. В различных источниках в формулировке данной теоремы могут быть различия, основным из которых является знак сравнения в формуле 1: $fд \geq 2 \cdot F_{max}$ или $fд > 2 \cdot F_{max}$. Мы придерживаемся формулировки со знаком **строго больше,** так как при частоте оцифровки равной максимальной частоте в спектре возникают неоднозначности начальной фазы и амплитуды.

На практике аналоговый сигнал, как правило, оцифровывают с частотой в несколько раз превышающей удвоенную частоту в спектре сигнала, хотя существуют методики оцифровки сигнала с нарушением теоремы отсчетов.

Ход работы:

1. В табличном процессоре изобразите графики сигналов:

а) синусоидальный сигнал частотой 5кГц;

б) видеоимпульсы прямоугольной формы длительностью 0,25; 0,5; 1,0 мс;

в) видеоимпульсы пилообразной формы длительностью 0,5 мс; 1,0 мс.

2. Рассчитайте и постройте идеальные выборочные сигналы для сигналов, при $f_{выб}$=5, 10, 20, 40 кГц.

3. Ответьте на контрольные вопросы:

– Сформулируйте теорему Котельникова для сигналов с ограниченным спектром.

– Объясните погрешности синтезирования реальных сигналов по дискретным отсчетам.

4. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №5

Название практической работы: Определение пропускной способности канала

Цель работы: научиться рассчитывать информационные характеристики каналов передачи данных.

знания (актуализация)**:**

– способы передачи цифровой информации;

– методы и средства определения количества информации.

умения:

– применять теорему Котельникова.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Пусть сигнал $y(t)$ на выходе канала представляет собой сумму полезного сигнала $x(t)$ и шума $n(t)$, т.е. $y(t) = x(t) + n(t)$, причем $x(t)$ и $n(t)$ статистически независимы. Допустим, что канал имеет ограниченную полосу пропускания шириной $\Delta F_{ИК}$. Тогда в соответствии с теоремой Котельникова (см. п. 1.5) функции $y(t)$, $x(t)$ и $n(t)$ можно представить совокупностями отсчетов y_i, x_i, и n_i, $i = 1,2,\ldots,L$, где $L = 2\Delta F_{ИК} T$. При этом статистические свойства сигнала $x(t)$ можно описать многомерной ПРВ $w(x_1, x_2, \ldots, x_L) = w(x)$, а свойства шума – ПРВ $w(n_1, n_2, \ldots, n_L) = w(n)$.

Пропускная способность непрерывного канала определяется следующим образом:

$$C = \lim_{T \to \infty} \frac{1}{T} \max_{w(x)} I(X,Y), \quad (1)$$

где $I(X,Y)$ – количество информации о какой-либо реализации сигнала $x(t)$ длительности T, которое в среднем содержит реализация сигнала $y(t)$ той же длительности T, а максимум ищется по всем возможным распределениям $w(x)$.

Ход работы:

1. Решите задачи:

1. Число символов алфавита m = 4. Вероятности появления символов равны соответственнор1 = 0,15; p2 = 0,4; p3 = 0,25; p4 = 0,2. Длительности символов t1 = 3c; t2 = 2c; t3 = 5c, t4 = 6c. Чему равна скорость передачи сообщений, составленных из таких символов?

2. Сообщения составлены из пяти качественных признаков (m = 5). Длительность элементарной посылки t= 20мс. Определить, чему равна скорость передачи сигналов и информации.

3. Определить пропускную способность бинарного канала связи, способного передавать 100 символов 0 или 1 в единицу времени, причем каждый из символов искажается (заменяется противоположным) с вероятностью p = 0,01.

2. Решите задачи:

1. Через ADSL-соединение файл размером 0,25 Мбайт передавался 8 секунд. Сколько секунд потребуется для передачи файла размером 800 Кбайт?

2. Модем передаёт данные со скоростью 1Мбит/сек. Передача текстового файла заняла 30 секунд. Определите, сколько страниц содержал переданный текст, если известно, что он был представлен в кодировке Unicode, а на одной странице – 3072 символа?

3. Какое количество байтов будет передаваться за 1 секунду. По каналу с пропускной способностью 100 Кбит/с?

4. Пропускная способность канала связи 1 Мбит/с. Канал не подвержен воздействию шума (например, оптоволоконная линия). Определите, за какое время будет передан файл объемом 2 Мбайт.

5. Пропускная способность канала связи 1 Мбит/с. Канал подвержен воздействию шума, поэтому избыточность кода передачи составляет 20%. Определите, за какое время будет передан файл объемом 2 Мбайт.

6. Документ объемом 5 Мбайт можно передать с одного компьютера на другой двумя способами:

а) Сжать архиватором, передать архив по каналу связи, распаковать.

б) Передать по каналу связи без использования архиватора.

7. Какой способ быстрее и насколько, если средняя скорость передачи данных по каналу связи составляет 222 бит в секунду, объем сжатого архиватором документа равен 20% от исходного, время, требуемое на сжатие документа— 8 секунд, на распаковку– 2 секунды?

В ответе напишите букву А, если способ А быстрее, или Б, если быстрее способ Б. Сразу после буквы напишите количество секунд, насколько один способ быстрее другого. Так, например, если способ Б быстрее способа А на 23 секунды, в ответе нужно написать Б23. Слов «секунд», «сек.», «с.» к ответу добавлять не нужно.

8. Документ (без упаковки) можно передать по каналу связи с одного компьютера на другой за 40 сек. Если предварительно упаковать документ архиватором, передать упакованный документ, а потом распаковать на компьютере получателя, то общее время передачи (включая упаковку и распаковку) составит 20 сек. Размер упакованного документа составляет 20% размера исходного документа. Сколько всего времени (в секундах) ушло на упаковку и распаковку данных? Слов «секунд», «сек.», «с.» к ответу добавлять не нужно.

9. По каналу связи передается последовательность символов "0" и "1" равной длительности 0=0,71 мс. Вероятности появления символов равны p(0)=0,1; p(1)=0,9. Определить скорость передачи информации и пропускную способность канала связи.

3. Ответьте на контрольные вопросы:

– Что такое пропускная способность канала передачи информации? Чем отличается пропускная способность от скорости передачи информации по каналу связи?

– Чем отличается информационная скорость передачи от технической, и в каких единицах эти скорости измеряются?

– Как изменяется пропускная способность дискретного канала связи при воздействии на канал помех.

– Какие параметры влияют на объем сигнала.

– От чего зависит пропускная способность непрерывного канала связи.

4. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №6

Название практической работы: Поиск энтропии случайных величин

Цель работы: научиться вычислять энтропию случайной величины.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;
– методы и средства определения количества информации.

умения:

– применять закон аддитивности информации.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Энтропия в теории информации — мера хаотичности информации, неопределённость появления какого-либо символа первичного алфавита. При отсутствии информационных потерь численно равна количеству информации на символ передаваемого сообщения.

Так, возьмём, например, последовательность символов, составляющих какое-либо предложение на русском языке. Каждый символ появляется с разной частотой, следовательно, неопределённость появления для некоторых символов больше, чем для других. Если же учесть, что некоторые сочетания символов встречаются очень редко, то неопределённость ещё более уменьшается (в этом случае говорят об энтропии n-ого порядка). Концепции информации и энтропии имеют глубокие связи друг с другом, но, несмотря на это, разработка теорий в статистической механике и теории информации заняла много лет, чтобы сделать их соответствующими друг другу.

Энтропия независимых случайных событий *x* с *n* возможными состояниями (от 1 до *n*) рассчитывается по формуле:

$$H(x) = -\sum_{i=1}^{n} p(i) \log_2 p(i) \tag{1}$$

Эта величина также называется *средней энтропией сообщения*. Величина $\log_2 \frac{1}{p(i)}$ называется *частной энтропией,* характеризующей только i-е состояние.

Таким образом, энтропия события *x* является суммой с противоположным знаком всех произведений относительных частот появления события *i*, умноженных на их же двоичные логарифмы (основание 2 выбрано только для удобства работы с информацией, представленной в двоичной форме). Это определение для дискретных случайных событий можно расширить для функции распределения вероятностей.

Шеннон вывел это определение энтропии из следующих предположений:

- мера должна быть непрерывной; т.е. изменение значения величины вероятности на малую величину должно вызывать малое результирующее изменение энтропии;
- в случае, когда все варианты (буквы в приведенном примере) равновероятны, увеличение количества вариантов (букв) должно всегда увеличивать полную энтропию;
- должна быть возможность сделать выбор (в нашем примере букв) в два шага, в которых энтропия конечного результата должна будет является суммой энтропий промежуточных результатов.

Шеннон показал, что любое определение энтропии, удовлетворяющее этим предположениям, должно быть в форме:

$$-K \sum_{i=1}^{n} p(i) \log_2 p(i) \tag{1}$$

где *K* — константа (и в действительности нужна только для выбора единиц измерения).

Шеннон определил, что измерение энтропии ($H = -p_1 \log_2 p_1 - \ldots - p_n \log_2 p_n$), применяемое к источнику информации, может определить требования к минимальной пропускной способности канала, требуемой для надежной передачи информации в виде закодированных двоичных чисел. Для вывода формулы Шеннона необходимо вычислить математическое

ожидание«количества информации», содержащегося в цифре из источника информации. Мера энтропии Шеннона выражает неуверенность реализации случайной переменной. Таким образом, энтропия является разницей между информацией, содержащейся в сообщении, и той частью информации, которая точно известна (или хорошо предсказуема) в сообщении. Примером этого является избыточность языка — имеются явные статистические закономерности в появлении букв, пар последовательных букв, троек и т.д.

В общем случае b-арная энтропия (где b равно 2,3,...) источника $\mathcal{S} = (S,P)$ с исходным алфавитом $S= \{a_1, \ldots, a_n\}$ и дискретным распределением вероятности $P= \{p_1, \ldots, p_n\}$ где p_i является вероятностью $a_i (p_i=p(a_i))$ определяется формулой:

$$H_b(\mathcal{S}) = -\sum_{i=1}^{n} p_i \log_b p_i \qquad (2)$$

Избыточность показывает, какая доля максимально возможной при заданном объеме алфавита неопределенности не используется источником.

$$\mu = (H_{max} - H_u)/H_{max}, \qquad (3)$$

где H_u – энтропия рассматриваемого источника, H_{max} – максимально возможное значение его энтропии, которое может быть достигнуто подбором распределения и ликвидацией взаимозависимости элементов алфавита. Так, для дискретного источника с M элементами

$$H_{max} = \log_2 M \qquad (4)$$

Пример:

Измерительное устройство вырабатывает временные интервалы, распределенные случайным образом в пределах от 100 до 500 мс. Как изменится энтропия случайной величины при изменении точности измерения с 1 мс до 1 мкс?

Решение.

При точности 1мс дискретная случайная величина X – результат измерения – может равновероятно принимать одно из $n = \frac{500-100}{1} = 400$ значений. Энтропия равна $H_1(x) = \log_2 n$.

При точности 1мкс дискретная случайная величина X – результат измерения – может равновероятно принимать одно из $m = \frac{500-100}{10^{-3}} = 400 \cdot 10^3 = 1000n$ значений. Энтропия равна $H_2(x) = \log_2 m$.

Изменение энтропии

$\Delta H(x) = H_2(x) - H_1(x) = \log_2 m - \log_2 n = \log_2 1000n - \log_2 n = \log_2 1000 \approx \log_2 1024 = 10$ бит.

Энтропия увеличилась примерно на 10 бит.

Ход работы:

1. Решите задачи:

1. Найдите энтропию для числа белых шаров при извлечении двух шаров из урны, содержащей два белых и один черный шар.

2. Найдите энтропию для числа козырных карт при извлечении двух карт из колоды в 36 карт.

3. Какую степень неопределенности содержит опыт угадывания суммы очков на извлеченной кости из полного набора домино?

4. Найдите энтропию для числа тузов при извлечении трех карт из карт с картинками.

5. Найдите дифференциальную энтропию для равномерного распределения.

6. Найдите дифференциальную энтропию для показательного закона распределения, если известно, что случайная величина *x* принимает значение меньше единицы с вероятностью 0,5.

2. Ответьте на контрольные вопросы:

–Как определяется энтропия дискретных случайных величин?

–Приведите примеры энтропий для классических законов распределения.

3. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №7

Название практической работы: Расчет вероятностей

Цель работы: научиться решать задачи с элементами теории вероятности.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;
– методы и средства определения количества информации.

умения:

– применять закон аддитивности информации.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Для количественного сравнения событий по степени возможности их появления вводится числовая мера, которая называется вероятностью события. Вероятностью случайного события называется число, являющееся выражением меры объективной возможности появления события.

Величины, определяющие, насколько значительны объективные основания рассчитывать на появление события, характеризуются вероятностью события. Необходимо подчеркнуть, что вероятность есть объективная величина, существующая независимо от познающего и обусловленная всей совокупностью условий, которые способствуют появлению события.

Объяснения, которые мы дали понятию вероятности, не являются математическим определением, так как они не определяют это понятие количественно. Существует несколько определений вероятности случайного

события, которые широко применяются при решении конкретных задач (классическое, аксиоматическое, статистическое и т. д.).

Классическое определение вероятности события сводит это понятие к более элементарному понятию равновозможных событий, которое уже не подлежит определению и предполагается интуитивно ясным. Например, если игральная кость - однородный куб, то выпадения любой из граней этого куба будут равновозможными событиями.

Пусть достоверное событие распадается на nравновозможных случаев, сумма которых дает событие. То есть случаи изn, на которые распадается, называются благоприятствующими для события, так как появление одного из них обеспечивает наступление события.

Вероятность события будем обозначать символом Р.

Вероятность события равна отношению числа случаев, благоприятствующих ему, из общего числа единственно возможных, равновозможных и несовместных случаев к числу.

Это есть классическое определение вероятности. Таким образом, для нахождения вероятности события необходимо, рассмотрев различные исходы испытания, найти совокупность единственно возможных, равновозможных и несовместных случаев, подсчитать общее их число n, число случаев m, благоприятствующих данному событию, и затем выполнить расчет по вышеприведенной формуле.

Вероятность события, равная отношению числа благоприятных событию исходов опыта к общему числу исходов опыта называется классической вероятностью случайного события.

Из определения вытекают следующие свойства вероятности:

Свойство 1. Вероятность достоверного события равна единице.

Свойство 2. Вероятность невозможного события равна нулю.

Свойство 3. Вероятность случайного события есть положительное число, заключенное между нулем и единицей.

Свойство 4. Вероятность наступления событий, образующих полную группу, равна единице.

Свойство 5. Вероятность наступления противоположного события определяется так же, как и вероятность наступления события А.

- число случаев, благоприятствующих появлению противоположного события. Отсюда вероятность наступления противоположного события равна разнице между единицей и вероятностью наступления события А:

Ход работы:

1. Применяя формулы для вычисления вероятности, решите задачи:

а). Событие В является частным случаем события *А*. Чему равны их сумма и произведение?

б). Пусть *A*, *B*, *C* – случайные события. Выяснить смысл равенств:

а) $A \cap B \cap C = A$;

б) $A \cup B \cup C = A$.

в). Пусть *A*, *B*, *C* – три произвольных события. Найти выражения для событий, состоящих в том, что из *A*, *B*, *C*:

а) Произошло только *A*;

б) Произошли *A* и *B*, но *C* не произошло;

в) Все три события произошли;

г) Произошло по крайней мере одно из этих событий;

д) Произошли по крайней мере два события;

е) Произошло одно и только одно событие;

ж) Произошло два и только два события;

з) Ни одно событие не произошло.

г).В урне имеется 10 шаров: 3 белых и 7 черных. Из урны наугад вынимают один шар. Какова вероятность того, что этот шар: а) белый; б) черный?

д). Из слова «НАУГАД» наугад выбирается одна буква. Какова вероятность того, что эта буква *А*? Какова вероятность того, что это гласная буква?

е). Монета бросается два раза. Найти вероятности событий:

1. *A* = {герб выпадет один раз};
2. *B* = {герб выпадет хотя бы один раз};
3. *C* = {герб не выпадет ни разу}.

ж). Бросаются две монеты. Какое из событий является более вероятным:

1. *A* = {монеты лягут одинаковыми сторонами};
2. *B* = {монеты лягут разными сторонами}?

з). Бросаются одновременно две игральные кости. Найти вероятности событий:

1. *A* = {произведение выпавших очков равно 8};
2. *B* = {сумма выпавших очков равна 8};
3. *C* = {произведение выпавших очков четно};
4. *Д* = {сумма выпавших очков четна};

5. E = {на обеих костях выпадет четное число очков};

и). Брошены три монеты. Найти вероятность того, что выпадут два 2 «герба».

к). При стрельбе была получена относительная частота (частость) попадания 0,6. Сколько было сделано выстрелов, если получено 12промахов?

л). При наборе телефонного номера абонент забыл две последние цифры и набрал их наудачу, помня только, что эти цифры нечетные и разные. Найти вероятность того, что номер набран правильно.

м). Из пяти карточек с буквами *А*, *Б*, *В*, *Г*, *Д* наугад одна задругой выбираются три и располагаются в ряд в порядке появления. Какова вероятность того, что получится слово «ДВА»?

н). В урне 3 белых и 7 черных шаров. Какова вероятность того, что вынутые наугад два шара окажутся черными? Одного цвета? Разных цветов?

2. Ответьте на контрольные вопросы:

– Чему равна вероятность происшедшего события?

– Перечислите свойства вероятности.

3. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №8

Название практической работы: Энтропийное кодирование

Цель работы: научиться решать задачи с элементами теории вероятности.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;

– методы и средства определения количества информации.

умения:

– применять закон аддитивности информации.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Энтропийное кодирование— кодирование последовательности значений с возможностью однозначного восстановления с целью уменьшения объёма информации (длины последовательности) с помощью усреднения вероятностей появления элементов последовательности.

Энтропия алфавита – это количество информации, приходящееся на один символ. Или информационная нагрузка, которую несет один символ алфавита. Установлено, что энтропия достигает максимума, когда все состояния источника равновероятны. Следовательно, символы равновероятного алфавита несут максимальную информационную нагрузку

$$H_{max} = \log_2 N, \quad (1)$$

где N – объем алфавита.

Избыточностью алфавита называется уменьшение информационной нагрузки на один символ вследствие неравновероятности и взаимозависимости

появления его символов. Информационная избыточность, характеризующая относительную недогруженность алфавита является безразмерной величиной (часто ее выражают в процентах) и рассчитывается так:

$$D = (H_{max} - H) / H_{max} \times 100\% \quad (2)$$

Очевидно, D = 0 когда $H = H_{max}$

Это соответствует случаю равновероятного алфавита. Предполагается, что до кодирования отдельные элементы последовательности имеют различную вероятность появления. После кодирования в результирующей последовательности вероятности появления отдельных символов практически одинаковы (энтропия на символ максимальна).

Различают несколько вариантов кодов:

– Сопоставление каждому элементу исходной последовательности различного числа элементов результирующей последовательности. Чем больше вероятность появления исходного элемента, тем короче соответствующая результирующая последовательность. Примером могут служить код Шеннона — Фано, код Хаффмана,

– Сопоставление нескольким элементам исходной последовательности фиксированного числа элементов конечной последовательности. Примером является код Танстола.

– Другие структурные коды, основанные на операциях с последовательностью символов. Примером является кодирование длин серий.

– Если приблизительные характеристики энтропии потока данных предварительно известны, может быть полезен более простой статический код, такой как унарное кодирование, гамма-код Элиаса, кодирование Фибоначчи, кодирование Голомба или кодирование Райса.

Согласно теореме Шеннона, существует предел сжатия без потерь, зависящий от энтропии источника. Чем более предсказуема получаемая информация, тем лучше её можно сжать. Случайная последовательность сжатию без потерь не поддаётся.

Ход работы:

1. Дана кодовая таблица азбуки Морзе

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

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

— — — — — • — • • — — — — — • • — • — • — • — — —

2. Закодируйте с помощью азбуки Морзе слова **СТЕНОГРАФИЯ, ШИФРОВАНИЕ, КОДИРОВАНИЕ.**

3. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ КОДИРОВАТЬ ИНФОРМАЦИЮ”. Зашифрованный текст должен быть записан без пропусков.

4. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ!

Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

5. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения закодированы с помощью этой таблицы?

16	55	54	10	69	09	61	89	29	90	49	44	10	08	02	73	21	32	83	54	74
41	55	77	10	23	68	08	20	66	90	76	44	21	61	90	55	21	61	83	54	42
57	30	27	10	91	68	32	20	80	02	49	45	40	32	46	55	40	08	83	27	17

6. Используя таблицу вероятности появления букв в русском тексте, посчитайте объем данного ниже сообщения:

Частота появления букв в русском тексте							
Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
пробел	0,175	о	0,090	е (ё)	0,072	а	0,062
и	0,062	т	0,053	н	0,053	с	0,045
р	0,040	в	0,038	л	0,035	к	0,028
м	0,026	д	0,025	п	0,023	у	0,021
я	0,018	ы	0,016	з	0,016	ь (ъ)	0,014
б	0,014	г	0,013	ч	0,012	й	0,010
х	0,009	ж	0,007	ю	0,006	ш	0,006
ц	0,004	щ	0,003	э	0,003	ф	0,002

Челябинск расположен на восточном склоне Уральских гор, южнее Екатеринбурга. Город находится на границе Урала и Сибири.

Стоит на реке Миасс, территорию города омывают Шершнёвское водохранилище и три озера: Смолино, Синеглазово, Первое. Рельеф города слабо холмистый на западе с постепенным понижением к востоку. Климат континентальный.

Рассчитать энтропию и избыточность алфавита

7. Возьмите произвольный текст на английском языке (3-4 страницы) и составьте частотный словарь английского языка. Определите, какое количество информации несет каждая буква этого словаря.

Рассчитать энтропию и избыточность алфавита.

8. Ответьте на контрольные вопросы:

– Что такое энтропийное кодирование?

– Дайте понятия избыточности алфавита.

9. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №9

Название практической работы: Составление закона распределения вероятностей

Цель работы: научиться решать задачи с элементами теории вероятности.

знания (актуализация)**:**

– виды и формы представления информации;

– методы и средства определения количества информации;

умения:

– использовать формулу Шеннона.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Случайная величина – величина, численное значение которой может меняться в зависимости от результата стохастического эксперимента.

Дискретной назовём случайную величину, возможные значения которой образуют конечное множество.

Законом распределения дискретной случайной величины называется правило, по которому каждому возможному значению x_i ставится в соответствие вероятность p_i, с которой случайная величина может принять это значение, причём $\sum_{i=1}^{n} p_i = 1$.

Пример. Абитуриент сдаёт два вступительных экзамена: по математике и физике. Составить закон распределения случайной величины x, числа

полученных пятёрок, если вероятность получения пятёрки по математике равна 0,8, а по физике – 0,6.

Решение. Обозначим A_1и A_2 – события, заключающиеся в том, что и математика, и физика сданы на 5. Очевидно, возможные значения x есть 0, 1, 2, причём

$$p(x=0)=p(\overline{A_1}*\overline{A_2})=p(\overline{A_1})*p(\overline{A_2})=0.2*0.4=0.08;$$
$$p(x=1)=p(A_1*\overline{A_2}+\overline{A_1}*A_2)=0.8*0.4+0.2*0.6=0.44;$$
$$p(x=2)=p(A_1*A_2)=p(A_1)*p(A_2)=0.8*0.6=0.48$$

Полученные результаты сведём в таблицу:

x_i	0	1	2
p_i	0.08	0.44	0.48

$$\sum_{i=1}^{n} p_i = 0{,}08+0{,}44+0{,}48=1.$$

Ход работы:

1. Решите задачи:

а) В ящике 10 красных и 6 синих пуговиц. Вынимаются на удачу две пуговицы. Какова вероятность того, что пуговицы будут одноцветными?

б) Найти вероятность того, что наудачу взятое двузначное число окажется кратным 2, либо 5, либо тому и другому одновременно.

в) Студент знает 10 вопросов из 30 программы. Определить вероятность того, что из трех предложенных ему преподавателем вопросов студент знает:

а) Все три вопроса;

б) Хотя бы один вопрос.

г) Студент пришел на зачет, зная из 30 вопросов только 24. Какова вероятность сдать зачет, если после отказа отвечать на вопрос преподаватель задает еще только один вопрос?

д) В круг радиуса *R* вписан квадрат. Чему равна вероятность того, что поставленные наудачу внутри круга две точки окажутся внутри квадрата?

е) Среди 25 экзаменационных билетов 5 «хороших». Два студента по очереди берут по одному билету. Найти вероятности следующих событий:

1. *A* ={первый студент взял хороший билет};

2. *B* ={второй студент взял хороший билет};

3. *C*= {оба студента взяли хорошие билеты}.

ж) Монета подбрасывается три раза подряд. Под исходом опыта будем понимать последовательность (*X*1, *X*2, *X*3), где каждый из *Xi* обозначает выпадение «герба» (Г) или цифры (Ц).

Необходимо:

– Построить пространство W элементарных событий;

– Описать событие *A*, состоящее в том, что выпало не менее двух«гербов».

з) Рабочий обслуживает 3 станка, вероятности выхода из строя каждого из которых в течение часа соответственно равны 0,2; 0,15; 0,1. Составить закон распределения числа станков, не требующих ремонта в течение часа. Найти математическое ожидание и дисперсию этой случайной величины

и) Вероятность безотказной работы в течение гарантийного срока для телевизоров первого типа равна 0,9, второго типа – 0,7, третьего типа – 0,8. Случайная величина X – число телевизоров, проработавших гарантийный срок, среди трех телевизоров разных типов.

к) Производятся три выстрела по мишени. Вероятность поражения мишени первым стрелком равна 0,4, вторым – 0,5, третьим – 0,6. Случайная величина X – число поражений мишени.

2. Найдите числовые характеристики дискретной случайной величины:

а) Стрелок производит четыре выстрела по мишени. Вероятность попадания в мишень при каждом выстреле равна 0,4. За каждое попадание стрелку насчитывается 5 очков.

б) а) Построить ряд распределения числа полученных очков (случайная величина X) по биномиальному закону. Проверить условие нормировки.

б) Построить многоугольник распределения.

в) в) Определить математическое ожидание, дисперсию и среднее квадратичное отклонение случайной величины X. Сделать выводы.

г) г) Записать функцию распределения случайной величины X, построить график функции.

д) Найти вероятности того, что стрелок получит:

- менее 10 очков;
- от 5 до 15 очков;
- более 10 очков.

д) В связке из 3 ключей только один ключ подходит к двери. Ключи перебирают до тех пор, пока не отыщется подходящий ключ. Построить закон распределения для случайной величины x – числа опробованных ключей.

3. Ответьте на контрольные вопросы:

– Что такое случайная величина?

– Закон распределения дискретной случайной величины.

4.Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №10

Название практической работы: Практическое применение различных алгоритмов сжатия. Сравнение и анализ архиваторов

Цель работы: научиться работать с архиваторами и освоить алгоритм сжатия информации.

знания (актуализация)**:**

– способы передачи цифровой информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

умения:

– применять закон аддитивности информации.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 9 Использовать информационные технологии в профессиональной деятельности.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Характерной особенностью большинства типов данных, с которыми традиционно работают пользователи, является определенная избыточность. Степень избыточности зависит от типа данных.

При обработке информации избыточность также играет важную роль. Так, например, при преобразовании или селекции информации избыточность используют для повышения ее качества (репрезентативности, актуальности, адекватности и т.п.). Однако, когда речь заходит не об обработке, а о хранении

готовых документов или их передаче, то избыточность можно уменьшить, что дает эффект сжатия данных.

Если методы сжатия информации применяют к готовым документам, то нередко термин *сжатие данных* подменяют термином *архивация данных,* а программные средства, выполняющие эти операции, называют *архиваторами.*

Степень сжатия файлов характеризуется коэффициентом K_c, определяемым как отношение объема сжатого файла V_c к объему исходного файла V, выраженное в процентах: $K_o=(V_c/V*100)$. Степень сжатия зависит от используемой программы, метода сжатия и типа исходного файла. Наиболее хорошо сжимаются файлы графических образов, текстовые файлы и файлы данных, для которых степень сжатия может достигать 5-40%, меньше сжимаются файлы исполняемых программ и загрузочных модулей –60-90%. Почти не сжимаются архивные файлы.

Ход работы:

1. Запустите программу «Проводник» (Пуск /Программы / Проводник).

1. Скопируйте в созданную папку несколько произвольных файлов.

2. Выделите один из файлов и откройте контекстное меню. Обратите внимание на то, что в нем имеются два пункта для создания архива (создание архива с произвольным именем и с именем, соответствующим текущему файлу). Появление этих пунктов связано с наличием в компьютерной системе диспетчера архивов и интеграции WinZip с Проводником Windows.

3. Выполните команду Добавить в архив. Далее произойдет автоматический запуск диспетчера архивов WinZip и откроется диалоговое окно Добавление в архив.

4. В поле Добавить в архив ввести название файла создаваемого архива, адрес текущей папки заносится автоматически. Проверив настройку прочих элементов управления, запустите процесс архивации щелчком на командной кнопке Добавить.

5. Перейдите в окно программы Проводник и убедитесь в том, что в папке появился архивный файл test.zip. Щелкните на значке архивного файла правой кнопкой мыши и изучите новые команды контекстного меню, позволяющие выполнить операции с архивным файлом.

6. Выполните команду Создать самораспаковывающийся архив. В открывшемся диалоговом окне щелкните на командной кнопке «Да» и в последующих диалоговых окнах откажитесь от проверки созданного архива.

7. Закройте открытые окна программы WinZip и в программе Проводник убедитесь в том, что в рабочей папке появился исполняемый файл (.exe).

8. В программе Проводник выполните перетаскивание значка любого файла (или группы файлов) на значок созданного ZIP-архива. При отпускании кнопки мыши в конце перетаскивания происходит автоматическое добавление новых файлов в архив. Если содержимое правой панели Проводника открыто в режиме Таблица, после каждого перетаскивания можно наблюдать увеличение размера файла архива.

2. Исследование свойств форматов сжатия графических данных

1. Откройте графический редактор Paint (Пуск/Программы/Стандартные/ Paint).

2. Загрузите в него заранее подготовленный многоцветный рисунок.

3. Определите размер рисунка в пикселях (Рисунок/Атрибуты).

4. Оцените теоретический размер рисунка в 24-разрядной палитре (3 байта на точку) по формуле:$S=M-N-3$,

где S– размер файла с рисунком (байт);

M – ширина рисунка (точек);

N– высота рисунка (точек).

5. Сохраните рисунок в папку X:\ОТИ\Pictures, выбрав имя файла test и назначив тип файла: 24-разрядный рисунок (.BMP).

6. Повторно сохраните рисунок, выбрав то же имя test, но назначив тип файла .GIF. При сохранении произойдет потеря определенной части графической информации.

7. Восстановите рисунок, загрузив его из ранее сохраненного файла Test.bmp.

8. Вновь сохраните его под тем же именем, но выбрав в качестве типа файла формата *.JPEG*.

9. Откройте папку X:\ОТИ\Pictures в режиме Таблица.

10. Определите размеры файлов Test.bmp, Test.gif и Test.jpg.

11. Определите коэффициент сжатия файлов *(R)*, взяв отношения размеров файлов к теоретической величине, полученной расчетным путем.

12. Создать или скопировать на рабочем диске в папке **Практика 10**5-7 файлов (текстовых, исполняемых, командных, программных).

13. Создать архивы для этих файлов с помощью различных архиваторов, например, WinRar, WinZip и др.

14. Сравнить объемы получившихся файлов, результаты занести в таблицу и сделать выводы:

Название архиватора	Тип файла	Размер файла	Размер файла после сжатия	Степень сжатия(%)

15. Сохраните файл под именем **Сравнение**.

16. С помощью архиватора выполнить следующие команды:

а) добавить в архив заданный файл;

б) поместить в архив все файлы из текущего каталога, за исключением файлов с заданным расширением;

в) создать защищенный архив;

г) создать архивный файл, позволяющий сохранить структуру каталогов;

д) добавить комментарии к архивам;

е) извлечь заданный файл из архива.

ж) создать многотомный архив, указав размер тома – 80 К;

з) выполнить поиск заданной строки в архивах по различным поисковым признакам.

17. Используя программу архивации, создать многотомный архив с паролем, заданным в параметрах, поместив в них все файлы из папки ОТИ, исключив файлы с расширением EXE.

18. Просмотреть списки созданных архивов.

19. Создать самораспаковывающиеся RAR- и ZIP-архивы, не поддерживающие распределенные архивы (включить переключатель «Без распределения» в группе SpanningSupport – Поддержка распределенного архива).

20. Создать самораспаковывающиеся распределенные архивы RAR- и ZIP-архивы.

21. Используя диспетчер архивов WinZip, выполнить интеграцию служебных и прикладных программ с операционной системой Windows.

22. Исследуйте свойства форматов сжатия графических данных (файлы .bmp, .gif, .jpg). Результаты занесите в таблицу, созданную в файле **Сравнение**:

Формат файла	Размер файла (Кбайт)	Степень сжатия (%)
24 разрядный .bmp		
.gif		
.jpg		
.png		

23. Используя табличный процессор, построить диаграммы по результатам, приведенным в таблицах, и сделать выводы.

3. Ответьте на контрольные вопросы:

1. Зачем нужно архивировать информацию?
2. По какому принципу архиваторы сжимают информацию.
3. Каковы функции архиваторов.
4. Чем отличаются SFX – архивы.

4. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 2).

Практическая работа №11

Название практической работы: Кодирование по алгоритму Хаффмана

Цель работы: освоить приемы работы с архиваторами и способы кодирования по методу Хаффмана.

знания (актуализация)**:**

– способы передачи цифровой информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

умения:

– применять закон аддитивности информации.

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 9 Использовать информационные технологии в профессиональной деятельности.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Пример 1: Пусть $A=\{a_1,a_2,\ldots,a_n\}$ - алфавит из n различных символов, $W=\{w_1,w_2,\ldots,w_n\}$ - соответствующий ему набор положительных целых весов. Тогда набор бинарных кодов $C=\{c_1,c_2,\ldots,c_n\}$, такой что:

1) c_i не является префиксом для c_j, при i!=j
2) $\sum_{i=1}^{n} w_i|c_i|$
3) минимальна (|ci| длина кода ci)

называется *минимально-избыточным префиксным кодом* или иначе *кодом Хаффмана*.

Наиболее известный простой подход и алгоритм сжатия информации обратимым путем - это кодирование серий последовательностей (RunLengthEncoding - RLE). Суть методов данного подхода состоит в замене цепочек или серий повторяющихся байтов или их последовательностей на один кодирующий байт и счетчик числа их повторений.

Коэффициент сжатия вычисляется по формуле:

$$К_{сж} = V_{сж} / V_{исх} \quad (1)$$

Процент сжатия вычисляется по формуле:

$$Р_{сж} = V_{сж} / V_{исх} * 100\% \quad (2)$$

Ход работы:

1. Решите задачи:

а). Средняя скорость передачи данных с помощью модема равна 36 864 бит/с. Сколько секунд понадобится модему, чтобы передать 4 страницы текста в 8-битной кодировке КОИ8, если считать, что на каждой странице в среднем 2 304 символа?

б). Определите количество секунд, которые потребуются модему, передающему сообщения со скоростью 28800 бит/с, для передачи цветного растровое изображения размером 640x480 пикселей, при условии, что цвет каждого пикселя кодируется тремя байтами.

в). Сколько секунд потребуется модему, передающему сообщение со скоростью 28800 бит/сек, чтобы передать цветное изображение размером 640*480 пикселей, при условии, что цвет каждого пикселя кодируется 3 байтам.

г).Известно, что длительность непрерывного подключения к сети Интернет с помощью модема для некоторых АТС не превышает 10 мин. Определите максимальный размер файла (Кбайт), который может быть передан за время такого подключения, если модем передает информацию в среднем со скоростью 32 Кбит/сек.

2. Используя метод Хаффмана, выполните сжатие информации:

«КАКАЯ ЗИМА ЗОЛОТАЯ!
КАК БУДТО ИЗ ДЕТСКИХ ВРЕМЕН...
НЕ НАДО НИ СОЛНЦА, НИ МАЯ –
ПУСТЬ ДЛИТСЯ ТОРЖЕСТВЕНИЫЙ СОН.

ПУСТЬ Я В ЭТОМ СНЕ ПОЗАБУДУ
КОГДА-ТО МАНИВШИЙ ОГОНЬ,
И ЛЕТО ПРЕДАМ, КАК ИУДА,

ЗА ТРИДЦАТЬ СНЕЖИНОК В ЛАДОНЬ.

ЗАТЕМ, ЧТО И Я ХОЛОДЕЮ,
ТЕПЛО УЖЕ СТРАШНО ПРИНЯТЬ:
Я СЛИШКОМ ДАВНО НЕ УМЕЮ
НИ ТЛЕТЬ, НИ ГОРЕТЬ, НИ СЖИГАТЬ…

ВСЕ ЧАЩЕ, ВСЕ ДОЛЬШЕ НЕМЕЮ:
К ЗИМЕ УЖЕ ДЕЛО, К ЗИМЕ...
И ТОЛЬКО ТОГО ОТОГРЕЮ,
КОМУ ХОЛОДНЕЕ, ЧЕМ МНЕ»

3. Используя метод RLE, выполните сжатие информации:

1 последовательность:

SSSSOOOEEERROOOAAYYYYYDDDDOEUUUUUWWWWJJJORRUUUUUUUUUXXXKHHHHHHMMMMMMMGGGLLLLLLLJJJJ

2 последовательность:

FFFFFFFFKKKKKSSSSUURERRRRRRRRRPPPPPPPPDDDDKKKKKKGLDDDDDDDDKKKKKKKKKGGGGMGMMMM

4. Сравните размеры исходного файла и архивного. Вычислите коэффициент и процент сжатия.

5. Ответьте на контрольные вопросы:

– Опишите сжатие информации по методу Хаффмана;

– Напишите формулу для расчета пропускной способности канала (линии) связи.

6. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №12

Название практической работы: Таблично-символьное кодирование

Цель работы: сформировать умения символьного кодирования, научиться определять числовые коды символов.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

умения:

– применять закон аддитивности информации;

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Для удобства изучения методы кодирования информации принято рассматривать по категориям. Роль этих категорий выполняют так называемые *схемы кодирования*.

Существуют три основные схемы кодирования. Это аналоговое, табличное и цифровое кодирование.

Схемы аналогового кодирования распространены в живой природе. В ходе развития научно-технического прогресса общество постепенно адаптировало их под свои нужды. Именно аналоговое кодирование нашло наиболее раннее применение при записи изображений, звука, видео.

Схемы табличного кодирования не имеют и не могут иметь реализаций в живой природе — это изобретение общества. Люди пользуются табличным кодированием с того момента как научились на пальцах обозначать предметы, животных, людей. На табличном кодировании основаны все виды письменности. Табличное кодирование обеспечивает большинство потребностей неавтоматизированного общественного информационного обмена.

Среди табличных схем кодирования особо выделяют две самостоятельные категории:

– схемы таблично-символьного кодирования;

– схемы таблично-цифрового кодирования.

Таблично-символьное кодирование широко используют при непосредственном информационном обмене, а схемы табличного и цифрового кодирования применяют, когда информационный обмен между людьми осуществляется с помощью средств вычислительной техники. Например, для обмена письменными сообщениями достаточно схем символьного кодирования. Но если сообщение должно быть отправлено по телеграфу или по электронной почте, то без цифрового кодирования не обойтись.

Цифровое кодирование не имеет реализаций ни в живой природе, ни в непосредственном информационном обмене между людьми. Это достижение современного общества. Применяется оно в системах автоматического информационного обмена и действует при сохранении информации или при её передаче между техническими устройствами.

Ход работы:

1. Укажите десятичный код выражения «I promise» в соответствии с кодовой таблицей ASCII.

2. Укажите шестнадцатеричный код выражения «теория информации» в соответствии с кодовой таблицей ASCII.

3. Закодируйте свое имя, фамилию и отчество с помощью одной из таблиц (win-1251, KOI-8).

4. Буква Z имеет десятичный код 90, а z – 122. Записать слово «sport» в десятичном коде.

5. С помощью десятичных кодов зашифровано слово «info» 105 110 102 111. Записать последовательность десятичных кодов для этого же слова, но записанного заглавными буквами.

6. С помощью 3 таблиц кодировки представьте двоичный код следующего предложения: «Цифровое кодирование не имеет реализаций ни в живой природе, ни в непосредственном информационном обмене между людьми***»***

7. Ответьте на контрольные вопросы:

–Что такое таблица кодировки?

– Перечислите основные схемы кодирования

8. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №13

Название практической работы: Цифровое кодирование

Цель работы: сформировать умения кодирования числовой информации.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

умения:

– применять закон аддитивности информации;

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Для представления информации в памяти ЭВМ (как числовой, так и не числовой) используется двоичный способ кодирования. Элементарная ячейка памяти ЭВМ имеет длину 8 бит (байт). Каждый байт имеет свой номер (его называют **адресом**). Наибольшую последовательность бит, которую ЭВМ может обрабатывать как единое целое, называют **машинным словом**. Длина машинного слова зависит от разрядности процессора и может быть равной 16, 32, 64 битам и т.д.

Двоичные разряды в любой ячейке памяти нумеруются справа налево, начиная с нуля. Существуют два основных формата представления чисел в памяти компьютера. Один из них используется для кодирования целых чисел, второй (так называемое представление числа *в формате с плавающей точкой*) используется для задания некоторого подмножества действительных чисел. Для

положительных и отрицательных чисел существует знаковый способ представления числа. Под знак отводится старший разряд ячейки:

0 - для положительных чисел,

1 - для отрицательных чисел.

Для упрощения реализации арифметических операций в компьютере целые числа представляются специальными кодами - прямым, обратным и дополнительным.

Для положительного числа прямой, обратный и дополнительный коды выглядят одинаково.

Прямой код двоичного числа – это само двоичное число, причем значение знакового разряда для положительных чисел равно 0, а для отрицательных чисел - 1.

Обратный код отрицательного числа получается из прямого кода путем замены нулей единицами, а единиц нулями, исключая знаковый разряд.

Дополнительный код отрицательного числа образуется как результат суммирования обратного кода с единицей младшего разряда. Перенос в знаковый разряд при этом теряется.

Дополнительный код целого отрицательного числа может быть получен по следующему алгоритму:

1) записать прямой код модуля числа;
2) инвертировать его (заменить единицы нулями, нули — единицами);
3) прибавить к инверсному коду единицу.

Например, запишем дополнительный код числа -37, интерпретируя его как величину типа LongInt (тридцатидвухбитовое со знаком):

1) прямой код числа 37 есть 00000000000000000000000000100101;
2) инверсный код 11111111111111111111111111011010;
3) дополнительный код 11111111111111111111111111011011 или $FFFFFFDB_{(16)}$.

При получении числа по его дополнительному коду прежде всего необходимо определить его знак. Если число окажется положительным, то просто перевести его код в десятичную систему счисления. В случае отрицательного числа необходимо выполнить следующий алгоритм:

1) вычесть из кода числа 1;
2) инвертировать код;
3) перевести в десятичную систему счисления. Полученное число записать со знаком минус.

Пример№1: Запишем числа, соответствующие дополнительным кодам:

1) 0000000000010111. Поскольку в старшем разряде записан нуль, то результат будет положительным. Это код числа 23.

2) 1111111111000000. Здесь записан код отрицательного числа.

Исполняем алгоритм:

1) $1111111111000000_{(2)} - 1_{(2)} = 1111111110111111_{(2)}$;

2) 0000000001000000;

3) $1000000_{(2)} = 64_{(10)}$.

Ответ: -64.

Для представления числа в нормализованной форме нужно представить число в виде:

$$R=m*P^n \qquad (6)$$

где *m -мантисса числа;*

P - основание системы счисления;

n - порядок, указывающий, на какое количество позиций и в каком направлении должна сместиться точка, отделяющая дробную часть в мантиссе.

Нормализованная мантисса меньше единицы и первая значащая цифра не ноль.

Например, $159,6 = 0,15916 \cdot 10^3$

$0,05975 = 0,5975 \cdot 10^{-1}$

$0,000142 = 0,142 \cdot 10^{-3}$

Ход работы:

1. Запишите нормализованную форму десятичных чисел:

а). 3,1415926;

б). 0,00000578;

в). 25, 01;

г). 134, 9887;

д). 0,010765.

2. Получите внутреннее 8-разрядное и 16-разрядное представление десятичного числа 200_{10}.

3. Получите внутреннее 8-разрядное представление отрицательного числа -117_{10}.

4. Получите дополнительный код двоичного числа -1000_2 для 8-разрядной ячейки памяти.

5. Получите двоичную форму внутреннего представления целых чисел 1689_{10} и -1689_{10} в 2-х байтовой ячейке.

6. Получите двоичную форму внутреннего представления целых чисел 259_{10} и -259_{10} в 4-х байтовой ячейке.

7. Запишите в десятичной системе счисления целое число, если его дополнительный код 1000000110101110.

8. Получите внутреннее представление целого числа 84_{10} в 8-разрядной ячейке памяти компьютера. Результат переведите в шестнадцатеричную систему счисления.

9. Получите внутреннее представление целого числа -134_{10} в 8-разрядной ячейке памяти компьютера. Результат переведите в шестнадцатеричную систему счисления.

10. Получите внутреннее представление целого числа 123_{10} в 8-разрядной ячейке памяти компьютера. Результат переведите в шестнадцатеричную систему счисления.

11. Получите внутреннее представление вещественного числа $12{,}005_{10}$ в 32-разрядной ячейке памяти компьютера. Результат переведите в шестнадцатеричную систему счисления.

12. Получите внутреннее представление числа вещественного-$0{,}000125_{10}$ в 32-разрядной ячейке памяти компьютера. Результат переведите в шестнадцатеричную систему счисления.

13. Выполните сложение в компьютере над числами (тип чисел Integer):

а). 177_{10} и 318_{10}

б). -39_{10} и 68_{10}

в). 111_{10} и -199_{10}

г). 137_{10} и -125_{10}.

14. Ответьте на контрольные вопросы:

– Как записать число в нормализованном виде;

– Запишите алгоритм создания дополнительного кода целого отрицательного числа.

15. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №14

Название практической работы: Аналоговое кодирование

Цель работы: научиться кодировать мультимедийную информацию.

знания (актуализация)**:**

– принципы кодирования и декодирования информации;

– методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных;

умения:

– применять закон аддитивности информации;

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

При двоичном кодировании аналогового звукового сигнала непрерывный сигнал дискретизируется, т.е. заменяется серией его отдельных выборок - отсчётов. Качество двоичного кодирования зависит от двух параметров: количества дискретных уровней сигнала и количества выборок в секунду. Количество выборок или частота дискретизации в аудиоадаптерах бывает различной: 11 кГц, 22 кГц, 44,1 кГц и др. Если количество уровней равно 65536, то на один звуковой сигнал рассчитано 16 бит (216). 16-разрядный аудиоадаптер точнее кодирует и воспроизводит звук, чем 8-разрядный.

Количество бит, необходимое для кодирования одного уровня звука, называется глубиной звука. Объём моноаудиофайла (в байтах) определяется по формуле:

$$I(\text{бит})=f(\text{Гц})*R(\text{бит})*N(\text{каналов})*t(\text{сек}) \quad (1)$$

где f – частота дискретизации (Гц);

R – глубина кодирования (разрядность звуковой карты);

N – количество каналов (1 – моно, 2 – стерео);

t – время звучания в сек.

При стереофоническом звучании объём аудиофайла удваивается, при квадрофоническом звучании – учетверяется.

Если известна глубина кодирования, то количество уровней громкости цифрового звука можно рассчитать по формуле:

$$N = 2^I \quad (8)$$

где I – глубина кодирования.

Пусть глубина кодирования звука составляет 16 битов, тогда количество уровней громкости звука равно: $N = 2^I = 2^{16} = 65536$.

Пример №1:Рассчитайте объем стереоаудиофайла длительностью 20 секунд при 20-битном кодировании и частоте дискретизации 44.1 кГц.

Решение.

V = 20 бит * 20 * 44100 * 2 = 35280000 бит = 4410000 байт = 4.41 Мб

При кодировании графической растровой информации учитывается количество цветов и разрешение монитора, размер изображения.

Количество цветов в палитре изображения вычисляется по формуле:

$$N = 2^I \quad (9)$$

где I – глубина цвета.

Объем графического изображения определяется по формуле:

$$V = M \times N \cdot I \quad (10)$$

где I – глубина цвета;

M x N - Разрешающая способность экрана в пикселях или размер изображения в битах.

Пример №2: Если экран монитора имеет растр 600Х800 пикселей и каждый пиксель имеет размер 24 бита, то общий объём изображения со всего экрана

V = 600Х800·24 = 11520000 бит =11520000/8 = 1440000 байт/1024 = 1406,25 кб/1024 = 1,37 Мб

Ход работы:

1. Определите цвет, закодированный в RGB при 256 градациях тона:

а) (255,255,255);

б) (0, 255,0);

в) (0,0,127);

г) (127, 0,0).

2. Решите задачи:

б). Определите количество цветов, отображаемых на экране монитора при глубине цвета 16 бит;

в). Определите количество цветов, отображаемых на экране монитора при глубине цвета 24 бита;

г).Для хранения растрового изображения размером 64×64 пикселя отвели 512 байтов памяти. Определите максимально возможное число цветов в палитре изображения;

д). Для хранения растрового изображения размером 128x128 пикселей отвели 4 Килобайта памяти. Определите максимально возможное число цветов в палитре изображения. Использовать операции со степенями двойки;

е). Укажите минимальный объем памяти (в килобайтах), достаточный для хранения любого растрового изображения размером 64×64 пикселя, если известно, что в изображении используется палитра из 256 цветов. Саму палитру хранить не нужно;

ж). Голубой цвет на компьютере с объемом страницы видеопамяти 250 Кбайт кодируется кодом 0000 0011. Определите разрешающую способность графического дисплея;

з).Известно, что видеопамять компьютера имеет объем 512 Кбайт. Разрешающая способность экрана 640 на 200. Сколько страниц экрана одновременно разместится в видеопамяти при палитре из 8 цветов/16 цветов/256 цветов?

и). Определите объем памяти, который занимает одна минута цифрового звука (стерео), записанного с частотой 44,1 кГц и разрядностью 16 бит;

к). Определите объем памяти, который занимает одна минута цифрового звука (моно), записанного с частотой 32 кГц и разрядностью16 бит;

л). Определите объем памяти, который занимает 5 минут цифрового звука (стерео), записанного с частотой 32 кГц и разрядностью16 бит;

м). Определите объем памяти, который занимает одна минута цифрового звука (стерео), записанного с частотой 44,1 кГц и разрядностью 8 бит;

н). Объем свободной памяти на диске — 5,25 Мб, разрядность звуковой платы — 16 битов. Какова длительность звучания цифрового аудиофайла, записанного с частотой дискретизации 22,05 кГц?

о). Одна минута записи цифрового аудиофайла занимает на диске 1,3 Мб, разрядность звуковой платы – 8 бит. С какой частотой дискретизации записан звук?

п). Две минуты записи цифрового аудиофайла занимают на диске 5,1 Мб. Частота дискретизации — 22 050 Гц. Какова разрядность аудиоадаптера?

р). Объем свободной памяти на диске — 0,1 Гб, разрядность звуковой платы — 16. Какова длительность звучания цифрового аудиофайла, записанного с частотой дискретизации 44 1001Гц?

3. Ответьте на контрольные вопросы:

– Перечислите параметры, влияющие на объем графического изображения;

– Напишите формулу для вычисления объёма моноаудиофайла.

4. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №15

Название практической работы: Практическое применение криптографии. Изучение и сравнительный анализ методов шифрования

Цель работы: освоить простейшие методы криптографической зашиты информации.

знания (актуализация)**:**

– методы криптографической защиты информации;
– способы генерации ключей.

уметь:

– применять закон аддитивности информации

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Криптография - наука о методах преобразования информации с целью ее защиты от незаконных пользователей.

Стеганография - набор средств и методов сокрытия факта передачи информации.

Некоторые методы стеганографии:

1. В древности голову раба брили, на коже головы писали сообщение и, после отрастания волос, раба отправляли к адресанту.

2. Скрытое письмо между строк: молоком, апельсиновым (или лимонным) соком, другими химическими веществами.

3. "Микроточка". Сообщение с помощью современной технологии записывается на очень маленький носитель ("микроточку"), которая пересылается адресату, например, под обычной маркой.

4. Акростих - первые буквы слов стихотворения несут информацию:

Добрый удод наелся ягод,

Умный удод наелся на год.

Наелся удод и песни поет.

Ягод наелся удод.

5. Например, каждое четвертое слово в посылаемом сообщении несет информацию (остальные слова ничего не значат). Пример: "Тридцать первого августа встреча судебного совета округа состоялась. Подтвердите дату следующего как можно скорее. Участники договорились собраться там же. Борис."

Разновидности шифров

1. Шифр замены. Каждая буква заменяется на определенный символ или последовательность символов. Пример: "Пляшущие человечки" Конан Дойля.

2. Шифр перестановки. Буквы в передаваемом сообщении меняются местами в соответствии с определенным правилом. Примеры: МАМА - АМАМ.

3. Книжный шифр. В шифрованном тексте каждое слово заменено на пару чисел номер страницы в книге и номер этого слова на странице. (т.е. текст выглядит примерно так: 3-45 45-67 …).

Ключ - сменный элемент шифра, который применен для шифрования конкретного сообщения.

Шифры перестановки

Маршрутная транспозиция

Т - дополнительная буква.

В О С К Р Е

А М Я А Н С

Т Е М А Т И

Я А К С Е Ч

Ш К О Л А Т

Фраза "Воскресная математическая школа" становится: "ЕСИЧТ АЕТНР КААСЛ ОКМЯС ОМЕАК ШЯТАВ".

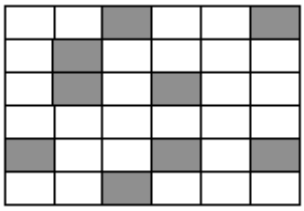
Ключ - число 6.

Постолбцовая транспозиция

К	А	Ш	А
3	1	4	2
Ш	Л	А	С
А	Ш	А	П
О	Ш	О	С
С	Е	И	С
О	С	А	Л
А	С	У	Ш
К	И		

Лшшессиспсслшшаосоакааои ау.
Над столбцами записывается ключевое слово, затем в соответствии с порядком букв в алфавите столбцы нумеруются, а затем выписываются подряд: первый столбец, за ним второй и т.д.
Ключ здесь - "каша".

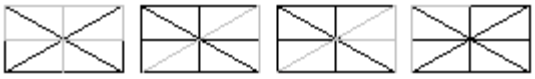
Шифр "Решетка"



Если хочешь быть красивым поступи в гусары. (Высказывание Козьмы Пруткова)
Пьеиисвлыбымтивхгьукпросоарчсеташуыс.
Ключом является решетка

Шифры замены

Шифр "Британский флаг"



Ответ: флаг.

Каждая буква заменяется несколькими символами

Криптография	11179161915417121932
	К1К7А9К6К9К5А4К7А1Ф1А9Ю2
	И2О2ИО1О4ОА3О2АУ1ИЯ

Ход работы:

1. Придумать акростих, в котором скрыто ваше имя.
2. Придумать послание, используя лишние слова.
3. Зашифровать, используя шифр перестановки:

a) Французский математик Пьер Ферма по образованию был юрист.

b) Леонардо Пизанского математики знают под именем "сын добряка" или Фибоначчи.

4. Дешифровать (восстановить сообщение, зная ключ) Ключ 8. Чинои сечем лчгмсхыеооеаитнккыинлтсбчвтрйыеооссееорснеомвбадерпокп.

Примечание: АБ-дополнительные буквы.

5. Расшифровать (восстановить сообщение, не зная ключа). Осузуааневемисчитдьмодоаьлвьрдвобыи.

6. Расшифровать:

Етгртуойдкмиуиавцлишлаегврныинисаяоплыдбаанполбр.

Ключом является правило расстановки.

В	О	Е	С	М	А	Л	А	Воесмаласрнетокатикяачшмеяса к.
С	Р	Н	Е	Т	О			Или Воес мала срне тока тикяачшмеяса к.
К	А	Т	И	К				
Я	А	Ч	Ш					
М	Е	Я						
С	А							
К								

7. Расшифровать фразу: Сошки ввнлыохеденванзбркоееуквсизазх.

8. Расшифровать фразу: Леортиюдтнетмауаялееочнмкжхойчейооотлсечи_пчсднит _киехса_члилж_ашоо_врп_уо_ к_ _

<u>Используя постолбцовую транспозицию:</u>

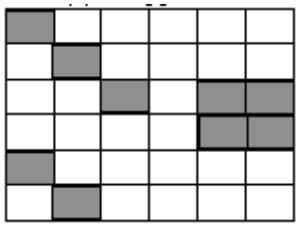
9. Зашифруйте фразу: Не плюй в колодец: вылетит - не поймаешь.

10. Дешифруйте старинное японское хайку: (ключом будет имя известного японского поэта "Басё") Тйдгадгалвисыуылоякпкшрррувлшссиеаппнвуувет н.

11. Расшифруйте высказывание Козьмы Пруткова: Акоеаь дне дсцтанжодсскдагрео о.

12. Придумать решетку и зашифровать фразу: "Евклид был древнегреческим математиком"

13. Дешифровать:



а) Сиекпетпароокоолкойслтйстськвонвоски.

б) Двплгораимидрувтайгуектегньдотыоруам.

14. Зашифровать фразу: "ВГГУ", используя шифры замены

15. Расшифровать:

а). 1111712 20 111211728 201117112 11517112121228

б). 11212941191517 16122812 1615 176116 111514415

в). 11176191832 5157529 1815291716191832

г). И1А2А5И5О4 Е3И5О4Я1О2 Я1И5О4Е3И5 И6О1И6О1О5 И3Ю1О2И5У8 И1А3И6И3Е3 А2О5А4О3И2 Е3И1О2А5Е1 Е3О3О3А5О2.

5. Ответьте на контрольные вопросы:

– Что такое криптография?

– Перечислите методы шифрования.

6. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №16

Название практической работы: Криптография с симметричным ключом, с открытым ключом

Цель работы: освоить простейшие методы криптографической зашиты информации.

знания (актуализация)**:**

– методы криптографической защиты информации;
– способы генерации ключей.

уметь:

– применять закон аддитивности информации

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Шифры "Пляшущие человечки"

Основной метод расшифровки подобных шифров - частотный анализ. (+ логические рассуждения).

Таблица частот:

В русском языке в каждой тысяче символов в среднем встречается

пробел	175	р	40	я	18	х	9
о	90	в	38	з	16	ж	7
е, ё	72	л	35	ы	16	ш	6
а	62	к	28	б	14	ю	6

и	62	м	26	ъ, ь	14	ц	4
н	53	д	25	г	13	э	3
т	53	п	23	ч	12	щ	3
с	45	у	21	й	10	ф	2

Чаще всего буквы заменяют другими буквами.

Шифр Цезаря

В шифре Цезаря каждая буква заменяется на букву, которая идет через 3 после этой: т.е. А=>Г, О=>С, Я=>В.

Примечание: можно делать сдвиг не на три, а на произвольное количество букв.

Шифр Виженера

Ключ ВАЗА: /3 1 8 1/

Сдвиг осуществляется не на постоянную величину, а на номер буквы в ключевом слове. КРИПТОГРАФИЯ => НСРРХПЛСГХРА.

Сложность при расшифровке в том, что одинаковые буквы переходят в разные, а разные - в одинаковые => частотный анализ не применим.

Ход работы:

1. При помощи таблицы Вижинера зашифровать тексты:

а). «Полиалфавитная замена». Ключ «Шифр»

б). «Кодирование информации». Ключ ЕВРО

2. Зашифруйте выражение «toletknow» с помощью таблиц Полибинийского квадрата;

3. Расшифровать текст, используя шифры "Пляшущие человечки":

СзргйзютсуцълнУйиефнлмцкрго, ъхс зов кргнспфхег ф зиецынсмргзстсзсмхл, ритулрцйзиррстсжсесулхя с тсжзи л тсфоиахсжстуизфхгелхяфв. Ргсзрсмлктусжцосн ср тсефхуиъгожцовбьцб ф дсосрнсмзиецынц. Тсуцълнтсзсыио н рим, трцоиидсосрнцхгн, ъхсхгзгоинсцоихиог л фнгкго:

- Рлкнсоихлх. Елзгхя, н зсйзб. Нфхгхл, угкуиылхитуизфхгелхяфв, тсуцълнУйиефнлм.

С – 37

И - 21

Г-18

Н – 18

Л - 18
З – 17
Р -16
Ц - 14
Т – 14
Ф – 13
У – 13
Е – 10
М - 7
Й - 5
Я -3
А – 1
Ю – 1

4. Расшифровать текст, используя шифры "Пляшущие человечки":

СзргйзютсуцълнУйиефнлмцкрго, ъхс зов кргнспфхег ф зиецынсмргзстсзсмхл, ритулрцйзиррстсжсесулхя с тсжзси л тсфоиахсжстуизфхгелхяфв. Ргсзрсмлктусжцосн ср тсефхуиъгожцовбьцб ф дсосрнсмзиецынц. Тсуцълнтсзсыио н рим, трцоиидсосрнцхгн, ъхсхгзгоинсцоихиог л фнгкго:

- Рлкнсоихлх. Елзгхя, н зсйзб. Нфхгхл, угкуиылхитуизфхгелхяфв, тсуцълнУйиефнлм.

5. Используя шифр Цезаря:

Зашифровать фразу: "Идет занятие по криптографии".

Расшифровать фразу: Схсоябхфвнсынипюынлрюфоикнл.

Зашифровать фразу: Математика - царица наук.

6. Ответьте на контрольные вопросы:

– Перечислите методы криптографической защиты информации
– Приведите алгоритм шифрования методом Вижинера

7. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Практическая работа №17

Название практической работы: Шифрование с использованием перестановок. Шифрование с использованием замен

Цель работы: освоить простейшие методы криптографической зашиты информации.

знания (актуализация)**:**

– методы криптографической защиты информации;
– способы генерации ключей.

уметь:

– применять закон аддитивности информации

элементы следующих компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 4 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

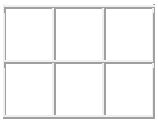
ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Теоретический материал:

Шифр Гронсфельда: Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

Сообщение		В	О	С	Т	О	Ч	Н	Ы	Й		Э	К	С	П	Р	Е	С	С
Ключ		2	7	1	8	2	7	1	8	2		7	1	8	2	7	1	8	2
Шифртекст		Д	Х	Т	Ь	Р	Ю	О	Г	Л		Д	Л	Щ	С	Ч	Ж	Щ	У

Чтобы зашифровать первую букву сообщения В, используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В в алфавите:



получается первая буква шифртекста Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Ход работы:

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	Σ
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	ω
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♣		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №1

- И.РЮУ.ЪФОБГНО
- СЛХГ.ЪЛХО.ФОО.ЩВ

2. Пусть исходный алфавит содержит следующие символы:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:

- КРИПТОСТОЙКОСТЬ
- ГАММИРОВАНИЕ

3. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_

Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:

- ШВМБУЖНЯ
- ЯБХЪШЮМХ

4. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:

- ЖЕЛТЫЙ_ОГОНЬ
- МЫ_НАСТУПАЕМ

5. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:

- СЛПИЬНАЕ
- РОИАГДВН

6. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:

- МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
- СИГНАЛ БОЯ – НИСАГО ЛЯБ

7. Зашифруйте с помощью шифра Гронсфельда и ключа КАЛИНА сообщения:

- КРИПТОГРАФИЯ
- ГРОНСВЕЛЬД.

7. Ответьте на контрольные вопросы:

– Перечислите методы криптографической защиты информации с открытым и закрытым ключом.

– Приведите алгоритм шифрования методом Гронсфельда.

8. Оформите и сдайте отчет преподавателю (образец отчета представлен в Приложении 3).

Информационные источники

Основные источники:

1. Цветкова, М.С. Информатика : учебник для студ. учреждений сред. проф. образования / М.С. Цветкова, И.Ю. Хлобыстова. - 3-е изд. . стер. - М. : Академия, 2017. - 352с. : ил.

Дополнительные источники:

2. Павлов, С.В. Теория вероятностей и математическая статистика [Электронный ресурс]. – М. : ИЦ РИОР: ИНФРА-М, 2014.-186с.- доступ из ЭБС "Знаниум"

3. Гусева А.И. Дискретная математика: сборник задач [Электронный ресурс]. – М.: КУРС: НИЦ ИНФРА-М, 2017.- 224с.- (Среднее профессиональное образование).- доступ из ЭБС "Знаниум"

Приложение 1

Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный технический колледж»

ОТЧЕТ
по практическим работам

учебная дисциплина

«ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ»

специальность 09.02.06
Сетевое и системное администрирование
Квалификация: сетевой и системный администратор

Выполнил: _____
Группа:_____
Проверил: _____

Челябинск, год

Приложение 2
Отчет по практической работе

Практическая работа № 1

Название практической работы: Способы хранения обработки и передачи информации

Цель работы: сформировать умения систематизировать и упорядочивать документы на ПК, организовывать их размещение, хранение, обработку, поиск и передачу файлов

Ход работы:

1. Выполните вставку скриншотов файлов: Моя профессия, Фамилия, Моя группа.

2. Опишите алгоритм создания файла Моя группа

3. Ответы на контрольные вопросы:

– ...

– ...

4. Вывод по работе: …

Приложение 3
Отчет по практической работе

Практическая работа № 2
Название практической работы: Измерение количества информации

Цель работы: научиться измерять информацию различными методами, использовать правила перевода информации из одних единиц измерения в другие.

Ход работы:

1. Выполните перевод единиц измерения информации:

Расчеты

2. Используя содержательный подход к измерению информации, решите задачи:

Условия задач и решение

3. Используя алфавитный подход к измерению информации, решите задачи:

Условия задач и решение

4. Решите задачи на измерение информации:

Условия задач и решение

5. Ответы на контрольные вопросы:

– ...
– ...

6. Вывод по работе: …