АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»
(АНО ВО «РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»)

IT-Колледж

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
для оценки результатов освоения
учебной дисциплины

ОП. 12 ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ

для специальности
09.02.06 Сетевое и системное администрирование

г. Москва
2024 год

1. Паспорт комплекта контрольно-оценочных средств дисциплины

Комплект контрольно-оценочных средств для проведения текущего контроля, промежуточной аттестации разработан в соответствии с программой учебной дисциплины.

Комплект контрольно-оценочных средств разработан на основании:

- основной образовательной программы по специальности СПО 09.02.06 Сетевое и системное администрирование программы учебной дисциплины Основы теории информации.

2. Результаты освоения учебной дисциплины

В результате аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих компетенций.

В результате освоения учебной дисциплины ОПЦ.12. Основы теории информации студент должен обладать предусмотренными ФГОС по специальности СПО 09.02.06 Сетевое и системное администрирование следующими умениями, знаниями, которые формируют профессиональные компетенции, и общими компетенциями:

Код ПК, ОК	Умения	Знания
ОК 01-ОП 02, ОП 09; ПК 1.3	Применять закон аддитивности информации. Применять теорему Котельникова. Использовать формулу Шеннона.	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.

Умения:

У1 Применять закон аддитивной информации.
У2 Применять теорему Котельникова.
У3 Использовать формулу Шеннона.

Знания:

З1. Виды и формы представления информации;
З2. Методы и средства определения количества информации;
З3. Принципы кодирования и декодирования информации;
З4. Способы передачи цифровой информации;
З5. Методы повышения помехозащищенности передачи и приема данных, основы теории сжатия данных
З6. Методы криптографической защиты информации

37. Способы генерации ключей

Формой промежуточной аттестации по учебной дисциплине является экзамен.

3.Оценка освоения учебной дисциплины

3.1. Формы и методы контроля

Контроль и оценка освоения учебной дисциплины по темам

Элемент учебной дисциплины	Формы и методы контроля				
	Текущий контроль			Промежуточная аттестация	
	Форма контроля	Самостоятельная работа	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З
Раздел 1. Базовые понятия теории информации	*Устный опрос по теме «*Формальное представление знаний. Виды информации» *Устный опрос по теме «*Способы измерения информации» *Устный опрос по теме «*Вероятностный подход к измерению информации» Проверочная работа (тест) по теме «Базовые понятие теории информации» Практическая работа «Способы хранения обработки и передачи информации» Практическая работа «Измерение количества информации»	*Информация в материальном мире, информация в живой природе, информация в человеческом обществе, информация в науке, классификация информации.* *Дисперсия случайной величины*	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10,, 31, 32, 33, 34	Экзамен	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10,, 31, 32, 33, 34
Раздел 2. Информация и энтропия	*Устный опрос по теме «*Теорема отсчетов» *Устный опрос по теме «*Понятие энтропии.	*Математическая модель системы передачи информации b-арная*	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09,	Экзамен	ОК 01, ОК 02, ОК

	Виды энтропии» *Устный опрос по теме «*Смысл энтропии Шеннона» Практическая работа «Применение теоремы отчетов» Практическая работа «Определение пропускной способности канала» Практическая работа «Интерполяционная формула Уиттекера-Шеннона, частота Найквиста» Практическая работа «Поиск энтропии случайных величин» Практическая работа «Энтропийное кодирование» Практическая работа «Дифференциальная энтропия» Практическая работа «Расчет вероятностей. Составление закона распределения вероятностей»	*энтропия, взаимная энтропия Закон аддитивности информации*	ОК 10, У1, У2, У3, З3, З4, З5		04, ОК 05, ОК 09, ОК 10, У1, У2, У3, З3, З4, З5
Раздел 3. Защиты и передача информации	*Устный опрос по теме «*Сжатие информации» Тест на тему «Сжатие информации» *Устный опрос по теме «*Кодирование» Тест «Кодирование информации» Практическая работа «ПУ кодирование» Практическая работа «Адаптивное	*Применение алгоритмов кодирования в архиваторах для обеспечения продуктивной работы в WINDOWS Дельта-кодирование*	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, З5, У3	Экзамен	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, З5, У3

	арифметическое кодирование. Дельта-кодирование» Практическая работа «Цифровое кодирование и аналоговое кодирование. Таблично-символьное кодирование»				
Раздел 4. Основы теории защиты информации	*Устный опрос по теме «*Стандарты шифрования данных. Криптография» *Тест по теме* «Криптография» Практическая работа «Практическое применение криптографии. Изучение и сравнительный анализ методов шифрования» Практическая работа «Криптография с симметричным ключом, с открытым ключом» Практическая работа «Шифрование с использованием перестановок» Практическая работа «Шифрование с использованием замен» Практическая работа «Практическое применение различных алгоритмов сжатия. Сравнение и анализ архиваторов. Кодирование Хаффмана»	*Различные методы шифрования*	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, У3, З5, З6, З7	Экзамен	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, У3, З5, З6, З7

3.2. Задания для оценки освоения учебной дисциплины

РАЗДЕЛ 1. БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

УСТНЫЙ ОПРОС ПО ТЕМЕ

«ФОРМАЛЬНОЕ ПРЕДСТАВЛЕНИЕ ЗНАНИЙ. ВИДЫ ИНФОРМАЦИИ»

Вопросы:

1. Понятие теории информации.
2. Формальное представление данных.
3. Виды информации.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

УСТНЫЙ ОПРОС ПО ТЕМЕ

«СПОСОБЫ ИЗМЕРЕНИЯ ИНФОРМАЦИИ»

Вопросы:

1. Базовые понятия теории информации.
2. Способы измерения информации.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

УСТНЫЙ ОПРОС ПО ТЕМЕ

«ВЕРОЯТНОСТНЫЙ ПОДХОД К ИЗМЕРЕНИЮ ИНФОРМАЦИИ»

Вопросы:

1. Вероятностный подход к измерению информации.
2. Решение упражнений по данной теме.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРОВЕРОЧНАЯ РАБОТА (ТЕСТ) ПО ТЕМЕ
«БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ»

Вариант 1

Выберите правильный вариант ответа:

1) Информацию, изложенную на доступном для получателя языке, называют…

   а) понятной;

b) актуальной;
c) достоверной;
d) полной.

2) Наибольший объем информации человек получает при помощи…
a) вкусовых рецепторов;
b) органов осязания;
c) органов зрения;
d) органов слуха;
e) органов обоняния.

3) К формальным языкам можно отнести…
a) язык программирования;
b) русский язык;
c) китайский язык;
d) язык жестов.

4) Материальный объект, предназначенный для хранения информации, называется…
a) носитель информации;
b) получатель информации;
c) хранитель информации;
d) канал связи.

5) Сообщение, уменьшающее неопределенность знаний в два раза, несет…
a) 1 бит;
b) 4 бита;
c) 1 байт;
d) 2 бита.

6) Алфавит языка состоит из 16 знаков. Сколько информации несет сообщениедлиной 32 символа?
a) 16 бит;
b) 128 бит;
c) 256 бит;
d) 80 бит.

7) Сколько байт в словах «информационные технологии» (без учета кавычек)?
a) 24 байта;
b) 192 байт;
c) 25 байт;
d) 2 байта.

8) Сколько байт в 4 Мбайт?a)
4000;
b) 2^{22};
c) 2^{12};
d) 4^{20}.

9) В какой из последовательностей единицы измерения указаны в порядке возрастания
   a) мегабайт, килобайт, байт, гигабайт;
   b) байт, килобайт, мегабайт, гигабайт;
   c) гигабайт, килобайт, мегабайт, байт;
   d) гигабайт, мегабайт, килобайт, байт.

10) Процесс представления информации (сообщения) в виде кода называется…
   a) декодированием;
   b) дешифрованием;
   c) кодированием;
   d) дискретизацией.

11) Является ли верным утверждение: "В позиционной системе счисления количественный эквивалент цифры зависит от места цифры в записи числа"?
   a) да;
   b) нет.

12) Алфавит системы счисления 0, 1, 2, 3, 4, 5. Какая это система счисления?
   a) шестеричная;
   b) пятеричная;
   c) восьмеричная;
   d) римская.

13) Двоичное число 1001_2 соответствует десятичному числу…a) 1001_{10};
   b) 6_{10};
   c) 9_{10};
   d) 8_{10}.

14) Найти двоичный эквивалент числа X, представленного в десятичной системе счисления,
   если X = 5.
   a) 110_2;
   b) 101_2;
   c) 1001_2;
   d) 11_2.

15) Укажите самое большое число.
   a) 144_{16};
   b) 144_{10};
   c) 144_6;
   d) 144_8.

16) Какое число лишнее?a) 11111111_2;
   b) 377_8;
   c) FF_{16};
   d) 226_{10}.

17) Сложите числа $5A_{16}+43_8+111_2+5_{10}$, результат получите в двоичной системе счисления.
   a) 11110001_2;
   b) 10000011_2;
   c) 10001001_2;
   d) 10011101_2.

18) Пусть небольшая книжка, сделанная с помощью компьютера, содержит 15 страниц; на каждой странице — 40 строк, в каждой строке — 60 символов. Сколько информации она содержит?
   a) 36000 байт;
   b) 19200 байт;
   c) 256 бит;
   d) 2400 байт

19) Изображение представляющее собой совокупность точек (пикселей) разных цветов называется…
   a) векторным;
   b) цветным;
   c) аналоговым;
   d) растровым.

20) Многопроходная линия для информационного обмена между устройствами компьютера называется…
   a) модемом;
   b) контроллером;
   c) магистралью;
   d) провайдером.

21) Устройством вода информации является…
   a) сканер;
   b) дисковод;
   c) принтер;
   d) клавиатура.

22) Комплекс взаимосвязанных программ, обеспечивающий пользователю удобный способ общения с программами, называется…
   a) утилитой;
   b) драйвером;
   c) интерпретатором;
   d) интерфейсом.

23) Расширение имени файла характеризует…
   a) время создания файла;
   b) тип информации, содержащейся в файле;
   c) объем файла;
   d) место, занимаемое файлом на диске.

24) Архивный файл представляет собой…
   a) файл, которым долго не пользовались;
   b) файл, защищенный от несанкционированного доступа;
   c) файл, защищенный от копирования;

d) файл, сжатый с помощью архиватора.

25) По среде обитания компьютерные вирусы классифицируют на…
a) неопасные, опасные и очень опасные;
b) паразиты, репликаторы, невидимки, мутанты, троянские;
c) сетевые, файловые, загрузочные, макровирусы.

26) К антивирусным программам не относятся…
a) интерпретаторы;
b) фаги;
c) ревизоры;
d) сторожа.

27) В каком году появилась первая ЭВМ?
a) 1823;
b) 1951;
c) 1980;
d) 1905.

28) На какой электронной основе созданы ЭВМ I поколения?
a) транзисторы;
b) электронно-вакуумные лампы;
c) зубчатые колеса;
d) реле.

Вариант 2

Выберите правильный вариант ответа:

1) Информацию, отражающую истинное положение вещей, называют…
a) актуальной;
b) понятной;
c) полезной;
d) достоверной.

2) Тактильную информацию человек получает посредством…
a) специальных приборов;
b) органов слуха;
c) термометра;
d) органов осязания.

3) К естественным языкам можно отнести…
a) язык программирования;
b) английский язык;
c) язык математики;
d) язык химических формул.

4) Информация в компьютере хранится, передается и обрабатывается в виде…
a) знаков и импульсов;
b) сигналов и импульсов;
c) импульсов;
d) символов.

5) Если сообщение несет 1 бит информации, то оно уменьшает неопределенность знаний…

a) в два раза;
b) в один раз;
c) в три раза;
d) на 8 бит.

6) В зоопарке 64 клетки, тигр сидит в клетке номер 16. Сколько информации несет это сообщение?

a) 16 бит;
b) 256 бит;
c) 6 бит;
d) 64 бита.

7) Сколько байт в словосочетании «Системы счисления» (без учета кавычек)?

a) 17 байт;
b) 2 бита;
c) 8 бит;
d) 136 бит.

8) 1 Кбайт =?

a) 1024 байт;
b) 2^{10} бит;
c) 2^{30} байт;
d) 1000 бит.

9) В какой из последовательностей единицы измерения указаны в порядке убывания.

a) гигабайт, мегабайт, килобайт, байт;
b) мегабайт, килобайт, байт, гигабайт;
c) гигабайт, килобайт, мегабайт, байт;
d) байт, килобайт, мегабайт, гигабайт.

10) Процесс преобразования кода к форме исходной символьной системы, т.е. получение исходного сообщения называется…

a) декодированием;
b) кодированием;
c) шифрованием;
d) дискретизацией.

11) Для какого класса систем счисления выполняется условие: количественный эквивалент цифры не зависит от места цифры в записи числа?

a) для позиционного;
b) для непозиционного.

12) Алфавит системы счисления 0, 1, 2, 3, 4, 5, 6. Какая это система счисления?

a) восьмеричная;
b) семеричная;
c) римская;
d) шестеричная.

13) Двоичное число 1100_2 соответствует десятичному числу…
   a) 11_{10};
   b) 12_{10};
   c) 9_{10};
   d) 1100_{10}.

14) Найти двоичный эквивалент числа X, представленного в десятичной системе счисления,
   если X = 6.
   a) 111;
   b) 11;
   c) 011;
   d) 110.

15) Укажите самое маленькое число.
   a) 144_{16}
   e) 144_{10}
   f) 144_6
   g) 144_8

16) Какое число лишнее?
   a) 10101111_2
   b) 256_8
   c) AF_{16}
   d) 175_{10}

17) Сложите числа $A5_{16}+23_8+101_2+10_{10}$, результат получите в двоичной системе счисления.
   a) 11000111;
   b) 11101000;
   c) 10000001;
   d) 10000011.

18) Сколько информации содержит лист текста, сделанный с помощью компьютера, если на странице — 30 строк, в каждой строке — 50 символов?
   a) 16 Кбит;
   b) 256 бит;
   c) 1500 бит;
   d) 12000 бит.

19) Минимальный участок изображения, цвет которого можно задать независимым образом называется…
   a) бит;
   b) пиксель;
   c) примитив;
   d) растр.

20) Во время исполнения прикладная программа хранится…
   a) в видеопамяти;
   b) в процессоре;
   c) на жестком диске;
   d) в оперативной памяти.

21) Устройство для подключения компьютера к сети Интернет, называется…
   a) модем;
   b) факс;
   c) плоттер;
   d) браузер.

22) Программа, позволяющая управлять внешним устройством компьютера, называется …
   a) браузером;
   b) драйвером;
   c) операционная система;
   d) система программирования.

23) Исполняемые файлы имеют расширение…
   a) doc, txt;
   b) txt, sys;
   c) sys, exe;
   d) com, exe.

24) Программа для уменьшения информационного объема (сжатия) файлов, называется …
   a) утилитой;
   b) драйвером;
   c) архиватором;
   d) компилятором.

25) Компьютерные программы-вирусы…
   a) возникают в результате сбоев в аппаратных средствах компьютерах;
   b) пишутся специально для нанесения ущерба пользователям ПК;
   c) имеют биологическое происхождение;
   d) являются следствием ошибок в операционной системе.

26) Вирусы поражающие загрузочные секторы дисков, называются…
   a) загрузчиками;
   b) файловыми;
   c) загрузочными;
   d) сетевыми.

27) Кого называют первой в истории женщиной-программистом:
   a) Софью Ковалевскую;
   b) Марию Склодовскую-Кюри;
   c) Аду Лавлейс.

28) Сколько поколений ЭВМ принято считать созданными до нашего времени?
   a) три;
   b) четыре;
   c) шесть;
   d) два.

Вариант 3

Выберите правильный вариант ответа:

29) Информацию, существенную и важную в настоящий момент, называют:
   a) понятной;
   b) полезной;
   c) достоверной;
   d) актуальной.

30) По форме представления информация подразделяется на…
   a) книжную, газетную, компьютерную;
   b) текстовую, числовую, графическую, звуковую;
   c) тактильную, вкусовую, обонятельную, осязательную, визуальную, звуковую;
   d) массовую, личную, специальную.

31) В общей схеме передачи информации между источником и приемником информации должен существовать…
   a) канал связи;
   b) электрическое поле;
   c) воздух;
   d) линия связи.

32) Книги, картины, дискеты позволяют информацию в основном…
   a) передавать и обрабатывать;
   b) обрабатывать и хранить;
   c) хранить и передавать;
   d) запоминать.

33) Если сообщение несет 2 бита информации, то оно уменьшает неопределенность знаний…
   a) в два раза;
   b) в четыре раза;
   c) в три раза;
   d) на 8 бит.

34) В доме 32 квартиры, день рождения справляют в квартире номер 10. Сколько информации несет это сообщение?
   a) 10 байт;
   b) 5 бит;
   c) 64 бита;
   d) 4 бита.

35) Сколько байт в словосочетании «Тактильная информация» (без учета кавычек)?
   a) 25 байт;
   b) 5 байт;
   c) 21 байт;
   d) 2 байта.

36) 1 Гбайт =?
   a) 1024 байт;
   b) 2^{10} бит;
   c) 2^{30} байт;

d) 10000 бит.

37) Минимальной единицей измерения информации является…
a) 1 гигабайт;
b) 1 бод;
c) 1 байт;
d) 1 бит.

38) Сигнал, принимающий лишь конечное число значений, называется…
a) аналоговым;
b) частично дискретный;
c) дискретны;
d) частично аналоговый.

39) В какой системе счисления представлена информация, хранящаяся в компьютере?
a) в троичной;
b) в десятичной;
c) в двоичной;
d) в римской.

40) Какое количество цифр используется в восьмеричной системе счисления?
a) 10;
b) 8;
c) 2;
d) 7.

41) Двоичное число 101_2 соответствует десятичному числу
a) 6_{10};
b) 10_{10};
c) 101_{10};
d) 5_{10}.

42) Найдите двоичный эквивалент числа X, представленного в десятичной системе счисления, если X=8.
a) 1000;
b) 1001;
c) 1010;
d) 1110.

43) Укажите самое маленькое число.
a) 111_{16}
h) 111_{10}
i) 111_6
j) 111_8

44) Какое число лишнее?
a) 10101_2
b) 26_8
c) 15_{16}
d) 21_{10}

45) Сложите числа $A9_{16}+15_8+110_2+11_{10}$, результат получите в двоичной системе счисления.
   a) 11001000;
   b) 11111110;
   c) 10000001;
   d) 11100100.

46) Сколько информации содержит лист текста, сделанный с помощью компьютера, если на странице — 30 строк, в каждой строке — 40 символов?
   a) 16 Кбит;
   b) 9600 бит;
   c) 1200 бит;
   d) 256бит.

47) Какие изображения формируются из графических примитивов (линий, окружностей, прямоугольников и т.д.)
   a) векторные;
   b) растровые.

48) К внешним запоминающим устройствам относится…
   a) процессор;
   b) монитор;
   c) CD-диск;
   d) клавиатура.

49) Укажите устройства ввода.
   a) принтер, клавиатура, джойстик;
   b) графический планшет, клавиатура, сканер;
   c) мышь, световое перо, винчестер;
   d) телефакс, модем, принтер.

50) Совокупность программ, обеспечивающих совместное функционирование всех устройств компьютера и предоставляющих пользователю доступ к ресурсам компьютера, называется…
   a) утилитой;
   b) драйвером;
   c) операционной системой;
   d) интерфейсом.

51) Укажите тип файлов со следующими расширениями: *.txt, *.doc.
   a) исполнимые файлы;
   b) графические файлы;
   c) текстовые файлы.
   d) звуковые файлы.

52) Архивный файл отличается от исходного файла тем, что…
   a) доступ к нему занимает меньше времени;
   b) легче защищать от вирусов;
   c) более удобен для редактирования;
   d) занимает меньше места на диске.

53) Отличительными особенностями компьютерного вируса являются…
   a) легкость распознавания и уничтожения;
   b) способность к самокопированию и самостоятельному запуску;
   c) значительный объем программного кода;
   d) трудность распознавания и уничтожения.

54) Вирус, заражение которым может произойти при работе с электронной почтой, называется…
   a) файловым;
   b) макровирусом;
   c) сетевым;
   d) загрузочные.

55) Когда был создан первый арифмометр – механическое счетное устройство?
   a) в XIX веке;
   b) в XX веке;
   c) в XIV веке.

56) Электронной базой ЭВМ III поколения является…
   a) транзисторы;
   b) БИС;
   c) электронно-вакуумные лампы;
   d) интегральные схемы.

Вариант 4

Выберите правильный вариант ответа:

29) Информацию, не зависящую от личного мнения или суждения, называют:
   a) объективной;
   b) актуальной;
   c) достоверной;
   d) понятной.

30) Визуальной называют информацию, которая воспринимается человеком посредством…
   a) вкусовых рецепторов;
   b) органов осязания;
   c) органов зрения;
   d) органов слуха;
   e) органов обоняния.

31) Язык программирования относится к…
   a) формальным языкам;
   b) естественным языкам.

32) Носителем графической информации не может являться…
   a) дискета;
   b) грампластинка;
   c) холст;
   d) бумага.

33) Сообщение, уменьшающее неопределенность знаний в 4 раза, несет

a) 2 бита информации;
b) 4 бита информации;
c) 16 бит информации;
d) 1 байт информации.

34) Алфавит языка состоит из 32 знака. Сколько информации несет сообщение длиной 16 символа?
a) 16 бит;
b) 128 бит;
c) 256 бит;
d) 80 бит.

35) Сколько бит в слове «моделирование» (без учета кавычек)?
a) 13 бит;
b) 104 бит;
c) 12 бит;
d) 2 бита.

36) Сколько бит в 1 Кбайте?
a) 1024;
b) 2^{13} ;
c) 1000;
d) 2^{10} .

37) В какой из последовательностей единицы измерения указаны в порядке возрастания
a) мегабайт, килобайт, байт, гигабайт;
b) байт, килобайт, мегабайт, гигабайт;
c) гигабайт, килобайт, мегабайт, байт;
d) гигабайт, мегабайт, килобайт, байт.

38) Преобразование непрерывных изображений и звука в набор дискретных значений в форме кодов называют…
a) декодированием;
b) дешифрованием;
c) кодированием;
d) дискретизацией.

39) Система счисления - это ...
a) совокупность цифр;
b) совокупность цифр 0, 1;
c) совокупность цифр I, V, X, L, C, D, M;
d) способ записи чисел с помощью заданного набора специальных знаков (цифр).

40) Какое количество цифр используется в шестнадцатеричной системе счисления?
a) 16;
b) 15;
c) 6;
d) 8.

41) Двоичное число 1101_2 соответствует десятичному числу

a) 1101_{10};
b) 13_{10};
c) 10_{10};
d) 8_{10}.

42) Найти двоичный эквивалент числа X, представленного в десятичной системе счисления,
если X = 7.
a) 110;
b) 101;
c) 111;
d) 1001.

43) Укажите самое большое число.
a) 25_{16}
b) 25_{10}
c) 25_{6}
d) 25_{8}

44) Какое число лишнее?
a) 10101001_{2}
b) 253_{8}
c) AB_{16}
d) 171_{10}

45) Сложите числа $A4_{16}+36_{8}+110_{2}+10_{10}$, результат получите в двоичной системе счисления.
a) 11110011;
b) 11010010;
c) 10010010;
d) 11000110.

46) Пусть небольшая книжка, сделанная с помощью компьютера, содержит 5 страниц; на каждой странице — 120 строк, в каждой строке — 60 символов. Сколько информации она содержит?
a) 36000 байт;
b) 19200 байт;
c) 256 бит;
d) 2400 байт

47) Количество информации, которое используется для кодирования цвета точки изображения, называется…
a) палитрой;
b) разрешающей способностью;
c) глубиной цвета;
d) дискретизацией.

48) Системный диск необходим для…
a) хранения архивных файлов;
b) систематизации файлов;
c) лечения компьютера от вирусов;
d) загрузки операционной системы.

49) Дисковод – это устройство, предназначенное для …

a) чтения/записи данных с внешнего носителя.
b) хранения компакт-дисков;
c) долговременного хранения информации;
d) вывода информации на внешний носитель;

50) Процесс, в результате которого файлы записываются в секторы, последовательно идущие друг за другом, называется…
a) дефрагментацией;
b) форматированием;
c) архивацией;
d) копированием.

51) Порядок хранения файлов на диске определяется используемой …
a) операционной системой;
b) файловой системой.

52) Укажите расширение для архивных файлов.
a) *.rar, *.zip;
b) *.bmp, ipg;
c) mp3, wav.

53) Заражение компьютерным вирусом может произойти в процессе…
a) печати на принтере;
b) работы с файлами;
c) форматирования дискеты;
d) при выключении компьютера.

54) Какие типы файлов может заразить макровирус?
a) графические файлы;
b) звуковые и видеофайлы;
c) текстовые файлы с расширением doc.

55) На какой электронной основе созданы ЭВМ II поколения?
a) транзисторы;
b) электронно-вакуумные лампы;
c) реле;
d) БИС.

56) Какой фирмой и в каком году были созданы первые персональные компьютеры?
a) IBM в 1991 году;
b) Apple в 1982 году;
c) IBM в 1982 году;
d) Apple в 1990 году.

Ответы к тестовым заданиям. I вариант.

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
a	c	a	a	a	b	c	b	b	c	a	a	c	b
15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.
a	d	c	a	d	c	d	d	b	d	c	a	b	b

Ответы к тестовым заданиям. II вариант.

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
d	d	b	c	a	c	a	a	a	b	b	b	b	d
15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.
b	b	a	d	b	d	a	b	d	c	b	c	c	b

Ответы к тестовым заданиям. III вариант.

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
d	b	a	c	b	b	c	c	d	c	c	b	d	a
15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.
b	b	a	b	a	c	b	c	c	d	b	c	a	d

Ответы к тестовым заданиям. IV вариант.

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
a	c	a	b	c	d	b	b	b	d	d	a	b	c
15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.
a	d	b	a	c	d	a	a	b	a	b	c	a	c

Критерии оценивания теста:

5 (отлично) – правильно выполнены 27-28 заданий.

4 (хорошо) – правильно выполнены 21-26 задания.

3 (удовлетворительно) – правильно выполнены 15-20 заданий.

2 (неудовлетворительно) – правильно выполнены менее 15 заданий.

ПРАКТИЧЕСКАЯ РАБОТА

«ИЗМЕРЕНИЕ КОЛИЧЕСТВА ИНФОРМАЦИИ».

1 ВАРИАНТ

Задание №1. Заполните ячейки числами:

1	5 Кбайт =		байт	=		бит
2	12 Кбайт =		байт	=		бит
3	107 Гбайт=		Мбайт	=		Кбайт

Задание № 2. Решите следующие задачи

1 Сообщение занимает 3 страницы по 25 строк. В каждой строке записано по 60 символов. Сколько символов в использованном алфавите, если всё сообщение занимает 1125 байтов?
Ответ: [ ] символов

2 Для записи сообщения использовалась кодировка Unicode. На одной странице 60 строк. В каждой строке по 35 символов. Каков информационный объем одной страницы?
Ответ: [ ] байта

3 Емкость одной дискеты размером 3,5" 1, 44 Мб. Лазерный диск может содержать 650 Мб информации. Определите сколько дискет потребуется, чтобы разместить информацию с одного разерного диска?
Ответ: [ ] дискет(-а)

2 ВАРИАНТ

Задание №1. Заполните ячейки числами:

1 ____ Кбайт = ____ байт = 12288 бит

2 6 Кбайт = ____ байт

3 5242880 Кб= ____ Гбайт

Задание № 2. Решите следующие задачи

1 Для передачи сообщения использовалась кодировка Unicode (N=65536). В сообщении 10 страниц, на каждой из которых 30 строк по 60 символов. Сколько килобайтов содержит сообщение?

Ответ: ____ Килобайт *(ответ округлите до двух знаков после запятой)*

2 Какова мощность алфавита, если информационное сообщение объемом 2 Кб содержит 2048 символов?

Ответ: ____ символов

3 Измерьте информационный объем сообщения (без учета кавычек) в битах, байтах и КБ, записанного символами компьютерного алфавита: "Ура! Сегодня будет урок информатики!"

Ответ: ____ бит
____ байт
____ Кбайт *(ответ округлите до двух знаков после запятой)*

3 ВАРИАНТ

Задание №1. Заполните ячейки числами:

1 ____ Кбайт = ____ байт = 8192 бит

2 ____ Гбайт = 1536 Мб = ____ Кбайт

3 94 Мбайта = ____ Кбайт

Задание № 2. Решите следующие задачи

1 Для записи сообщения использовалась кодировка Unicode. На одной странице 60 строк. В каждой строке по 35 символов. Каков информационный объем одной страницы?

Ответ: _____ байта

2 Измерьте информационный объем сообщения (без учета кавычек) в битах, байтах и КБ, записанного символами компьютерного алфавита: "Ура! Сегодня будет урок информатики!"

Ответ: _____ бит
_____ байт
_____ Кбайт *(ответ округлите до двух знаков после запятой)*

3 Емкость одной дискеты размером 3,5" 1, 44 Мб. Лазерный диск может содержать 650 Мб информации. Определите сколько дискет потребуется, чтобы разместить информацию с одного разерного диска?

Ответ: _____ дискет(-а)

Критерии оценки практической работы:

5 (отлично) – правильно решены все 6 задач.

4 (хорошо) – не правильно решены 1 задача из 1 задания или 1 задача из 2 задания.

3 (удовлетворительно) – неправильно решены 2 задачи.

2 (неудовлетворительно) – неправильно решено более 3 задач.

ОТВЕТЫ:

Задание №1. Заполните ячейки числами:

5 Кбайт = 5120 байт = 40960 бит

1,5 Кбайт = 1536 байт = 12288 бит

1 Кбайт = 1024 байт = 8192 бит

1,5 Гбайт = 1536 Мб = 1572864 Кбайт

12 Кбайт =	12288	байт	=	98304	бит
6 Кбайт =	6144	байт			
94 Мбайта =	96256	Кбайт			
107 Гбайт=	109568	Мбайт	=	112197632	Кбайт
5242880 Кб=	5	Гбайт			

Задание № 2. Решите следующие задачи

Для передачи сообщения использовалась кодировка Unicode (N=65536). В сообщении 10 страниц, на каждой из которых 30 строк по 60 символов. Сколько килобайтов содержит сообщение?

Ответ: 35,16 Килобайт (Ответ округлите до двух знаков после запятой)

Сообщение занимает 3 страницы по 25 строк. В каждой строке записано по 60 символов. Сколько символов в использованном алфавите, если всё сообщение занимает 1125 байтов?

Ответ: 4 символов

Для записи сообщения использовалась кодировка Unicode. На одной странице 60 строк. В каждой строке по 35 символов. Каков информационный объем одной страницы?

Ответ: 4200 байта

Какова мощность алфавита, если информационное сообщение объемом 2 Кб содержит 2048 символов?

Ответ: 256 символов

Измерьте информационный объем сообщения (без учета кавычек) в битах, байтах и КБ, записанного символами компьютерного алфавита: "Ура! Сегодня будет урок информатики!"

Ответ: 288 бит
36 байт
0,04 Кбайт *(округлите до двух знаков после запятой)*

Емкость одной дискеты размером 3,5" 1, 44 Мб. Лазерный диск может содержать 650 Мб информации. Определите сколько дискет потребуется, чтобы разместить информацию с одного разерного диска?

Ответ: 451 дискет(-а)

ПРАКТИЧЕСКАЯ РАБОТА

«СПОСОБЫ ХРАНЕНИЯ ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ»

Цель: научиться сохранять, обрабатывать и передавать данные при помощи технических средств информации.

Время выполнения: 2 часа

Оборудование: ПК, сканер, фотоаппарат, микрофон, диск.

Раздаточный материал: инструкционно – технологическая карта для сканирования фотографии.

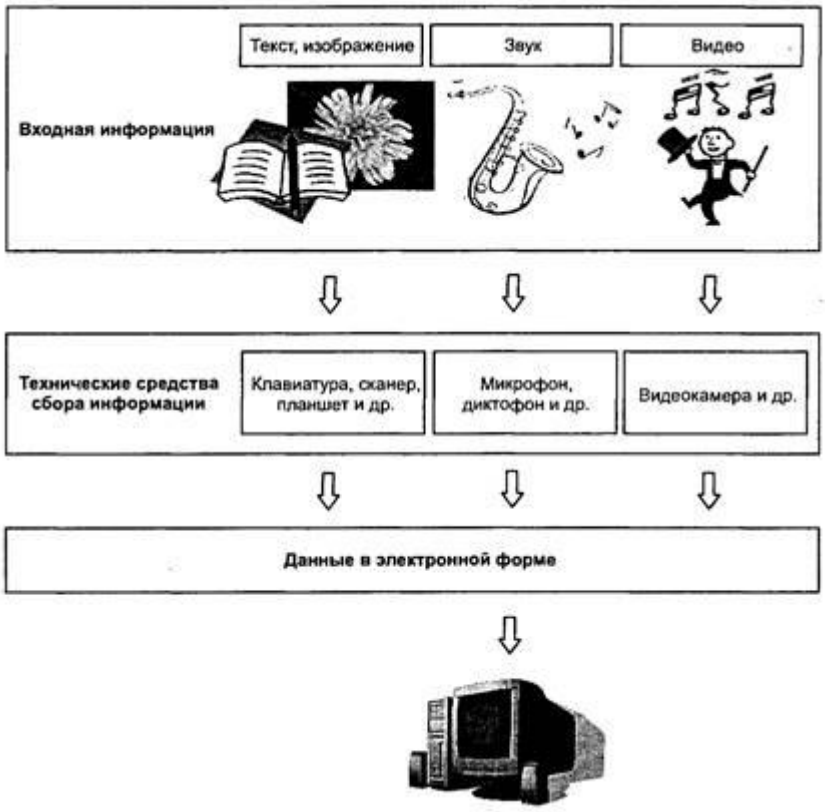
Программное обеспечение: операционная система, программа для работы с видеоинформацией.

Теоретические основы

1. Технологии сбора и хранения информации

Сбор предполагает получение максимально выверенной исходной информации и является одним из самых ответственных этапов в работе с информацией, поскольку от цели сбора и методов последующей обработки полностью зависит конечный результат работы всей информационной системы.

Технология сбора подразумевает использование определенных методов сбора информации и технических средств, выбираемых в зависимости от вида информации и применяемых методов ее сбора. На заключительном этапе сбора, когда информация преобразуется в данные, т. е. в информацию, представленную в формализованном виде, пригодном для компьютерной обработки, осуществляется ее ввод в систему Для сбора данных необходимо сначала определить технические средства, позволяющие осуществлять сбор быстро и высококачественно и поддерживающие операции ввода информации и представления данных в электронной форме.



2. Технологический процесс обработки информации

Технологический процесс обработки информации — есть строго определенная последовательность взаимосвязанных процедур, выполняемых для преобразования первичной информации с момента ее возникновения до получения требуемого результата.

Технологический процесс призван автоматизировать обработку исходной информации за счет привлечения технических средств базовой информационной технологии, сократить финансовые и трудовые затраты, обеспечить высокую степень достоверности результатной информации. Для конкретной задачи той или иной предметной области технологический процесс обработки информации разрабатывается индивидуально. Совокупность процедур зависит от следующих факторов:

- характер и сложность решаемой задачи;
- алгоритм преобразования информации;
- используемые технические средства;
- сроки обработки данных;
- используемые системы контроля;
- число пользователей и т. д.

В общем случае технологический процесс обработки информации включает процедуры.

3. Способы обработки информации

Современные информационные технологии позволяют обрабатывать информацию централизованным и децентрализованным (т. е. распределенным) способами.

Централизованный способ предполагает сосредоточение данных в информационно-вычислительном центре, выполняющем все основные действия технологического процесса обработки информации. Основное достоинство централизованного способа — сравнительная дешевизна обработки больших объемов информации за счет повышения загрузки вычислительных средств.

Децентрализованный способ характеризуется рассредоточением информационно-вычислительных ресурсов и распределением технологического процесса обработки информации по местам возникновения и потребления информации. Достоинством децентрализованного способа является повышение оперативности обработки информации и решения поставленных задач за счет автоматизации деятельности на конкретных рабочих местах, применения надежных средств передачи информации, организации сбора первичных документов и ввода исходных данных в местах их возникновения.

Децентрализованный способ обработки информации может быть реализован автономным или сетевым методом. При автономной обработке информации передача документов и данных на электронных носителях осуществляется по почте либо курьером, а при сетевой — через современные каналы связи.

На практике применяют смешанный способ обработки информации, для которого характерны признаки двух способов одновременно (централизованный с частичной децентрализацией или децентрализованный с частичной централизацией).

4. Режимы обработки информации на компьютере

Вычислительные средства участвуют в процессе обработки информации в двух основных режимах: пакетном или диалоговом.

В случае, когда технология обработки информации на компьютере представляет собой заранее определенную последовательность операций, не требующую вмешательства человека, и диалог с пользователем отсутствует, информация

обрабатывается в так называемом пакетном режиме. Суть его состоит в том, что программы обработки данных последовательно выполняются под управлением операционной системы как совокупность (пакет) заданий. Операционная система обеспечивает ввод данных, вызов требуемых программ, включение необходимых внешних устройств, координацию и управление технологическим процессом обработки информации.

Задачи, решаемые в пакетном режиме, характеризуются следующими свойствами:

- алгоритм решения задачи формализован, вмешательства пользователя не требуется;
- наличие большого объема входных и выходных данных, в основном хранящихся на устройствах хранения информации (например, жестких дисках компьютеров);
- расчет выполняется для большинства записей входных файлов;
- длительное время решения задачи — как правило, обусловлено большими объемами обрабатываемых данных;
- регламентность — задачи решаются с заданной периодичностью.

Пакетный режим возник первым и широко использовался с середины XX в., когда обработка информации на ЭВМ осуществлялась в специально создаваемых вычислительных центрах. Заказчики подготавливали исходные данные (обычно на перфокартах или перфолентах) и отправляли их в вычислительный центр, где данные обрабатывались и результаты обработки возвращались заказчику. С развитием персональных ЭВМ (начиная с 80-х гг. прошлого века) обработка данных стала осуществляться, в основном, непосредственно потребителями, поэтому в настоящее время пакетный режим используется достаточно редко. Сегодня более распространен диалоговый режим, когда необходимо непосредственное взаимодействие пользователя с компьютером и на каждое свое действие пользователь получает немедленные ответные действия компьютера. Диалоговый режим позволяет пользователю интерактивно управлять порядком обработки информации и получать результатные данные в виде необходимых документов либо файлов.

5. Технологии передачи и представления информации

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.

В современных цифровых системах связи функции передатчика и приемника выполняет модем. 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.

Воспроизведение информации — это процесс, при котором ранее записанная на носителе информация считывается устройством воспроизведения.

Отображение информации — есть представление информации, т. е. генерация сигналов на основе исходных данных, а также правил и алгоритмов их преобразования в форме, приемлемой для непосредственного восприятия человеком.

Потребителем информации наиболее часто выступает человек, и для принятия решений ему необходимы результаты обработки информации. Тем не менее человек не способен ощутить машинное представление информации, а может воспринимать ее лишь органами чувств (органами зрения, слуха, осязания, обоняния и т. д.), поэтому для организации взаимодействия человека с информационными моделями объектов информационная система должна быть наделена специальными средствами отображения данных.

Поскольку зрение используется для восприятия информации наиболее активно, то средства отображения в современных ИС должны представлять информацию в лучшей форме для визуального наблюдения. Заметим, что мультимедиа-системы позволяют также представлять информацию в форме аудио- и видеосигналов, однако для управленческих информационных систем наиболее характерно отображение информации в текстовой и графической форме, что осуществляется за счет использования мониторов и печатающих устройств (например, принтеров, плоттеров).

Прежде чем, например, на мониторе, появится информация в доступной для человека форме, компьютером будет автоматически осуществлена следующая последовательность операций:

- преобразование данных, представленных в машинной форме, в вид, приемлемый для экранного отображения;
- согласование формы представления данных с параметрами монитора;
- воспроизведение в соответствии с возможностями воспроизводящего устройства (т. е. в данном примере — монитора).

6.Инструкционно-технологическая карта для сканирования фотографий

Перед началом работы положите фотографию на стекло сканера, лицом вниз. Для того чтобы отсканировать фотографию воспользуйтесь «Мастером работы со сканером» или используйте программное обеспечение поставляемое производителем вашего сканера. Мы рассмотрим пример сканирования фотографии посредством «Мастера работы со сканером».

Для запуска мастера войдите в меню Пуск → Настройки → Панель управления → Сканеры и камеры → Выберите модель вашего сканера и нажмите дважды. В появившемся окне (см. рис.1) выберите «Особые параметры» и нажмите кнопку «Настроить»

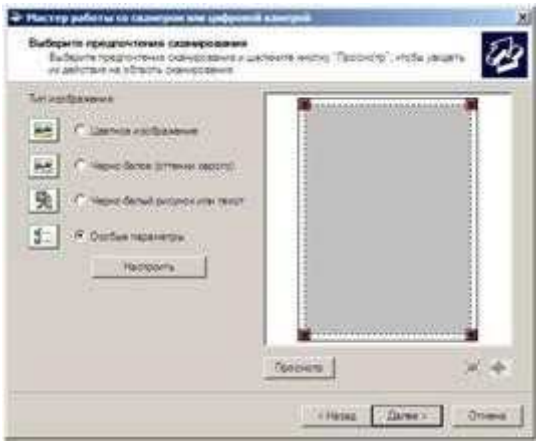


Рисунок 1

Рисунок 2

В появившемся окне (см. рис. 2) выберите «Разрешение (DPI)» - 300, «Тип изображения» - Цветной снимок и нажмите кнопку ОК, вы попадете в предыдущее меню в котором необходимо нажать кнопку «Просмотр» (см. рис. 1) У вас на экране появится предварительный просмотр изображения с вашего сканера (см.рис. 3)

Рисунок 3

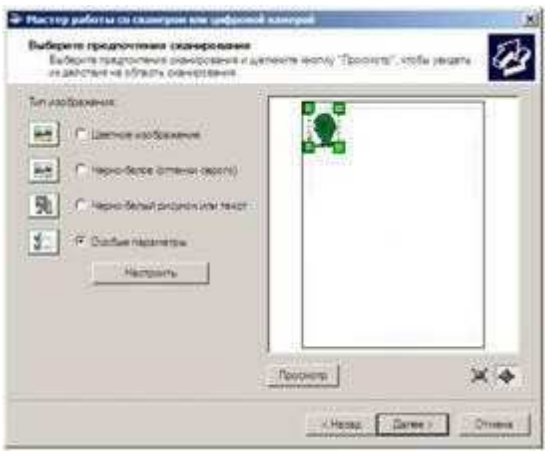


Рисунок 4

Для того чтобы отсканировать фотографию правильно необходимо выбрать область

сканирования (выделена пунктирной линией) как показано на рис. 4, в противном случае сканер кроме фотографии туриста отсканирует также и всю плоскость стекла, в результате чего в визе туриста вместо фотографии будет напечатан белый лист, такая визу будет считаться недействительной!

После того как вы выбрали область сканирования нажмите кнопку «Далее», в появившемся окне укажите название файла, выберите формат файла JPG и укажите папку для сохранения фотографии, после чего нажмите кнопку «Далее».

Порядок выполнения работы

1. Создание досье группы. Заранее заготовить материал: фотографии, текст.
2. Сфотографировать своих однокурсников.
3. Включить компьютер.
4. Создать общую папку на сервере.
5. Сканировать фотографии и сохранить в общую папку.
6. Включить текстовый редактор. Создать титульный лист с общей фотографией и названием группы: специальность и год.
7. Оформить каждый лист на одного человека. Записать данные: дата рождения, номер школы, хобби.
8. Сохранить данные на жесткий диск в свою папку под именем досье группы.

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Что такое сбор информации и каково его предназначение?
2. Что понимается под технологией сбора информации?
3. Чем отличаются понятия «информация» и «данные»?
4. Назовите основные требования к сбору данных и к хранимым данным.
5. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?
6. Какие еще методы сбора данных вам известны?
7. В чем заключается процедура хранения информации?
8. Перечислите основные требования к структурам хранения.
9. Что такое база данных?
10. В чем различие между базой и банком данных?
11. Что такое резервное копирование и для чего оно осуществляется?
12. Что такое архивное копирование и в чем его отличие от резервного копирования?

13. Что такое базовая информационная технология?

14. В чем заключается различие между централизованным и децентрализованным способами обработки информации?

15. Какие режимы обработки информации вам известны?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

РАЗДЕЛ 2. ИНФОРМАЦИЯ И ЭНТРОПИЯ

УСТНЫЙ ОПРОС ПО ТЕМЕ

«ТЕОРЕМА ОТСЧЕТОВ»

Вопросы:

1. Теорема отсчетов Котельникова и Найквиста — Шеннона.
2. Математическая модель системы передачи информации.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

УСТНЫЙ ОПРОС ПО ТЕМЕ

«ПОНЯТИЕ ЭНТРОПИИ. ВИДЫ ЭНТРОПИИ»

Вопросы:

1. Понятие энтропии.
2. Формула Хартли.
3. Виды условной энтропии.
4. Энтропия объединения двух источников.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

УСТНЫЙ ОПРОС ПО ТЕМЕ

«СМЫСЛ ЭНТРОПИИ ШЕННОНА»

Вопросы:

1. Статистический подход к измерению информации.
2. Закон аддитивности информации.
3. Формула Шеннона

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ПРИМЕНЕНИЕ ТЕОРЕМЫ ОТЧЕТОВ»

Цель: Изучение возможности синтезирования сигналов по дискретным отсчетам в соответствии с теоремой Котельникова.

Время выполнения: 2 часа

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор, текстовый редактор.

Практическое задание

1. Изобразить сигналы:

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

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Сформулируйте теорему Котельникова для сигналов с ограниченным спектром.

2. Объясните погрешности синтезирования реальных сигналов по дискретным отсчетам.

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ВЫПОЛНЕНИЕ РАСЧЕТОВ ПО ТЕОРЕМЕ ОТЧЕТОВ. ОПРЕДЕЛЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ ДИСКРЕТНОГО КАНАЛА»

Цель: научиться выполнять расчеты по теореме отчетов и определять пропускную способность дискретного канала.

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор, текстовый редактор.

Теоретические основы

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 1).

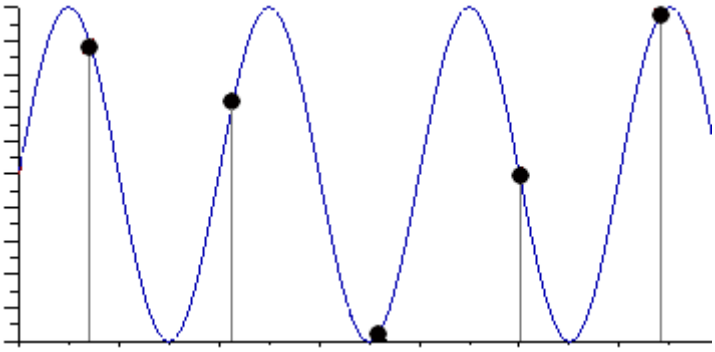


Рисунок 1

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 2).

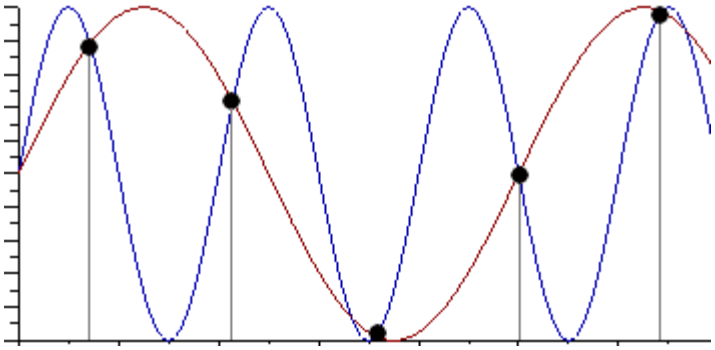


Рисунок 2

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).

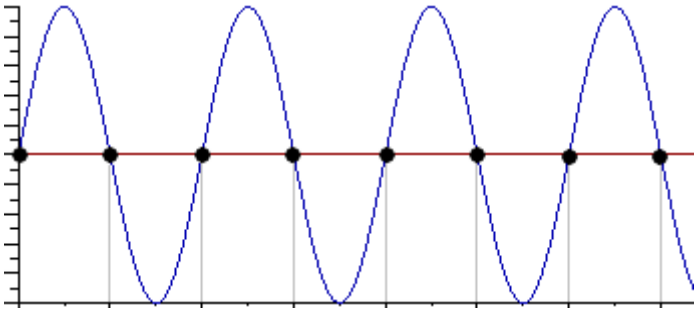


Рисунок 3

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 4). Данное утверждение теоретически обосновано, и мы его примем без доказательства.

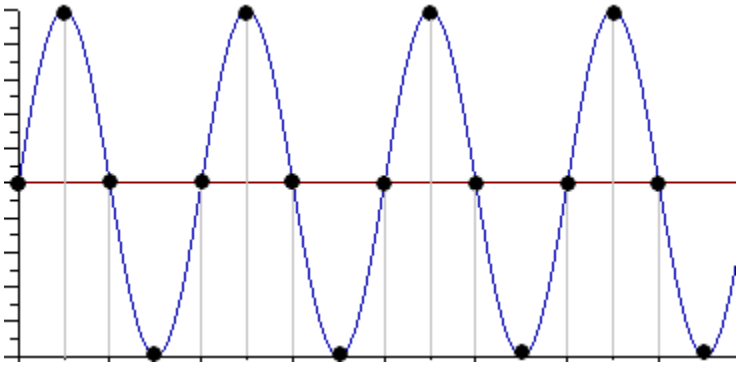


Рисунок 4

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.

$$fд > 2 \cdot F_{max} \quad (1)$$

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.

Пропускная способность непрерывного канала

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 $\Delta F_{НК}$. 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, $i = 1,2,...,L$, где $L = 2\Delta F_{НК} T$. При этом статистические свойства сигнала $x(t)$ можно описать многомерной ПРВ $w(x_1, x_2, ..., x_L) = w(x)$, а свойства шума – ПРВ $w(n_1, n_2, ..., n_L) = w(n)$.

Пропускная способность непрерывного канала определяется следующим образом:

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

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 $w(x)$.

Когда сигнал на входе канала имеет нормальное распределение и отсчеты независимы величина $h(X)$ максимизируется [6]. Поэтому пропускная способность гауссовского канала с дискретным временем, рассчитанная на единицу времени, с учетом (4.16) может быть записана в виде

$$C = V_H \cdot I(Y,X) = \frac{V_H}{2} \log_2 \left(\frac{\sigma_c^2 + \sigma^2}{\sigma^2} \right) = \frac{V_H}{2} \log_2 (1 + h^2). \qquad (4.17)$$

Полученное выражение показывает, что пропускная способность гауссовского канала с дискретным временем определяется числом импульсов, передаваемых в секунду, и отношением сигнал/шум (h).

С учетом взаимосвязи скорости передачи информации и полосы частот непрерывного канала от (4.17) можно перейти к формуле Шеннона, которая устанавливает связь пропускной способности гауссовского канала с полосой пропускания непрерывного канала и отношением мощности сигнала к мощности помехи:

$$C = \Delta F_{НК} \log_2 (1 + h^2). \qquad (4.18)$$

График отношения $\frac{C}{\Delta F_{НК}} = \log_2 (1 + h^2)$ изображен на рис. 4.6. Заметим, что при малом отношении $h^2 << 1$

$$C \cong \Delta F_{НК} \cdot 1{,}442 \cdot h^2,$$

а пропускная способность канала связи прямо пропорциональна этому отношению.

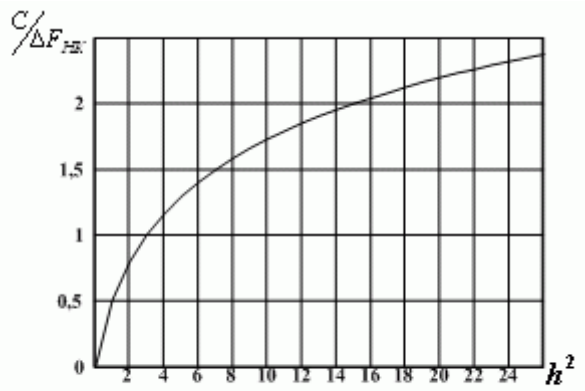


Рис. 4.6. Пропускная способность непрерывного канала

При большом отношении $h^2 >> 1$ в (4.18) можно пренебречь единицей и считать, что

$$\frac{C}{\Delta F_{НК}} \approx \log_2\left(h^2\right),$$

т.е. зависимость пропускной способности непрерывного канала от отношения сигнал/шум логарифмическая.

Пропускная способность канала, как предельное значение скорости безошибочной передачи информации, является одной из основных характеристик любого канала.

Определим пропускную способность стандартного канала тональной частоты, имеющего границы эффективно передаваемых частот $0{,}3...3{,}4$ кГц, среднюю мощность сигнала на выходе 56 мкВт при средней мощности помехи 69000 пВт.

Согласно (4.18), при заданных параметрах

$$C_{НК} = 3{,}1 \cdot 10^3 \cdot \log_2\left(\frac{56 \cdot 10^{-6}}{69 \cdot 10^{-12}}\right) = 3{,}0 \cdot 10^4$$ [бит/с].

Для непрерывных каналов справедлива теорема Шеннона, согласно которой сообщения дискретного источника могут быть закодированы и переданы по непрерывному каналу так, что вероятность ошибочного декодирования принятого сигнала $x(t)$ будет меньше наперед заданной положительной величины $p^*_{ош}$, если производительность источника $H'(X)$ меньше пропускной способности C непрерывного канала.

Для типовых непрерывных каналов многоканальной связи основные технические характеристики и пропускная способность, вычисленная по формуле Шеннона (4.18), при отношении сигнал/шум 20 дБ, приведены в табл. 4.4.

Зная пропускную способность канала и информационные характеристики сообщений (табл. 4.5), можно определить, какие сообщения (первичные сигналы) можно передавать по заданному каналу.

Таблица 4.4. Характеристики типовых каналов многоканальной связи

Наименование канала	Границы передаваемых частот, Гц	Пропускная способность, бит/с
Тональной частоты	300...3400	20,64·103
Предгрупповой широкополосный	12,3·103...23,4·103	73,91·103
Первичный широкополосный	60,6·103...107,7·103	313,6·103
Вторичный широкополосный	312,3·103...551,4·103	1,59·106
Третичный широкополосный	812,3·103...2043,7·103	8,2·106

Таблица 4.5. Производительность источников сообщений

Вид сообщения	Характер сообщения	Параметры АЦП		Производительность, бит/с
		$f_д$, Гц	$N = \log_2 L$	
Телеграфные, 50 Бод	дискретные	–	–	30…50
Телефонные	непрерывные	8·103	8	64·103
Звукового вещания: первого класса высшего класса	 непрерывные непрерывные	 24·103 32·103	 13	 240·103 416·103
Факсимильные, 120 строк/с: полутоновые штриховые	 непрерывные дискретные	 2,93·103 –	 4 –	 11,72·103 2,93·103
Передача данных, 2400 Бод	дискретные	–	–	2,4·103
Телевизионные	непрерывные	13·106	16	208·106

Например, первичный сигнал телевизионного вещания имеет $H'(X) = 208 \cdot 10^6 бит/с$ (табл. 4.5) и поэтому не может быть передан ни по одному из типовых непрерывных или цифровых каналов без потери качества. Следовательно, для передачи сигнала телевизионного вещания требуется создание специальных каналов с более высокой пропускной способностью или снижение скорости цифрового потока.

Задачи

1. Число символов алфавита m = 4. Вероятности появления символов равны соответственно p1 = 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.

4. Имеются источник информации с энтропией в единицу времени H(X) = 100 дв.ед. и два канала связи; каждый из них может передавать в единицу времени 70 двоичных знаков (0 или 1); каждый двоичный знак заменяется противоположным с вероятностью p = 0,1. Требуется выяснить, достаточна ли пропускная способность этих каналов для передачи информации, поставляемой источником.

5. Чему равна пропускная способность симметричного канала, если источник вырабатывает сигналы со скоростью 2 знака в секунду, закодированные кодом с основанием m = 10, а вероятность ложного приема p = 0,3?

6. Сообщения составлены из алфавита X = (x1, x2, x3). Вероятности появления символов алфавита 0,7; 0,2; 0,1 соответственно. Помехи в канале связи заданы следующей канальной матрицей:

$$P(Y/X) = \begin{vmatrix} 0,98 & 0,01 & 0,01 \\ 0,1 & 0,75 & 0,15 \\ 0,2 & 0,3 & 0,5 \end{vmatrix}$$

Определить скорость передачи информации, если время передачи одного символа t1 = 0,02с.

7. Чему раина пропускная способность канала связи, описанного канальной матрицей:

$$P(A,B) = \begin{vmatrix} 0,1 & 0 & 0 \\ 0,1 & 0,3 & 0 \\ 0 & 0,1 & 0,4 \end{vmatrix}$$

если известно, что на выходе источника сообщений символы вырабатываются со скоростью 100 знаков в секунду?

8. Определить максимально возможную скорость передачи информации по радиотехническому каналу связи пункта управления с телеуправляемой ракетой, если полоса пропускания канала связи равна 3 МГц, а минимальное отношение сигнал-шум по мощности в процессе наведения ракеты на цель равно 3.

9. Определить полосу пропускания канала передачи телевизионного черно-белого изображения с 5x105 элементами, 25 кадрами в секунду и 8 равновероятными градациями яркости для отношения P/N = 15 при условии, что изображение может принимать наиболее хаотичный вид «белого шума».

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

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

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

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

4. Сформулируйте основную теорему Шеннона о кодировании для канала без помех.

5. Сформулируйте и поясните теорему Шеннона о кодировании для канала с помехами.

6. Приведите выражение пропускной способности для дискретного канала без помех и с помехами.

7. Сформулируйте и поясните теорему отсчетов (Котельникова)

8. Какие параметры влияют на объем сигнала.

9. От чего зависит пропускная способность непрерывного канала связи.

10. Назовите условия согласования источников информации с пропускной способностью непрерывных каналов связи.

11. Какова скорость отображения информации приемным устройством отображения информации.

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ПОИСК ЭНТРОПИИ СЛУЧАЙНЫХ ВЕЛИЧИН»

Цель: научиться вычислять энтропию случайной величины.

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор, текстовый редактор.

Теоретические основы

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:

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

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:

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

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 ожидания «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:

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

Определение энтропии Шеннона очень связано с понятием термодинамической энтропии. Больцман и Гиббс проделали большую работу по статистической термодинамике, которая способствовала принятию слова «энтропия» в информационную теорию. Существует связь между понятиями энтропии в термодинамике и теории информации. Например, демон Максвелла также противопоставляет термодинамическую энтропию информации, и получение какого-либо количества информации равно потерянной энтропии.

СВОЙСТВА ЭНТРОПИИ

1. Энтропия является вещественной и неотрицательной величиной.

2. Энтропия – величина ограниченная.

3. Энтропия обращается в нуль лишь в том случае, если вероятность одного из состояний равна единице; тогда вероятности всех остальных состояний, естественно, равны нулю. Это положение соответствует случаю, когда состояние источника полностью определено.

4. Энтропия максимальна, когда все состояния источника равновероятны.

5. Энтропия источника и с двумя состояниями u1 и u2 изменяется от нуля до единицы, достигая максимума при равенстве их вероятностей:

p(u1) = p= p(u2) = 1 — p = 0,5.

6. Энтропия объединения нескольких статистически независимых источников информации равна сумме энтропии исходных источников.

7. Энтропия характеризует среднюю неопределенность выбора одного состояния из ансамбля. При ее определении используют только вероятности состояний, полностью игнорируя их содержательную сторону. Поэтому энтропия не может служить средством решения любых задач, связанных с неопределенностью.

8. Энтропия как мера неопределенности согласуется с экспериментальными данными, полученными при изучении психологических реакций человека, в частности реакции выбора. Установлено, что время безошибочной реакции на последовательность беспорядочно чередующихся равновероятных раздражителей (например, загорающихся лампочек) растет с увеличением их числа так же, как энтропия. Это время характеризует неопределенность выбора одного раздражителя. Замена равновероятных раздражителей неравновероятными приводит к снижению среднего времени реакции ровно настолько, насколько уменьшается энтропия.

Дифференциальной энтропией случайной величины X называется величина:

$$H_Д(x)=H(x)-H(y)= -\int_{-\infty}^{+\infty} p_x(x) * \log_2 d * p_x(x)dx$$

Если произвести квантование случайных величин X_1, $X_2 \ldots X_n$ по уровню с числом уровней квантования равным m , то возможное число реализаций длительностью T_n станет конечным и равным $M = m^n$.

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

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

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

$H_{max}=\log M$

Выполнение расчетных задач

Задача №1

Показать, что для регулярной марковской цепи энтропия $H(x)^{(r)}$ за r шагов равняется энтропии за один шаг, умноженной на число шагов r.

Решение:

Регулярная цепь Маркова полностью характеризуется матрицей переходных вероятностей $P = \begin{Bmatrix} p_{11} & \cdots & p_{1m} \\ . & . & . \\ p_{m1} & & p_{mm} \end{Bmatrix}$ и предельным стационарным распределением вероятностей состояний $(p_1, p_2, \ldots, p_m)$.

В стационарном режиме энтропия за один шаг не зависит от номера шага и равна $H(X)^{(1)} = \sum_{k=1}^{m} p_k H_k(x)$,

p_k - стационарная вероятность *k*-го состояния,

$H_k(x) = -\sum_{i=1}^{m} p_{ki} \log p_{ki}$ - энтропия в *k*-м состоянии.

Энтропия за *r* шагов равна сумме энтропий за каждый шаг. Так как энтропия за каждый шаг одинакова, то сумма энтропий равна $H(X)^{(r)} = r \cdot H(X)^{(1)}$.

Задача №2

В результате полной дезорганизации управления m самолетов летят произвольными курсами. Управление восстановлено, и все самолеты взяли общий курс со среднеквадратической ошибкой отклонения от курса $\sigma=3^0$. Найти изменение энтропии,

считая, что в первом случае имело место равномерное распределение вероятностей углов, а во втором случае – нормальное.

Решение.

Начальное распределение вероятностей углов курсов самолетов равномерное в интервале от $a = 0$ до $b = 360^\circ = 2\pi\ рад$ с плотностью вероятности $p_{1x}(x) = \frac{1}{b-a},\ a \le x \le b$.

Дифференциальная энтропия этого распределения

$$H_{1x}(x) = -\int_a^b \frac{1}{b-a}\log_2\frac{1}{b-a}dx = -\log_2\frac{1}{b-a} = \log_2(b-a) = \log_2 2\pi = 2,65$$ бит.

Конечное распределение вероятностей углов курсов самолетов нормальное с параметрами $a = 0,\ \sigma = 3^\circ = \frac{\pi}{60}\ рад$ и плотностью вероятности $p_{2x}(x) = \frac{1}{\sigma\sqrt{2\pi}}e^{-x^2/(2\sigma^2)}$.

Дифференциальная энтропия этого распределения

$$H_{2x}(x) = -\int_{-\infty}^{\infty} p_{2x}(x)\log_2\left[\frac{1}{\sigma\sqrt{2\pi}}e^{-x^2/(2\sigma^2)}\right]dx =$$

$$= -\log_2\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{\infty} p_{2x}(x)dx + \frac{\log_2 e}{2\sigma^2}\int_{-\infty}^{\infty} x^2 p_{2x}(x)dx =$$

$$= -\log_2\frac{1}{\sigma\sqrt{2\pi}} + \frac{\log_2 e}{2\sigma^2}\cdot\sigma^2 = \log_2\sigma\sqrt{2\pi} + \frac{\log_2 e}{2} = \log_2\frac{\pi\sqrt{2\pi e}}{60} = -2,21\ бит.$$

Изменение энтропии $\Delta H(x) = H_{2x}(x) - H_{1x}(x) = -2,21 - 2,65 = -4,86$ бит.

Энтропия уменьшилась на 4,86 бит.

Задача №3

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.

Задачи по вычислению энтропии

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.

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Как определяется энтропия дискретных случайных величин?

2. Приведите примеры энтропий для классических законов распределения.

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«РАСЧЕТ ВЕРОЯТНОСТЕЙ. СОСТАВЛЕНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ»

Цель: Приобрести практические навыки по расчету вероятностей.

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор, текстовый редактор.

Задачи

Задача № 1. Монета подбрасывается три раза подряд. Под исходом опыта будем понимать последовательность ($X1$, $X2$, $X3$), где каждый из Xi обозначает выпадение «герба» (Г) или цифры (Ц).

Необходимо:

а) Построить пространство W элементарных событий;

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

Задача № 2. Событие B является частным случаем события A. Чему равны их сумма и произведение?

Задача № 3. Пусть A, B, C – случайные события. Выяснить смысл равенств:

а) $A \cap B \cap C = A$;

б) $A \cup B \cup C = A$.

Задача № 4. 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.

Задача № 5. 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?

Задача № 6. Из слова «НАУГАД» наугад выбирается одна буква. Какова вероятность того, что эта буква *А*? Какова вероятность того, что это гласная буква?

Задача№ 7. Монета бросается два раза. Найти вероятности событий:

1. *А* = {герб выпадет один раз};

2. *В* = {герб выпадет хотя бы один раз};

3. *С* = {герб не выпадет ни разу}.

Задача № 8. Бросаются две монеты. Какое из событий является более вероятным:

1. *А* = {монеты лягут одинаковыми сторонами};

2. *В* = {монеты лягут разными сторонами}?

Задача № 9. Бросаются одновременно две игральные кости. Найти вероятности событий:

1. *А* = {произведение выпавших очков равно 8};

2. *В* = {сумма выпавших очков равна 8};

3. *С* = {произведение выпавших очков четно};

4. *Д* = {сумма выпавших очков четна};

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

Задача № 10. Брошены три монеты. Найти вероятность того, что выпадут

два 2 «герба».

Задача № 11. При стрельбе была получена относительная частота (частость) попадания 0,6. Сколько было сделано выстрелов, если получено 12 промахов?

Задача № 12. 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.

Задача № 13. Из пяти карточек с буквами *А*, *Б*, *В*, *Г*, *Д* наугад одна за другой выбираются три и располагаются в ряд в порядке появления. Какова вероятность того, что получится слово «ДВА»?

Задача № 14. В урне 3 белых и 7 черных шаров. Какова вероятность того, что вынутые наугад два шара окажутся черными? Одного цвета? Разных цветов?

Задача № 15. В ящике 10 красных и 6 синих пуговиц. Вынимаются наудачу две пуговицы. Какова вероятность того, что пуговицы будут одноцветными?

Задача № 16. Найти вероятность того, что наудачу взятое двузначное число окажется кратным 2, либо 5, либо тому и другому одновременно.

Задача № 17. 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.

Задача№ 18. 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?

Задача № 19. В круг радиуса R вписан квадрат. Чему равна вероятность того, что поставленные наудачу внутри круга две точки окажутся внутри квадрата?

Задача № 20. 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}.

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

ПРАКТИЧЕСКАЯ РАБОТА

СОСТАВЛЕНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ.

Цель: научиться составлять законы распределения вероятностей.

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор.

Теоретические основы

Дискретной называют случайную величину, возможные значения которой есть отдельные изолированные числа, которые эта величина принимает с определенными ненулевыми вероятностями. Число возможных значений может быть конечным или бесконечным (счетным).

Законом распределения дискретной случайной величины называют перечень её возможных значений и соответствующих им вероятностей. Закон распределения может быть задан одним из следующих способов.

1. Таблицей

x	x_1	x_2	…	x_n
p	p_1	p_2	…	p_n

где $\sum_{i=1}^{n} p_i = 1$.

2. Аналитически $P(X = x_i) = \varphi(x_i)$. Например:

а) *биномиальное распределение*

$P(X = k) = C_n^k p^k q^{n-k}$, 0□p□1, k=0, 1, 2, …, n;

б) *распределение Пуассона*

$P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}$, □□0, k=0, 1, 2, … .

3. С помощью *функции распределения F(x)*, определяющей для каждого значения *x* вероятность того, что случайная величина X примет значение, меньшее *x*, т. е. $F(x) = P(X < x)$.

Свойства F(x):

1) $0 \le F(x) \le 1$;

2) $F(x_2) \ge F(x_1)$, если $x_2 > x_1$;

3) $\lim_{x \to -\infty} F(x) = 0, \ \lim_{x \to +\infty} F(x) = 1$.

4. Закон распределения может быть задан графически - *многоугольником распределения (см. пример 1).*

Числовые характеристики дискретных случайных величин

Математическое ожидание $M(X)=\sum x_i p_i$;

Дисперсия $D(X)=M[X-M(X)]^2$ или $D(X)=M(X^2)-[M(X)]^2$;

Среднее квадратическое отклонение $\sigma(X)=\sqrt{D(X)}$.

Для биномиального распределения *M(X)=np*, *D(X)=npq*. Для распределения Пуассона *M(X)=*□*, D(X)=* □.

Пример 1.

Устройство состоит из трех независимо работающих элементов. Вероятность отказа каждого элемента в одном опыте равна 0,1. Составить закон распределения числа отказавших элементов в одном опыте, построить многоугольник распределения. Найти функцию распределения F(x) и построить её график. Найти M(X), D(X), □(X).

Решение: Дискретная случайная величина X (число отказавших элементов в одном опыте) имеет следующие возможные значения: $x_1=0$ (ни один из элементов устройства не отказал), $x_2=1$ (отказал один элемент), $x_3=2$ (отказало два элемента) и $x_4=3$ (отказали три элемента).

Отказы элементов независимы один от другого, вероятности отказа каждого элемента равны между собой, поэтому применима формула Бернулли. Учитывая, что, по условию, n=3, p=0,1 (следовательно, q=1–0,1=0,9), получим: $P_3(0)=q^3=0,9^3=0,729$; $P_3(1)=C_3^1 pq^2=3\cdot 0,1\cdot 0,9^2=0,243$;

$P_3(2)=C_3^2 p^2 q=3\cdot 0,1^2\cdot 0,9=0,027$; $P_3(3)=p^3=0,1^3=0,001$.

Контроль: $\sum_{i=1}^{4} p_i=1$; 0,729+0,243+0,027+0,001=1.

Искомый биномиальный закон распределения *X*:

X	0	1	2	3

p	0,729	0,243	0,027	0,001

Для построения многоугольника распределения строим прямоугольную систему координат. По оси абсцисс откладываем возможные значения x_i, а по оси ординат – соответствующие им вероятности p_i. Построим точки $M_1(0;0,729)$, $M_2(1;0,243)$, $M_3(2;0,027)$, $M_4(3;0,001)$. Соединив эти точки отрезками прямых, получаем искомый многоугольник распределения .

Найдем функцию распределения $F(x)=P(X<x)$.

Для $x \le 0$ имеем $F(x)=P(X<0)=0$;

для $0 < x \le 1$ имеем $F(x)=P(X<1)=P(X=0)=0,729$;

для $1 < x \le 2$ $F(x)=P(X<2)=P(X=0)+P(X=1)=0,729+0,243=0,972$;

для $2 < x \le 3$ $F(x)=P(X<3)=P(X=0)+P(X=1)+P(X=2)=0,972+0,027=0,999$;

для $x>3$ будет $F(x)=1$, т. к. событие достоверно.

$$F(x)=\begin{cases} 0 & при\ x \le 0, \\ 0,729 & при\ 0 < x \le 1, \\ 0,972 & при\ 1 < x \le 2, \\ 0.999 & при\ 2 < x \le 3, \\ 1 & при\ x > 3. \end{cases}$$

График этой функции приведен на Рис. 2.

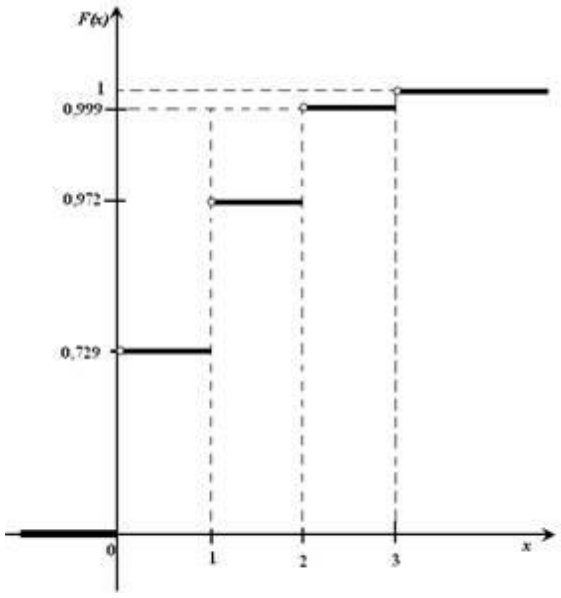


Рис. 2

Для биномиального распределения $M(X)=np=3\cdot0,1=0,3$; $D(X)=npq=3\cdot0,1\cdot0,9=0,27$; $\sigma(X)=\sqrt{D(X)}=\sqrt{0,27}\approx0,52$.

Пример 2.

В партии из 10 деталей имеется 8 стандартных. Наудачу отобраны две детали. Составить закон распределения случайной величины X – числа стандартных деталей среди отобранных. Найти $M(X)$, $D(X)$.

Решение: Случайная величина X – число стандартных деталей среди отобранных деталей – имеет следующие возможные значения: $x_1=0$; $x_2=1$; $x_3=2$. Найдем вероятности возможных значений X по формуле (пример 2) $P(X=k)=\frac{C_n^k\cdot C_{N-n}^{m-k}}{C_N^m}$ (N – число деталей в партии, n – число стандартных деталей в партии, m – число отобранных деталей, k – число стандартных деталей среди отобранных), находим:

$$P(X=0)=\frac{C_8^0\cdot C_2^2}{C_{10}^2}=\frac{1}{10\cdot9/(1\cdot2)}=\frac{1}{45};\quad P(X=1)=\frac{C_8^1\cdot C_2^1}{C_{10}^2}=\frac{8\cdot2}{45}=\frac{16}{45};$$

$$P(X=2)=\frac{C_8^2\cdot C_2^0}{C_{10}^2}=\frac{8\cdot7/(1\cdot2)}{45}=\frac{28}{45}.$$

Составим искомый закон распределения:

X	0	1	2
p	$\frac{1}{45}$	$\frac{16}{45}$	$\frac{28}{45}$

Контроль: $\frac{1}{45}+\frac{16}{45}+\frac{28}{45}=1$.

$$M(X)=\sum_{i=1}^{3}x_i p_i = 0\cdot\frac{1}{45}+1\cdot\frac{16}{45}+2\cdot\frac{28}{45}=\frac{72}{45}=\frac{8}{5}.$$

$$D(X)=M(X^2)-[M(X)]^2;\ M(X^2)=\sum_{i=1}^{3}x_i^2 p_i = 0^2\cdot\frac{1}{45}+1^2\cdot\frac{16}{45}+2^2\cdot\frac{28}{45}=\frac{128}{45};$$

$$D(X)=\frac{128}{45}-\left(\frac{8}{5}\right)^2=\frac{128}{45}-\frac{64}{25}=\frac{64}{225}.$$

Пример 3.

В устройстве независимо друг от друга выходят из строя три элемента. Вероятность выхода из строя первого элемента – 0,3, второго – 0,2, третьего – 0,4. Составить закон распределения случайной величины X – числа вышедших из строя элементов.

Решение: случайная величина X имеет следующие возможные значения: $x_1=0$, $x_2=1$, $x_3=2$, $x_4=3$. $p_1=0,3, q_1=1-p_1=0,7$, $p_2=0,2$, $q_2=1-p_2=0,8$, $p_3=0,4$, $q_3=1-p_3=0,6$.

P(X=k) вычисляем по следующим формулам (см. пример 4) $P(X=0)=q_1\cdot q_2\cdot q_3=0,7\cdot 0,8\cdot 0,9=0,336$;

$$P(X=1)=p_1\cdot q_2\cdot q_3+q_1\cdot p_2\cdot q_3+q_1\cdot q_2\cdot p_3=0,3\cdot 0,8\cdot 0,6+0,7\cdot 0,2\cdot 0,6+$$

$$+0,7\cdot 0,8\cdot 0,4=0,144+0,084+0,224=0,452;$$

$$P(X=2)=p_1\cdot p_2\cdot q_3+p_1\cdot q_2\cdot p_3+q_1\cdot p_2\cdot p_3=0,3\cdot 0,2\cdot 0,6+0,3\cdot 0,8\cdot 0,4+$$

$$+0,7\cdot 0,2\cdot 0,4=0,118;$$

$$P(X=0)=p_1\cdot p_2\cdot p_3=0,3\cdot 0,2\cdot 0,4=0,024.$$

Контроль: 0,336+0,452+0,118+0,024=1.

X	0	1	2	3
p	0,336	0,452	0,118	0,024

Искомый закон распределения:

Пример 4.

Среднее число заказов такси, поступающих на диспетчерский пункт в одну минуту, равно двум. Составить закон распределения случайной величины X – числа заказов, поступающих за 4 минуты. Найти M(X), D(X).

Решение: Поток заказов на такси можно считать *простейшим,* т. е. обладающим стационарностью, «отсутствием последствия» и ординарностью. *Интенсивность потока* (среднее число событий появляющихся в единицу времени) □=2. Вероятность появления k событий простейшего потока за время t=4 определяется формулой Пуассона $P_t(k)=\frac{(\lambda t)^k e^{-\lambda t}}{k!}$, для данной задачи $P_4(k)=\frac{8^k e^{-8}}{k!}$. Совокупность возможных значений X есть счетное множество, т.е. $x_1=0, x_2=1, \ldots, x_k=k+1, \ldots;$ тогда закон распределения случайной величины X – числа заказов, поступающих за 4 минуты принимает вид:

X	0	1	2	…	k	…
p	$e^{-\lambda t}$	$\frac{(\lambda t)\, e^{-\lambda t}}{1!}$	$\frac{(\lambda t)^2 e^{-\lambda t}}{2!}$	…	$\frac{(\lambda t)^k e^{-\lambda t}}{k!}$	…

или

X	0	1	2	…	k	…
p	e^{-8}	$\frac{8\, e^{-8}}{1!}$	$\frac{8^2 e^{-8}}{2!}$	…	$\frac{8^k e^{-8}}{k!}$	…

Воспользовавшись таблицей 3 приложения, окончательно получим:

X	0	1	2	…	k	…
p	0,00035	0,002684	0,010735	…	$\frac{8^k e^{-8}}{k!}$	…

Наивероятнейшее число заказов такси за 4 минуты можно определить по получившемуся закону распределения (значения *x*, при которых *p* максимально): $_0$=7, k_0=8. Для□

простейшего потока событий: математическое ожидание $M(X)=\lambda t=8$, дисперсия $D(X)=\lambda t=8$

Пример 5.

Y	1	3	6
p	0,2	0,5	0,3

Даны законы распределения независимых случайных величин *X* и *Y*. Составить закон распределения случайной величины *Z=X+2Y*. Найти *M(Z), D(Z).*

X	-3	0	1
p	0,1	0,03	0,06

Решение: Закон распределения *V=2Y* получается из распределения *Y* путем умножения всех значений y_i на 2. Получаем:

V	2	6	12
p	0,2	0,5	0,3

.

Для составления закона распределения случайной величины *Z* вычислим все ее возможные значения по формуле $z_k=x_i+v_j$, $k=1,2,...9$, $i,j=1,2,3$.

Соответствующие данным значениям z_k вероятности p_k можно вычислить по формуле умножения вероятностей $P_k=P(Z=z_k)=P(X=x_i)\cdot P(V=v_j)$, т. к. события $X=x_i$ и $V=v_j$ - независимы (исходим из независимости случайных величин X и Y) и наступают совместно (событие $\{Z=z_k\}$ ={совместное наступление событий $X=x_i$ и $V=v_j$}). Тогда распределение Z принимает вид

Z	-1	3	9	2	6	12	3	7	13
p	0,02	0,05	0,03	0,06	0,15	0.09	0,12	0,3	0,18

Рассмотрим значения $z_2 = z_7 = 3$. События $Z = z_2$ и $Z = z_7$ несовместны, поэтому вероятность наступления хотя бы одного из этих событий вычисляется по правилу сложения вероятностей

$$P(Z = z_2 \cup Z = z_7) = P(Z = z_2) + P(Z = z_7) = 0{,}05 + 0{,}12 = 0{,}17$$

Искомый закон распределения случайной величины Z получается после размещения z_k по возрастанию.

Z	-1	2	3	6	7	9	12	13
p	0,02	0,06	0,17	0,15	0,3	0,03	0,09	0,18

Математическое ожидание *M(Z)* и дисперсию *D(Z)* можно найти по формулам:

$$M(Z) = \sum_{k=1}^{8} z_k p_k \text{;} \quad D(Z) = M(Z^2) - [M(Z)]^2 \text{, где } M(Z^2) = \sum_{k=1}^{8} z_k^2 p_k .$$

Рассмотрим другой способ.

M(Z) и *D(Z)* можно найти через *M(X), M(Y), D(X), D(Y).*

$$M(X) = \sum_{i=1}^{3} x_i p_i = -3 \cdot 0{,}1 + 0 \cdot 0{,}3 + 1 \cdot 0{,}6 = 0{,}3$$

$$M(Y) = \sum_{j=1}^{3} y_j p_j = 0 \cdot 0{,}2 + 3 \cdot 0{,}5 + 6 \cdot 0{,}3 = 3{,}3$$

$$D(X) = \sum_{i=1}^{3} x_i^2 p_i - (M(X))^2 = (-3)^2 \cdot 0{,}1 + 0^2 \cdot 0{,}3 + 1^2 \cdot 0{,}6 - (0{,}3)^2 = 1{,}41$$

$$D(Y) = \sum_{j=1}^{3} y_j^2 p_j - (M(Y))^2 = 0^2 \cdot 0{,}2 + 3^2 \cdot 0{,}5 + 6^2 \cdot 0{,}3 - (3{,}3)^2 = 4{,}41$$

$$M(Z) = M(X + 2Y) = M(X) + M(2Y) = M(X) + 2M(Y) = 0{,}3 + 2 \cdot 3{,}3 = 6{,}9,$$

т. к. математическое ожидание суммы равно сумме математических ожиданий слагаемых; постоянный множитель можно вынести за знак математического ожидания.

$$D(Z) = D(X + 2Y) = D(X) + D(2Y) = D(X) + 4D(Y) = 1{,}41 + 4 \cdot 4{,}41 = 19{,}05,$$

т. к. дисперсия суммы независимых случайных величин равна сумме дисперсий слагаемых; постоянный множитель можно вынести за знак дисперсии, возведя его в квадрат.

Пример 6.

Стрелок ведет стрельбу с вероятностью попадания в цель 0,8 при каждом выстреле. Стрельба ведется до первого попадания, но делается не более 3 выстрелов. Составить закон распределения случайной величины X, если: а) X – число промахов; б) X – число попаданий; в) X – число произведенных выстрелов.

Решение: Вероятность попадания p=0,8; вероятность промаха q=1-p=0,2.

а) Случайная величина X – число промахов при трех выстрелах – имеет следующие возможные значения: $x_1 = 0$; $x_2 = 1$; $x_3 = 2$; $x_4 = 3$.

Событие X=0 равносильно попаданию с первой попытки, следовательно, P(X=0)=p=0,8.

Событие X=1 равносильно попаданию со второй попытки, т. е. совместному наступлению двух событий: промаха и попадания; следовательно, P(X=1)=q · p=0,2 ·0,8=0,16.

Событие X=2 равносильно попаданию с третьей попытки, т. е. P(X=2)=q · q · p=0,2 · 0,2 · 0,8=0,032.

Событие X=3 означает отсутствие попаданий, P(X=3)=q · q · q=$0,2^3$=0,008.

Искомый закон распределения X:

X	0	1	2	3
p	0,8	0,16	0,032	0,008

б) Случайная величина X – число попаданий – имеет следующие возможные значения: $x_1 = 0$ (допущено три промаха); $x_2 = 1$ (произошло попадание с первой, второй или третьей попытки).

Тогда P(X=0)= q^3 = $0,2^3$=0,008;

P(X=1)= p+q·p+q q p=0,8+0,16+0,032=0,992

или P(X=1)=1-P(X=0)=1-0,008=0,992.

Искомый закон распределения X:

X	0	1
P	0,008	0,992

в) Случайная величина X – число произведенных выстрелов – имеет следующие возможные значения: $x_1 = 1$; $x_2 = 2$; $x_3 = 3$.

Событие X=1 равносильно попаданию с первой попытки, т. е. P(X=1)=p=0,8.

Событие X=2 равносильно попаданию со второй попытки, т. е. $P(X=2)=q \cdot p=0,16$.

Событие X=3 означает, что либо произошло попадание с третьей попытки, либо было три промаха. Тогда $P(X=3)=q \cdot q \cdot p+q \cdot q \cdot q=0,032+0,008=0,04$.

Искомый закон распределения X:

X	1	2	3
P	0,8	0,16	0,04

Задачи

Вариант 1. Производятся последовательные независимые испытания приборов на надёжность. Каждый следующий прибор испытывается лишь в том случае, если предыдущий оказался надежным. Построить закон распределения случайного числа испытанных приборов, если вероятность выдержать испытание для каждого из них равна 0,9. Найти математическое ожидание числа испытанных приборов. Найти функцию распределения F(x) и построить ее график; найти M(X), □(X); построить многоугольник распределения.

Вариант 2. Известно, что в партии из 20 телефонных аппаратов 5 недействующих. Случайным образом из этой партии взято 4 аппарата. Построить закон распределения случайной величины X – числа недействующих аппаратов из отобранных. Найти дисперсию этой случайной величины. В каких единицах она измеряется? Построить график функции распределения F(x) случайной величины X, многоугольник распределения.

Вариант 3. Сырье на завод привозят от трех независимо работающих поставщиков. Вероятность своевременного прибытия сырья от первого поставщика равна 0,4, от второго – 0,7, от третьего – 0,6. Найти математическое ожидание M(X), дисперсию D(X) числа своевременных поставок сырья. Найти функцию распределения и построить ее график.

Вариант 4. Завод получает сырье на автомашинах от трех независимо работающих поставщиков. Вероятность прибытия автомашины от первого поставщика равна 0,2, от второго – 0,3 и от третьего – 0,1. Составить распределение числа прибывших автомашин. Найти математическое ожидание и дисперсию полученной величины. Построить график функции распределения F(x).

Вариант 5. Вероятность изготовления бракованной детали p=0,1. Изготовлено 4 детали. X – случайное число бракованных деталей. Построить закон распределения

случайной величины X, найти ее математическое ожидание и дисперсию. Построить график функции распределения, многоугольник распределения.

Вариант 6. Среднее число заявок, поступающих на предприятие бытового обслуживания за 1 час, ровно 2. Составить закон распределения случайной величины X – числа заявок, поступивших за 3 часа. Найти M(X), D(X) и наивероятнейшее число заявок за 3 часа.

Вариант 7. В среднем в магазин заходит 3 человека в минуту. Составить закон распределения случайной величины X – числа зашедших в магазин человек за 2 минуты. Построить многоугольник распределения. Найти M(X), D(X).

Вариант 8. Даны законы распределения независимых случайных величин

X	-3	0	1
P	0,1	0,3	0,6

Y	0	3	6
p	0,2	0,5	0,3

Составить законы распределения случайных величин:

а)XY; б) X+Y. Найти M(X+Y), D(X+Y). Справедливо ли равенство M(X)□M(Y)=M(X□Y)?

Вариант 9. Команда состоит из двух стрелков. Числа очков, выбиваемых каждым из них при одном выстреле, являются случайными величинами X_1 и X_2 , которые характеризуются следующими законами распределения:

X_1	3	4	5
P	0,3	0,4	0,3

и

X_2	2	3	4	5
P	0,2	0,1	0,2	0,5

Результаты стрельбы одного стрелка не влияют на результат стрельбы другого. Составить закон распределения числа очков, выбиваемых командой, если стрелки сделают по одному выстрелу. Убедиться в справедливости равенства $D(X_1+X_2)=D(X_1)+D(X_2)$.

Вариант 10. Производятся выстрелы из орудия с вероятностью попадания в цель 0,9 при каждом выстреле. Стрельба ведётся до первого попадания, но делается не более 4

выстрелов. Составить закон распределения случайной величины X, если: а) X – число произведенных выстрелов; б) X – число промахов; в) X – число попаданий. Найдите математическое ожидание всех найденных случайных величин.

Отчет

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Какие значения не может принимать вероятность?

2. Чему равна вероятность достоверного события? Невозможного?

3. Дайте определение закону распределения дискретной случайной величины.

4. Дайте определение математическому ожиданию?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

РАЗДЕЛ 3. ЗАЩИТЫ И ПЕРЕДАЧА ИНФОРМАЦИИ

УСТНЫЙ ОПРОС ПО ТЕМЕ «СЖАТИЕ ИНФОРМАЦИИ»

Вопросы:

1. Понятие сжатия информации
2. Простейшие алгоритмы сжатия информации,
3. Методы Лемпела-Зива,
4. Особенности программ архиваторов.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ТЕСТ НА ТЕМУ «СЖАТИЕ ИНФОРМАЦИИ»

1. Сжатие информации позволяет …

    а) уменьшить избыточность информации

    б) уменьшить энтропию информации

    в) уменьшить объективность информации

    г) уменьшить полноту информации

2. Какого вида (понятия) избыточности теории информации не существует?

    а) смысловой

    б) объективной

в) физической

г) статистической

3. Метод сжатия текстовой информации, предложенный в 1952 году Дэвидом Хафманом, и основанный на том, как часто встречается данный символ в тексте, это метод сжатия

а) без потерь

б) с потерями

4. Что такое префиксный код?

а) код, в котором требуется указывать длину кода

б) код, в котором коды символов имеют одинаковую длину

в) это код, в котором код одного символа не может быть началом кода другого символа

5. С каким видом избыточности информации в основном имеют дело алгоритмы архивации?

а) со смысловой избыточностью

б) с физической избыточностью

в) со статистической избыточностью

6. Какие типы файлов из перечисленных, плохо сжимаются?

а) *.xls

б) *.exe

в) *.doc

г) *.txt

7. Какой вид избыточности информации присущ только человеческому общению?

а) смысловая избыточность

б) физическая избыточность

в) статистическая избыточность

8. Четырем сообщениям поставлены в соответствие коды: 00 01 10 11. Как можно уменьшить избыточность, убрав бесполезный бит, но не исказив при этом передаваемую информацию?

а) 0 01 10 11

б) 00 1 10 11

в) 00 01 0 11

г) 00 01 10 1

9. Какие данные из перечисленных обладают большей избыточностью?

а) текстовые данные

б) графические данные

в) видеоданные

г) числовые данные

10. Метод сжатия, основанный на учете повторяющихся байтов или последовательности байтов, это

а) сжатие с потерями

б) сжатие без потерь

11. От чего не зависит степень сжатия файла?

а) от используемой программы

б) от метода сжатия

в) от типа исходного файла

г) от объема исходного файла

12. Лучшую степень сжатия можно получить от сжатия

а) с потерями

б) без потерь

Ответы на тест

1 а	7 а
2 б	8 г
3 а	9 в
4 в	10 б
5 в	11 г
6 б	12 а

Критерии оценивания теста:

5 (отлично) – правильно выполнены 11-12 заданий.

4 (хорошо) – правильно выполнены 9-10 задания.

3 (удовлетворительно) – правильно выполнены 7-8 заданий.

2 (неудовлетворительно) – правильно выполнены менее 7 заданий.

УСТНЫЙ ОПРОС ПО ТЕМЕ «КОДИРОВАНИЕ»

Вопросы:

1. Помехоустойчивое кодирование.
2. Адаптивное арифметическое кодирование.
3. Цифровое кодирование
4. Аналоговое кодирование
5. Таблично-символьное кодирование, числовое кодирование.

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ТЕСТ «КОДИРОВАНИЕ ИНФОРМАЦИИ»

Задание 1

Вопрос:

Декодируйте слова при помощи перестановки букв и сделайте сопоставление

Укажите соответствие для всех 3 вариантов ответа:

1) символ

2) сигнал

3) сканер

___ловсим

___гисанл

___ксаерн

Задание 2

Вопрос:

Правда ли, что одна и та же информация может быть закодирована разными способами и представлена в разных формах?

Выберите один из 2 вариантов ответа:

1) да
2) нет

Задание 3

Вопрос:

При помощи какого кода закодирована вся информация в компьютере?

Выберите один из 4 вариантов ответа:

1) восьмеричного

2) кода дорожных знаков

3) двоичного

4) азбуки Брайля

Задание 4

Вопрос:

Расшифруйте и запишите слово, закодированное при помощи шифра Цезаря, используя алфавит:

лрчсургщлв

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

Запишите ответ:

_____

Задание 5

Вопрос:

Расшифруйте и запишите слово, закодированное числовым способом:

17 33 20 10 12 13 1 19 19 15 10 12

Изображение:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

Запишите ответ:

_____

Задание 6

Вопрос:

Выберите способы кодирования информации:

Выберите несколько из 4 вариантов ответа:

1) экстрасенсорный

2) графический

3) числовой

4) символьный

Задание 7

Вопрос:

Сделайте сопоставление между рисунками и названиями видов кодирования информации

Укажите соответствие для всех 3 вариантов ответа:

1) графический способ кодирования

2) числовой способ кодирования

3) символьный способ кодирования

_ 

_ зжлрлщг

_ 20 16 20 15 6

Задание 8

Вопрос:

Вставьте в определении пропущенное слово. "Система условных знаков для представления информации называется ... "

Запишите ответ:

_____

Задание 9

Вопрос:

Как называется процесс обратный кодированию?

Выберите один из 4 вариантов ответа:

1) информирование

2) редактирование

3) изменение

4) декодирование

Задание 10

Вопрос:

Музыкальное произведение кодируется с помощью

Выберите один из 4 вариантов ответа:

1) азбуки Брайля

2) дорожных знаков

3) флажковой азбуки

4) нотных знаков

Ответы:

1) Верные ответы:

1;

2;

3;

2) Верные ответы: 1;

3) Верные ответы: 3;

4) Верный ответ: "информация".

5) Верный ответ: "пятиклассник".

6) Верные ответы: 2; 3; 4;

7) Верные ответы:

1;

3;

2;

8) Верный ответ: "код, кодом".

9) Верные ответы: 4;

10) Верные ответы: 4;

Критерии оценивания теста:

5 (отлично) – правильно выполнены 9-10 заданий.

4 (хорошо) – правильно выполнены 7-8 задания.

3 (удовлетворительно) – правильно выполнены 5-6 заданий.

2 (неудовлетворительно) – правильно выполнены менее 5 заданий.

ПРАКТИЧЕСКАЯ РАБОТА

«ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ АЛГОРИТМОВ КОДИРОВАНИЯ»

Цель: Познакомиться с различными кодировками символов, используя текстовые редакторы, выполнить задания в различных текстовых приложениях.

Оборудование: ПК.

Программное обеспечение: операционная система, текстовые редакторы.

Теоретические основы

Правило цифрового представления символов следующее: каждому символу ставится в соответствие некоторое целое число, то есть каждый символ нумеруется.

Пример:

Рассмотрим последовательность строчных букв русского алфавита: а, б, в, г, д, е, ё, ж, з, и, й. к, л, м. н. о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, в, э, ю, я. Присвоив каждой букве номер от 0 до 33. получим простейший способ представления символов. Последнее число - 32 в двоичной форме имеет вид 100000, то есть для хранения символа в памяти понадобится 6 бит.Так как с помощью шести бит можно представить число $2^6 - 1 = 63$, то шести бит будет достаточно для представления 64 букв.

Имеются разные стандарты для представления, символов, которые отличаются лишь порядком нумерации символов. Наиболее распространён американский стандартный код для информационного обмена - ASCII [American Standard-Code for Information Interchange] введён в США в 1963г. В 1977 году в несколько модифицированном виде он был принят в качестве всемирного стандарта Международной организации стандартов [International Standards Organization -. ISO] под названием ISO-646. Согласно этому стандарту каждому символу поставлено в соответствие число от 0 до 255. Символы от 0 до 127 - латинские буквы, цифры и знаки препинания - составляют постоянную часть таблицы. Остальные символы используются для представления национальных алфавитов. Конкретный состав этих символов определяется кодовой страницей. В русской версии ОС Windows95 используется кодовая, страница 866. В ОС Linux для представления русских букв более употребительна кодировка КОИ-8. Недостатки такого способа кодировки национального, алфавита очевидны. Во-первых, невозможно одновременное представление русских и ,например, французских букв. Во-вторых, такая кодировка совершенно непригодна для представления, китайских иероглифов. В 1991 году была создана некоммерческая организация Unicode, в которую входят представители ряда фирм (Borland. IBM, Noyell, Sun и др) и которая занимается развитием и внедрением нового стандарта. Кодировка

Unicode использует 16 разрядов ,и может содержать 65536 символов. Это символы большинства народов мира, элементы иероглифов, спецсимволы, 5000 – мест для частного использования, резерв из 30000 мест.

Пример:

ASCII-код символа A= 65_{10} =41_{16}= 01000111_2;

Unicode-код символа C= 67_{10}=0000000001100111_2

Задания

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

2. Раскодируйте ФИО соседа

3. Закодируйте следующие слова, используя таблицы ASCII-кодов: ИНФОРМАТИЗАЦИЯ, МИКРОПРОЦЕССОР, МОДЕЛИРОВАНИЕ

4. Раскодируйте следующие слова, используя таблицы ASCII-кодов:

88 AD E4 AE E0 AC A0 E2 A8 AA A0

50 72 6F 67 72 61 6D

43 6F 6D 70 75 74 65 72 20 49 42 4D 20 50 43

5. Текстовый редактор Блокнот

Открыть блокнот.

а) Используя клавишу Alt и малую цифровую клавиатуру раскодировать фразу: 145 170 174 224 174 255 170 160 173 168 170 227 171 235;

Технология выполнения задания: При удерживаемой клавише Alt, набрать на малой цифровой клавиатуре указанные цифры. Отпустить клавишу Alt, после чего в тексте появится буква, закодированная набранным кодом.

б) Используя ключ к кодированию, закодировать слово – зима;

Технология выполнения задания: Из предыдущего задания выяснить, каким кодом записана буква а. Учитывая, что буквы кодируются в алфавитном порядке, выяснить коды остальных букв.

Что вы заметили при выполнении этого задания во время раскодировки? Запишите свои наблюдения.

6. Текстовый процессор.

Технология выполнения задания: рассмотрим на примере: представить в различных кодировках слово Кодировка

Решение:

- Создать новый текстовый документ в текстовом редакторе;

- Выбрать – Команда – Вставка – Символ.

В открывшемся окне «Символ» установить из: Юникод (шестн.),

- В наборе символов находим букву К и щелкнем на ней левой кнопкой мыши (ЩЛКМ).

- В строке код знака появится код выбранной буквы 041А (незначащие нули тоже записываем).

- У буквы о код – 043Е и так далее: д – 0434, и – 0438, р – 0440, о – 043Е, в – 0432, к – 043А, а – 0430.

- Установить Кириллица (дес.)

- К – 0202, о – 0238, д – 0228, и – 0232, р – 0240, о – 0238, в –0226, к – 0202, а – 0224.

7. Открыть Текстовый редактор

Используя окно «Вставка символа» выполнить задания: Закодировать слово Forest

а) Выбрать шрифт Courier New, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116
б) Выбрать шрифт Courier New, кодировку Юникод(шест.) Ответ: 0046 006F 0072 0065 0073 0074

в) Выбрать шрифт Times New Roman, кодировку Кирилица(дес.) Ответ: 70 111 114 101 115 116

г) Выбрать шрифт Times New Roman, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116

Вывод: _____

Выполнение лабораторной работы оформить в виде таблицы.

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

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

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

11. С помощью десятичных кодов зашифровано слово «port» 112 111 114 116. Записать последовательность десятичных кодов для этого же слова, но записанного заглавными буквами. Ответ: 80 79 82 84

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Какие возможности предоставляет текстовые редакторы по работе с символами?

2. Какие вы знаете алгоритмы кодирования информации?

3. Где применяется алгоритм кодирования информации?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА «КОДИРОВАНИЕ ИНФОРМАЦИИ»

Цель: познакомиться с различными кодировками звуковой информации и с характеристиками звуковых файлов.

Оборудование: ПК.

Программное обеспечение: операционная система, звуковые редакторы.

Теоретические основы

С начала 90-х годов персональные компьютеры получили возможность работать со звуковой информацией. Каждый компьютер, имеющий звуковую плату, может сохранять в виде файлов (файл - это определённое количество информации, хранящееся на диске и имеющее имя) и воспроизводить звуковую информацию. С помощью специальных программных средств (редакторов аудио файлов) открываются широкие возможности по созданию, редактированию и прослушиванию звуковых файлов. Создаются программы распознавания речи, и появляется возможность управления компьютером голосом.

Именно звуковая плата (карта) преобразует аналоговый сигнал в дискретную фонограмму и наоборот, «оцифрованный» звук – в аналоговый (непрерывный) сигнал, который поступает на вход динамика.

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:

$$V_{моно} = \frac{\nu \cdot t \cdot G}{8},$$

где ν - частота дискретизации в Гц,
G – глубина звука в битах, t – время в секундах.

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

По мере усложнения программ и увеличения их функций, а также появления мультимедиа-приложений, растёт функциональный объём программ и данных. Если в середине 80-х годов обычный объём программ и данных составлял десятки и лишь иногда сотни килобайт, то в середине 90-х годов он стал составлять десятки мегабайт. Соответственно растёт объём оперативной памяти.

Пример решения: Подсчитать, сколько места будет занимать одна минута цифрового звука на жестком диске или любом другом цифровом носителе, записанного с частотой

а) 44.1 кГц;

б) 11 кГц;

в) 22 кГц;

г) 32 кГц

и разрядностью 16 бит.

Решение.

а) Если записывают моносигнал с частотой 44.1 кГц, разрядностью 16 бит (2 байта), то каждую минуту аналого-цифровой преобразователь будет выдавать 441000 * 2 * 60 = 529 000 байт (около 5 Мб) данных об амплитуде аналогового сигнала, который в компьютере записываются на жесткий диск.

Если записывают стереосигнал, то 1 058 000 байт (около 10 Мб).

Задания

1. Какой объем памяти требуется для хранения цифрового аудиофайла с записью звука высокого качества при условии, что время звучания составляет 3 минуты?

2. Какой объем данных имеет моноаудиофайл, длительность звучания которого 1 секунда, при среднем качестве звука (16 бит, 24 кГц)?

3. Рассчитайте объем стереоаудиофайла длительностью 20 секунд при 20-битном кодировании и частоте дискредитации 44.1 кГц. Варианты: 44,1 Mb, 4.21 Mb, 3,53 Mb.

4. Оцените информационный объем моноаудиофайла длительностью звучания 20 с, если "глубина" кодирования и частота дискретизации звукового сигнала равны соответственно 8 бит и 8 кГц;

5. Рассчитайте время звучания моноаудиофайла, если при 16-битном кодировании и частоте дискретизации 32 кГц его объем равен 700 Кбайт;

6. Запишите звуковой моноаудиофайл длительностью 20 с, с "глубиной" кодирования 8 бит и частотой дискретизации 8 кГц.

7. Определите качество звука (качество радиотрансляции, среднее качество, качество аудио-CD) если известно, что объем стериоаудиофайла длительностью звучания в 10 сек. Равен 940 Кбайт;

8. Оцените информационный объем стериоаудиофайла длительностью звучания 30 с, если "глубина" кодирования и частота дискретизации звукового сигнала равны соответственно 8 бит и 8 кГц;

9. Запишите звуковой файл длительностью 30с с "глубиной" кодирования 8бит и частотой дискретизации 8 кГц. Вычислите его объем и сверьтесь с полученным на практике значением.

10. Аналоговый звуковой сигнал был дискретизирован сначала с использованием 256 уровней интенсивности сигнала (качество звучания радиотрансляции), а затем с использованием 65536 уровней интенсивности сигнала (качество звучания аудио-CD). Во сколько раз различаются информационные объемы оцифрованного звука?

11. Оцените информационный объем моноаудиофайла длительностью звучания 1 мин. если "глубина" кодирования и частота дискретизации звукового сигнала равны соответственно:

16 бит и 48 кГц.

12. Запишите звуковой моноаудиофайл длительностью 1 минута с "глубиной" кодирования 16 бит и частотой дискретизации 48 кГц.

13. Подсчитать объем файла с 10 минутной речью записанного с частотой дискретизации 11025 Гц при 4 разрядном кодировании

14. Подсчитать время звучания звукового файла объемом 3.5 Мбайт содержащего стерео запись с частотой дискретизации 44100 Гц, 16-ти разрядном кодировании.

15. Определите количество уровней звукового сигнала при использовании 8-битных звуковых карт. Варианты: 256, 512,1024, 65 536.

16. Приведите пример:

а) аналогового способа представления звуковой информации;

б) дискретного способа представления звуковой информации.

17. Подготовить презентацию, демонстрирующую возможности звуковых форматов midi, wav, mp3, mod.

18. Перечислите параметры, от которых зависит качество двоичного кодирования звука.

Отчет

Отчет должен быть оформлен в текстовом редакторе и содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. С какими звуковыми форматами вы встречаетесь чаще в повседневной жизни?

2. Дайте определение аудиоадаптеру?

3. Что значит оцифровка звука?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«КОДИРОВАНИЕ ИНФОРМАЦИИ»

Цель: научиться кодировать растровые графические файлы; научиться измерять информационный объем графических файлов.

Оборудование: ПК.

Программное обеспечение: операционная система, графические редакторы.

Теоретические основы

Графическая информация на экране дисплея представляется в виде изображения, которое формируется из точек (пикселей). Всмотритесь в газетную фотографию, и вы увидите, что она тоже состоит из мельчайших точек. Если это только чёрные и белые точки, то каждую из них можно закодировать 1 битом. Но если на фотографии оттенки, то два бита позволяет закодировать 4 оттенка точек: 00 - белый цвет, 01 - светло-серый, 10 - тёмно-серый, 11 - чёрный. Три бита позволяют закодировать 8 оттенков и т.д.

Количество бит, необходимое для кодирования одного оттенка цвета, называется глубиной цвета.

$K=2^G$, где K – количество оттенков, G – глубина цвета в битах.

В современных компьютерах разрешающая способность (количество точек на экране), а также количество цветов зависит от видеоадаптера и может изменяться программно.

Цветные изображения могут иметь различные режимы: 16 цветов, 256 цветов, 65536 цветов (high color), 16777216 цветов (true color). На одну точку для режима high color необходимо 16 бит или 2 байта.

Наиболее распространённой разрешающей способностью экрана является разрешение 800 на 600 точек, т.е. 480000 точек. Рассчитаем необходимый для режима high color объём видеопамяти: 2 байт *480000=960000 байт.

Для измерения объёма информации используются и более крупные единицы:

1 Кбайт (один килобайт) = 2^{10} байт=1024 байт
1 Мбайт (один мегабайт) = 2^{20} байт=1048576 байт
1 Гбайт (один гигабайт) = 2^{30} байт=около1млрд. байт

Следовательно, 960000 байт приблизительно равно 937,5 Кбайт. Если человек говорит по восемь часов в день без перерыва, то за 70 лет жизни он наговорит около 10 гигабайт информации (это 5 миллионов страниц - стопка бумаги высотой 500 метров).

Скорость передачи информации - это количество битов, передаваемых в 1 секунду. Скорость передачи 1 бит в 1 секунду называется 1 бод.

1 Кбод = 1024 бит/сек; 1 Мбод = 1024 Кбод; 1 Гбод = 1024 Мбод

В видеопамяти компьютера хранится битовая карта, являющаяся двоичным кодом изображения, откуда она считывается процессором (не реже 50 раз в секунду) и отображается на экран.

Таблица. Объём видеопамяти в зависимости от типов разрешающей способности компьютеров.

Разрешение	**16 цветов**	**256 цветов**	**65536 цветов**	**16777216 цветов**
640 x 480	150 Кб	300 Кб	600 Кб	900 Кб
800 x 600	234,4 Кб	468,8 Кб	937,5 Кб	1,4 Мб
1024 x 768	384 Кб	768 Кб	1,5 Мб	2,25 Мб
1280x 1024	640 Кб	1,25 Мб	2,5 Мб	3,75 Мб

Задачи:

1. Известно, что видеопамять компьютера имеет объем 512 Кбайт. Разрешающая способность экрана 640 на 200. Сколько страниц экрана одновременно разместится в видеопамяти при палитре: а) из 8 цветов, б) 16 цветов; в) 256 цветов?
2. Сколько бит требуется, чтобы закодировать информацию о 130 оттенках?
3. Подумайте, как уплотнить информацию о рисунке при его записи в файл, если известно, что: а) в рисунке одновременно содержится только 16 цветовых оттенков из 138 возможных; б) в рисунке присутствуют все 130 оттенков одновременно, но количество точек, закрашенных разными оттенками, сильно различаются.
4. Найдите в сети Интернет информацию на тему «Цветовые модели HSB, RGB, CMYK» и создайте на эту тему презентацию. В ней отобразите положительные и отрицательные стороны каждой цветовой модели, принцип ее функционирования и применение.
5. В приложении «Точечный рисунок» создайте файл размером (по вариантам):

А) 200*300, (№ по списку 1, 8, 15, 22, 29)
Б) 590*350, (№ по списку 2, 9, 16, 23, 30)
В) 478*472, (№ по списку 3, 10, 17, 24, 31)
Г)190*367, (№ по списку 4, 11, 18, 25, 32)
Д) 288*577; (№ по списку 5, 12, 19, 26, 33)
Е) 100*466, (№ по списку 5, 13, 20, 27, 34)
Ж) 390*277. (№ по списку 6, 14, 21, 28)

Сохраните его под следующими расширениями:
- монохромный рисунок,
- 16-цветный рисунок,
- 256-цветный рисунок,
- 24-битный рисунок,
- формат JPG.

Используя информацию о размере каждого из полученных файлов, вычислите количество используемых цветов в каждом из файлов, проверьте с полученным на практике. Объясните, почему формула расчета количества цветов не подходит для формата JPG. Для этого воспользуйтесь информацией из сети Интернет.

6. На бумаге в клетку (или в приложении табличный редактор) нарисуйте произвольный рисунок 10*10 клеток. Закодируйте его двоичным кодом (закрашена клетка – 1, не закрашена - 0). Полученный код отдайте одногруппнику для раскодирования и получения изображения.

Отчет

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Влияет разрешение рисунка на объем файла?

2. Чем отличаются цветовые модели?

3. Что означает глубина цвета?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ДЕКОДИРОВАНИЕ ИНФОРМАЦИИ»

Цель работы: Ознакомление с правилами и получение практических навыков кодирования и декодирования информации.

Оборудование: ПК.

Программное обеспечение: операционная система, графические редакторы.

Теоретические основы

Кодирование информации это преобразование формы представления информации с целью ее передачи или хранения. Кодирование это представление символов одного алфавита символами другого. Правила, по которым осуществляется кодирование называются кодом. Под словом понимают последовательность символов, количество символов в которой называется длиной кода. Слова так же называют кодовыми комбинациями. Если при кодировании получают комбинации одинаковой длины, то такой код называют равномерным, а длину кодовых комбинаций в этом слове называют значимостью кода. Если кодовые комбинации различной длины, то код называется неравномерным.

Процесс обратный кодированию называется декодированием.

Если в коде ни одна более короткая комбинация не является началом более длинной кодовой комбинации, то код называется префиксным.

- кодирование – это перевод информации с одного языка на другой (запись в другой системе символов, в другом алфавите)
- обычно кодированием называют перевод информации с «человеческого» языка на формальный, например, в двоичный код, а декодированием – обратный переход
- один символ исходного сообщения может заменяться одним символом нового кода или несколькими символами, а может быть и наоборот – несколько символов исходного сообщения заменяются одним символом в новом коде (китайские иероглифы обозначают целые слова и понятия)
- кодирование может быть *равномерное* и *неравномерное*;
  при равномерном кодировании все символы кодируются кодами равной длины;
  при неравномерном кодировании разные символы могут кодироваться кодами разной длины, это затрудняет декодирование

Пример задания:

Для кодирования букв А, Б, В, Г решили использовать двухразрядные последовательные двоичные числа (от 00 до 11, соответственно). Если таким способом закодировать последовательность символов БАВГ и записать результат шестнадцатеричным кодом, то получится

1) $4B_{16}$ 2) 411_{16} 3)$BACD_{16}$ 4) 1023_{16}

Решение:

1) из условия коды букв такие: А – 00, Б –01, В – 10 и Г – 11, код равномерный
2) последовательность БАВГ кодируется так: 01 00 10 11 = 1001011
3) разобьем такую запись на тетрады справа налево и каждую тетраду переведемв шестнадцатеричную систему (то есть, сначала в десятичную, а потом заменим все числа от 10 до 15 на буквы A, B, C, D, E, F); получаем

$$1001011 = 0100\ 1011_2 = 4B_{16}$$

4) правильный ответ – 1.

Возможные ловушки:

- расчет на то, что при переводе тетрад в шестнадцатеричную систему можно забыть заменить большие числа (10–15) на буквы ($1011_2 = 11$, получаем неверный ответ 411_{16})
- может быть дан неверный ответ, в котором нужные цифры поменяли местами (расчет на невнимательность), например, $B4_{16}$
- в ответах дана последовательность, напоминающая исходную (неверный ответ $BACD_{16}$), чтобы сбить случайное угадывание

Пример задания:

Для 5 букв латинского алфавита заданы их двоичные коды (для некоторых букв – из двух бит, для некоторых – из трех). Эти коды представлены в таблице:

A	B	C	D	E
000	01	100	10	011

Определить, какой набор букв закодирован двоичной строкой 0110100011000

1) EBCEA 2) BDDEA 3) BDCEA 4) EBAEA

Решение (вариант 1, декодирование с начала):

1) здесь используется неравномерное кодирование, при котором декодирование может быть неоднозначным, то есть, заданному коду может соответствовать несколько разных исходных сообщений
2) попробуем декодировать с начала цепочки, первой буквой может быть B или E, эти случаи нужно рассматривать отдельно
3) пусть первая буква – E с кодом 011, тогда остается цепочка 0100011000
   - для кода 0100011000 первой буквой может быть только B с кодом 01, тогда остается 00011000 (начало исходной цепочки – EB?)
   - для кода 00011000 первой буквой может быть только A с кодом 000, тогда остается 11000, а эта цепочка не может быть разложена на заданные коды букв
   - поэтому наше предположение о том, что первая буква – E, неверно
4) пусть первая буква – B с кодом 01, тогда остается цепочка 10100011000
   - для кода 10100011000 первой буквой может быть только D с кодом 10, тогда остается 100011000 (можно полагать, что начало исходной цепочки – BD?)
   - для кода 100011000 первой буквой может быть только C с кодом 100, тогда остается 011000 (начало исходной цепочки – BDC?)

     Несмотря на то, что среди ответов есть единственная цепочка, которая начинается с BDC, здесь нельзя останавливаться, потому что «хвост» цепочки может «не сойтись»
   - для кода 011000 на первом месте может быть B (код 01) или E (011); в первом случае «хвост» 1000 нельзя разбить на заданные коды букв, а во втором –

остается код 000 (буква А), поэтому исходная цепочка может быть декодирована как BDCEA

5) правильный ответ – 3

Возможные ловушки и проблемы:

- при декодировании неравномерных кодов может быть очень много вариантов, их нужно рассмотреть все; это требует серьезных усилий и можно легко запутаться
- нельзя останавливаться, не закончив декодирование до конца и не убедившись, что все «сходится», на это обычно и рассчитаны неверные ответы

Решение (вариант 2, декодирование с конца):

1) для кода 0110100011000 последней буквой может быть только А (код 000), тогда остается цепочка 0110100011
2) для 0110100011 последней может быть только буква Е (011), тогда остается цепочка 0110100
3) для 0110100 последней может быть только буква С (100), тогда остается цепочка 0110
4) для 0110 последней может быть только буква D (10), тогда остается 01 – это код буквы В
5) таким образом, получилась цепочка BDCEA
6) правильный ответ – 3

Возможные ловушки и проблемы:

- при декодировании неравномерных кодов может быть очень много вариантов (здесь *случайно* получилась единственно возможная цепочка), их нужно рассмотреть все; это требует серьезных усилий и можно легко запутаться
- нельзя останавливаться, не закончив декодирование до конца и не убедившись, что все «сходится», на это обычно и рассчитаны неверные ответы

Решение (вариант 3, кодирование ответов):

1) в данном случае самое простое и надежное – просто закодировать все ответы, используя приведенную таблицу кодов, а затем сравнить результаты с заданной цепочкой
2) получим

1) EBCEA – 01101100011000 2) BDDEA – 011010011000

3) BDCEA – 0110100011000 4) EBAEA – 01101000011000

3) сравнивая эти цепочки с заданной, находим, что правильный ответ – 3.

Возможные проблемы:

- сложно сравнивать длинные двоичные последовательности, поскольку они однородны, содержат много одинаковых нулей и единиц

Пример задания:

Для передачи по каналу связи сообщения, состоящего только из букв А, Б, В, Г, решили использовать неравномерный по длине код: А=0, Б=10, В=110. Как нужно закодировать букву Г, чтобы длина кода была минимальной и допускалось однозначное разбиение кодированного сообщения на буквы?

1) 1 2) 1110 3) 111 4) 11

Решение (вариант 1, метод подбора):

1) рассмотрим все варианты в порядке увеличения длины кода буквы Г
2) начнем с Г=1; при этом получается, что сообщение «10» может быть раскодировано двояко: как ГА или Б, поэтому этот вариант не подходит
3) следующий по длине вариант – Г=11; в этом случае сообщение «110» может быть раскодировано как ГА или В, поэтому этот вариант тоже не подходит
4) третий вариант, Г=111, дает однозначное раскодирование во всех сочетаниях букв, поэтому…
5) … правильный ответ – 3.

Возможные проблемы:
- при переборе можно ошибиться и «просмотреть» какой-нибудь вариант

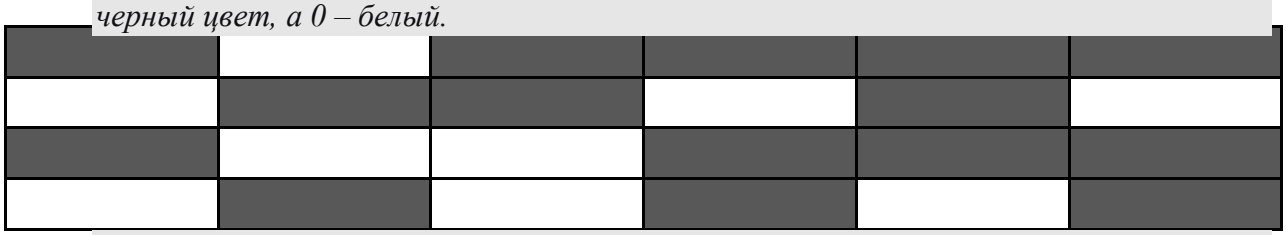
Решение (вариант 2, «умный» метод):

1) для того, чтобы сообщение, записанное с помощью неравномерного по длине кода, однозначно раскодировалось, требуется, чтобы никакой код не был началом другого (более длинного) кода; это условие называют *условием Фано*
2) как и в первом решении, рассматриваем варианты, начиная с самого короткого кода для буквы Г; в нашем случае код Г=1 является началом кодов букв Б и В, поэтому условие Фано не выполняется, такой код не подходит
3) код Г=11 также является началом другого кода (кода буквы В), поэтому это тоже ошибочный вариант
4) третий вариант кода, Г=111, не является началом никакого уже известного кода; кроме того, ни один уже имеющийся код не является началом кода 111; таким образом, условие Фано выполняется
5) поэтому правильный ответ – 3.

Возможные проблемы:
- нужно знать условие Фано

Пример задания:

Черно-белое растровое изображение кодируется построчно, начиная с левого верхнего угла и заканчивая в правом нижнем углу. При кодировании 1 обозначает черный цвет, а 0 – белый.

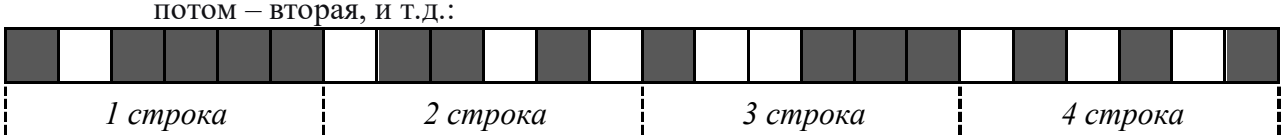


Для компактности результат записали в шестнадцатеричной системе счисления. Выберите правильную запись кода.

1) BD9AA5 2) BDA9B5 3) BDA9D5 4) DB9DAB

Решение:

1) «вытянем» растровое изображение в цепочку: сначала первая (верхняя) строка, потом – вторая, и т.д.:



1 строка	*2 строка*	*3 строка*	*4 строка*

2) в этой полоске 24 ячейки, черные заполним единицами, а белые – нулями:

1	*0*	*1*	*1*	*1*	*1*	*0*	*1*	*1*	*0*	*1*	*0*	*1*	*0*	*0*	*1*	*1*	*1*	*0*	*1*	*0*	*1*	*0*	*1*
1 строка						*2 строка*						*3 строка*						*4 строка*					

3) поскольку каждая цифра в шестнадцатеричной системе раскладывается ровно в 4 двоичных цифры, разобьем полоску на тетрады – группы из четырех ячеек (в данном случае все равно, откуда начинать разбивку, поскольку в полоске целое число тетрад – 6):

1	*0*	*1*	*1*	*1*	*1*	*0*	*1*	*1*	*0*	*1*	*0*	*1*	*0*	*0*	*1*	*1*	*1*	*0*	*1*	*0*	*1*	*0*	*1*

4) переводя тетрады в шестнадцатеричную систему, получаем последовательно цифры B (11), D(13), A(10), 9, D(13) и 5, то есть, цепочку BDA9D5

5) поэтому правильный ответ – 3.

Возможные проблемы:

- нужно уметь быстро переводить тетрады в шестнадцатеричные цифры (в крайнем случае, это можно сделать через десятичную систему)

Пример задания:

Для передачи чисел по каналу с помехами используется код проверки четности. Каждая его цифра записывается в двоичном представлении, с добавлением ведущих нулей до длины 4, и к получившейся последовательности дописывается сумма её элементов по модулю 2 *(например, если передаём* 23*, то получим последовательность* 0010100110*). Определите, какое число передавалось по каналу в виде* 01010100100111100011*?*

1) 59143 2) 5971 3) 102153 4) 10273

Решение:

1) сначала разберемся, как закодированы числа в примере; очевидно, что используется код равномерной длины; поскольку 2 знака кодируются 10 двоичными разрядами (битами), на каждую цифру отводится 5 бит, то есть
   2 → 00101 и 3 → 00110
2) как следует из условия, четыре первых бита в каждой последовательности – это двоичный код цифры, а пятый бит (бит четности) используется для проверки и рассчитывается как «сумма по модулю два», то есть остаток от деления суммы битов на 2; тогда
   $2 = 0010_2$, бит четности (0 + 0 + 1 + 0) mod 2 = 1
   $3 = 0011_2$, бит четности (0 + 0 + 1 + 1) mod 2 = 0
3) но бит четности нам совсем не нужен, важно другое: пятый бит в каждой пятерке можно отбросить!
4) разобъем заданную последовательность на группы по 5 бит в каждой:
   01010, 10010, 01111, 00011.
5) отбросим пятый (последний) бит в каждой группе:
   0101, 1001, 0111, 0001.

это и есть двоичные коды передаваемых чисел:

$0101_2 = 5$, $1001_2 = 9$, $0111_2 = 7$, $0001_2 = 1$.

6) таким образом, были переданы числа 5, 9, 7, 1 или число 5971.
7) Ответ: 2.

Отчет

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Где применяется кодирование информации?

2. Дать определение понятие декодер?

3. Какие существуют методы декодирования?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

РАЗДЕЛ 4. ОСНОВЫ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

УСТНЫЙ ОПРОС ПО ТЕМЕ

«СТАНДАРТЫ ШИФРОВАНИЯ ДАННЫХ. КРИПТОГРАФИЯ»

Вопросы:

1. Понятие криптографии,
2. Использование криптографии на практике
3. Различные методы криптографии
4. Свойства шифрования
5. Методы шифрования

Критерии оценки устного ответа:

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ТЕСТ НА ТЕМУ «КРИПТОГРАФИЯ»

1. Шифрование – это…

А) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

Б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

В) удобная среда для вычисления конечного пользователя

2. Кодирование – это…

А) преобразование обычного, понятного текста в код

Б) преобразование

В) написание программы

3. Что требуется для восстановления зашифрованного текста

А) ключ

Б) матрица

В) вектор

4. Когда появилось шифрование

А) четыре тысячи лет назад

Б) две тысячи лет назад

В) пять тысяч лет назад

5. Первым известным применением шифра считается

А) египетский текст

Б) русский

В) нет правильного ответа

6. Какую секретную информацию хранит Windows

А) пароли для доступа к сетевым ресурсам

Б) пароли для доступа в Интернет

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

7. Алфавит – это…

А) конечное множество используемых для кодирования информации знаков

Б) буквы текста

В) нет правильного ответа

8. Текст – это…

А) упорядоченный набор из элементов алфавита

Б) конечное множество используемых для кодирования информации знаков

В) все правильные

9. Примеры алфавитов:

А) Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8

Б) восьмеричный и шестнадцатеричный алфавиты

В) AEE

10. Шифрование – это…

А) преобразовательный процесс исходного текста в зашифрованный

Б) упорядоченный набор из элементов алфавита

В) нет правильного ответа

11. Дешифрование – это…

А) на основе ключа шифрованный текст преобразуется в исходный

Б) пароли для доступа к сетевым ресурсам

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Криптографическая система представляет собой…

А) семейство T преобразований открытого текста, члены его семейства индексируются символом k

Б) программу

В) систему

13. Пространство ключей k – это…

А) набор возможных значений ключа

Б) длина ключа

В) нет правильного ответа

14. Криптосистемы разделяются на:

А) симметричные

Б) ассиметричные

В) с открытым ключом

15. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования

А) 1

Б) 2

В) 3

16. Сколь ключей используется в системах с открытым ключом

А) 2

Б) 3

В) 1

17. Какие ключи используются в системах с открытым ключом

А) открытый

Б) закрытый

В) нет правильного ответа

18. Как связаны ключи друг с другом в системе с открытым ключом

А) математически

Б) логически

В) алгоритмически

19. Электронной подписью называется…

А) присоединяемое к тексту его криптографическое преобразование

Б) текст

В) зашифрованный текст

20. Криптостойкость – это…

А) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа

Б) свойство гаммы

В) все ответы верны

21. Показатели криптостойкости:

А) количество всех возможных ключей

Б) среднее время, необходимое для криптоанализа

В) количество символов в ключе

22. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) знание алгоритма шифрования не должно влиять на надежность защиты

Б) структурные элементы алгоритма шифрования должны быть неизменными

В) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) длина шифрованного текста должна быть равной лине исходного текста

Б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа

В) нет правильного ответа

24. Основные современные методы шифрования:

А) алгоритма гаммирования

Б) алгоритмы сложных математических преобразований

В) алгоритм перестановки

25. Символы исходного текста складываются с символами некой случайной последовательности – это…

А) алгоритм гаммирования

Б) алгоритм перестановки

В) алгоритм аналитических преобразований

26. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…

А) алгоритм перестановки

Б) алгоритм подстановки

В) алгоритм гаммрования

27. Самой простой разновидность подстановки является

А) простая замена

Б) перестановка

В) простая перестановка

28. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера

А) 3

Б) 4

В) 5

29. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования

А) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке

Б) в качестве ключа используется случайность последовательных чисел

В) нет правильного ответа

30. В чем суть метода перестановки

А) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов

Б) замена алфавита

В) все правильные

31. Сколько существует способов гаммирования

А) 2

Б) 5

В) 3

32. Чем определяется стойкость шифрования методом гаммирования

А) свойством гаммы

Б) длина ключа

В) нет правильного ответа

33. Что может использоваться в качестве гаммы

А) любая последовательность случайных символов

Б) число

В) все ответы верны

34. Какой метод используется при шифровании с помощью аналитических преобразований

А) алгебры матриц

Б) матрица

В) факториал

35. Что используется в качестве ключа при шифровании с помощью аналитических преобразований

А) матрица А

Б) вектор

В) обратная матрица

36. Как осуществляется дешифрование текста при аналитических преобразованиях

А) умножение матрицы на вектор

Б) деление матрицы на вектор

В) перемножение матриц

37. Комбинации комбинированного метода шифрования:

А) подстановка+гаммирование

Б) гаммирование+гаммирование

В) подстановка+перестановка

38. Для чего использовался DES-алгоритм из-за небольшого размер ключа

А) закрытия коммерческой информации

Б) шифрования секретной информации

В) нет правильного ответа

39. Основные области применения DES-алгоритма

А) хранение данных на компьютере

Б) электронная система платежей

В) аутентификация сообщений

40. Когда был введен в действие ГОСТ 28147-89

А) 1990

Б) 1890

В) 1995

41. Достоинства ГОСТа 28147-89

А) высокая стойкость

Б) цена

В) гибкость

42. Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма

А) отсутствием начальной перестановки и числом циклов шифрования
Б) длиной ключа
В) методом шифрования

43. Ключ алгоритма ГОСТ – это…
А) массив, состоящий из 32-мерных векторов
Б) последовательность чисел
В) алфавит

44. Какой ключ используется в шифре ГОСТ
А) 256-битовый
Б) 246-битовый
В) 356-битовый

45. Примеры программных шифраторов:
А) PGP
Б)BestCrypt 6.04
В) PTR

46. Плюсы программных шифраторов:
А) цена
Б) гибкость
В) быстродействие

47. УКЗД – это…
А) устройство криптографической защиты данных
Б) устройство криптографической заданности данных
В) нет правильного ответа

48. Блок управления – это…
А) основной модуль шифратора, который «заведует» работой всех остальных
Б) устройство криптографической заданности данных
В) проходной шифратор

49. Вычислитель – это…

А) набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных

Б) файлы, использующие различные методы кэширования

В) язык описания данных

50. Блок управления – это…

А) аппаратно реализованная программа, управляющая вычислителем

Б) язык описания данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

51. Какой шифратор можно использовать для защиты передаваемой в Сеть информации

А) обычный шифратор

Б) проходной шифратор

В) табличный шифратор

52. Египетский текст дотировался примерно…

А) 1900 г. д. н.э.

Б) 1890 г. д. н.э.

В) 1990 г.

53. Один из самых известных методов шифрования носит имя…

А) Цезаря

Б) Гейца

В) Вижинера

54. Из каких структурных единиц состоит шифропроцессор

А) вычислитель

Б) блок управления

В) буфер ввода-вывода

55. Криптографические действия выполняет…

А) вычислитель

Б) буфер ввода-вывода

В) блок управления

56. Наиболее известные разновидности полиалфавита:

А) одноконтурные

Б) многоконтурные

В) поликрнтурные

57. Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это…

А) виртуальный контейнер

Б) файл

В) программа

58. Устройство, дающее статически случайный шум – это…

А) генератор случайных чисел

Б) контроль ввода на компьютер

В) УКЗД

59. Какие дополнительные порты ввода-вывода содержит УКЗД:

А) COM

Б) USB

В) FGR

60. Сколько существует перестановок в стандарте DES

А) 3

Б) 4

В) 2

61. Какие перестановки существуют в стандарте DES

А) простые
Б) расширенные
В) сокращенные

62. Как называется модификация DESa
А) Triple Des
Б) M-506
В) Deh

63. Шифрование – это…
А) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
Б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
В) удобная среда для вычисления конечного пользователя

64. Кодирование – это…
А) преобразование обычного, понятного текста в код
Б) преобразование
В) написание программы

65. Что требуется для восстановления зашифрованного текста
А) ключ
Б) матрица
В) вектор

66. Когда появилось шифрование
А) четыре тысячи лет назад
Б) две тысячи лет назад
В) пять тысяч лет назад

67. Первым известным применением шифра считается
А) египетский текст
Б) русский
В) нет правильного ответа

68. Какую секретную информацию хранит Windows

А) пароли для доступа к сетевым ресурсам

Б) пароли для доступа в Интернет

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

69. Алфавит – это…

А) конечное множество используемых для кодирования информации знаков

Б) буквы текста

В) нет правильного ответа

70. Текст – это…

А) упорядоченный набор из элементов алфавита

Б) конечное множество используемых для кодирования информации знаков

В) все правильные

71. Примеры алфавитов:

А) Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8

Б) восьмеричный и шестнадцатеричный алфавиты

В) AEE

72. Шифрование – это…

А) преобразовательный процесс исходного текста в зашифрованный

Б) упорядоченный набор из элементов алфавита

В) нет правильного ответа

73. Дешифрование – это…

А) на основе ключа шифрованный текст преобразуется в исходный

Б) пароли для доступа к сетевым ресурсам

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

74. Криптографическая система представляет собой…

А) семейство T преобразований открытого текста, члены его семейства индексируются символом k

Б) программу

В) систему

75. Пространство ключей k – это…

А) набор возможных значений ключа

Б) длина ключа

В) нет правильного ответа

76. Криптосистемы разделяются на:

А) симметричные

Б) ассиметричные

В) с открытым ключом

77. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования

А) 1

Б) 2

В) 3

78. Сколь ключей используется в системах с открытым ключом

А) 2

Б) 3

В) 1

79. Какие ключи используются в системах с открытым ключом

А) открытый

Б) закрытый

В) нет правильного ответа

80. Как связаны ключи друг с другом в системе с открытым ключом

А) математически

Б) логически

В) алгоритмически

81. Электронной подписью называется…

А) присоединяемое к тексту его криптографическое преобразование

Б) текст

В) зашифрованный текст

82. Криптостойкость – это…

А) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа

Б) свойство гаммы

В) все ответы верны

83. Показатели криптостойкости:

А) количество всех возможных ключей

Б) среднее время, необходимое для криптоанализа

В) количество символов в ключе

84. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) знание алгоритма шифрования не должно влиять на надежность защиты

Б) структурные элементы алгоритма шифрования должны быть неизменными

В) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

85. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) длина шифрованного текста должна быть равной лине исходного текста

Б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа

В) нет правильного ответа

86. Основные современные методы шифрования:

А) алгоритма гаммирования

Б) алгоритмы сложных математических преобразований

В) алгоритм перестановки

87. Символы исходного текста складываются с символами некой случайной последовательности – это…

А) алгоритм гаммирования

Б) алгоритм перестановки

В) алгоритм аналитических преобразований

88. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…

А) алгоритм перестановки

Б) алгоритм подстановки

В) алгоритм гаммрования

89. Самой простой разновидность подстановки является

А) простая замена

Б) перестановка

В) простая перестановка

90. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера

А) 3

Б) 4

В) 5

91. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования

А) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке

Б) в качестве ключа используется случайность последовательных чисел

В) нет правильного ответа

92. В чем суть метода перестановки

А) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов

Б) замена алфавита

В) все правильные

93. Сколько существует способов гаммирования

А) 2

Б) 5

В) 3

94. Чем определяется стойкость шифрования методом гаммирования

А) свойством гаммы

Б) длина ключа

В) нет правильного ответа

95. Что может использоваться в качестве гаммы

А) любая последовательность случайных символов

Б) число

В) все ответы верны

96. Какой метод используется при шифровании с помощью аналитических преобразований

А) алгебры матриц

Б) матрица

В) факториал

97. Что используется в качестве ключа при шифровании с помощью аналитических преобразований

А) матрица А

Б) вектор

В) обратная матрица

98. Как осуществляется дешифрование текста при аналитических преобразованиях

А) умножение матрицы на вектор

Б) деление матрицы на вектор

В) перемножение матриц

99. Комбинации комбинированного метода шифрования:

А) подстановка+гаммирование

Б) гаммирование+гаммирование

В) подстановка+перестановка

100. Для чего использовался DES-алгоритм из-за небольшого размер ключа

А) закрытия коммерческой информации

Б) шифрования секретной информации

В) нет правильного ответа

101. Основные области применения DES-алгоритма

А) хранение данных на компьютере

Б) электронная система платежей

В) аутентификация сообщений

102. Когда был введен в действие ГОСТ 28147-89

А) 1990

Б) 1890

В) 1995

103. Достоинства ГОСТа 28147-89

А) высокая стойкость

Б) цена

В) гибкость

104. Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма

А) отсутствием начальной перестановки и числом циклов шифрования

Б) длиной ключа

В) методом шифрования

105. Ключ алгоритма ГОСТ – это…

А) массив, состоящий из 32-мерных векторов

Б) последовательность чисел

В) алфавит

106. Какой ключ используется в шифре ГОСТ

А) 256-битовый

Б) 246-битовый

В) 356-битовый

107. Примеры программных шифраторов:

А) PGP

Б)BestCrypt 6.04

В) PTR

108. Плюсы программных шифраторов:

А) цена

Б) гибкость

В) быстродействие

109. УКЗД – это…

А) устройство криптографической защиты данных

Б) устройство криптографической заданности данных

В) нет правильного ответа

110. Блок управления – это…

А) основной модуль шифратора, который «заведует» работой всех остальных

Б) устройство криптографической заданности данных

В) проходной шифратор

111. Вычислитель – это…

А) набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных

Б) файлы, использующие различные методы кэширования

В) язык описания данных

112. Блок управления – это…

А) аппаратно реализованная программа, управляющая вычислителем

Б) язык описания данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

113. Какой шифратор можно использовать для защиты передаваемой в Сеть информации

А) обычный шифратор

Б) проходной шифратор

В) табличный шифратор

114. Египетский текст дотировался примерно…

А) 1900 г. д. н.э.

Б) 1890 г. д. н.э.

В) 1990 г.

115. Один из самых известных методов шифрования носит имя…

А) Цезаря

Б) Гейца

В) Вижинера

116. Из каких структурных единиц состоит шифропроцессор

А) вычислитель

Б) блок управления

В) буфер ввода-вывода

117. Криптографические действия выполняет…

А) вычислитель

Б) буфер ввода-вывода

В) блок управления

118. Наиболее известные разновидности полиалфавита:

А) одноконтурные

Б) многоконтурные

В) поликрнтурные

119. Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это…

А) виртуальный контейнер

Б) файл

В) программа

120. Устройство, дающее статически случайный шум – это…

А) генератор случайных чисел

Б) контроль ввода на компьютер

В) УКЗД

121. Какие дополнительные порты ввода-вывода содержит УКЗД:

А) COM

Б) USB

В) FGR

122. Сколько существует перестановок в стандарте DES

А) 3

Б) 4

В) 2

123. Какие перестановки существуют в стандарте DES

А) простые

Б) расширенные

В) сокращенные

124. Как называется модификация DESa

А) Triple Des

Б) M-506

В) Deh

Критерии оценивания теста:

5 (отлично) – правильно выполнены 115-124 заданий.

4 (хорошо) – правильно выполнены 99-114 задания.

3 (удовлетворительно) – правильно выполнены 75-98 заданий.

2 (неудовлетворительно) – правильно выполнены менее 75 заданий.

ПРАКТИЧЕСКАЯ РАБОТА

«ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ КРИПТОГРАФИИ»

Цель работы: исследование простейших методов криптографической зашиты информации.

Программное обеспечение: операционная система, калькулятор.

Теоретические основы

Под *конфиденциальностью* понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности.

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Алфавит - конечное множество используемых для кодирования информации знаков.

Текст - упорядоченный набор из элементов алфавита. В качестве примеров алфавитов можно привести следующие:

алфавит $Z_{33\ -\ 32}$ буквы русского алфавита (исключая "ё") и пробел;

алфавит Z_{256} - символы, входящие в стандартные коды ASCII и КОИ-8;

двоичный алфавит - $Z_2 = \{0, 1\}$;

восьмеричный или шестнадцатеричный алфавит

Под *шифром* понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования. В шифре всегда различают два элемента: алгоритм и ключ. Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Криптографическая система, или *шифр* представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число k,

называемое *ключом.* Преобразование *Tk* определяется соответствующим алгоритмом и значением ключа *k.*

Ключ - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному.

Пространство ключей *K* - это набор возможных значений ключа.

Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия "ключ" и "пароль". *Пароль* также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а *расшифрованием* данных - процесс преобразования закрытых данных в открытые с помощью шифра.

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

Шифрованием называется процесс зашифрования или расшифрования данных. Также термин шифрование используется как синоним зашифрования. Однако неверно в качестве синонима шифрования использовать термин "кодирование" (а вместо "шифра" - "код"), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Криптология - это наука о преобразовании информации для обеспечения ее секретности, состоящая из двух ветвей: криптографии и криптоанализа.

Криптоанализ - наука (и практика ее применения) о методах и способах вскрытия шифров.

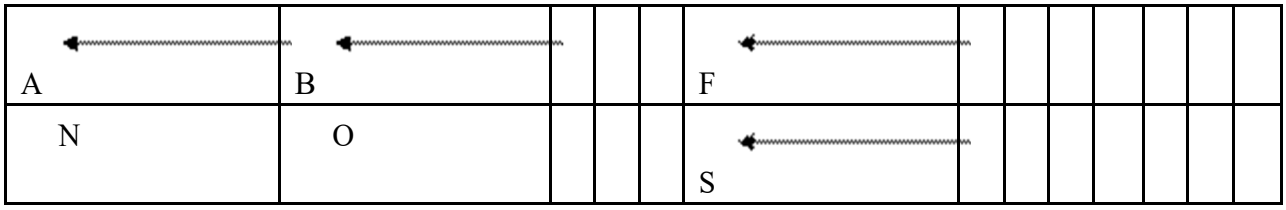
Криптография - наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития новых подходов и методов.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря

VENI VI D I VICI, где



пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в

SBKF SFAF SFZF

при смещении на 4 символа влево.

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый полибианский квадрат размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в зашифрованное сообщение букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

M	T	L	E	X
A	K	F	Q	Y
N	B	R	O	W
C	J	H	D	P
U	I	S	G	V

Схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. На рисунке показана верхняя часть таблицы Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

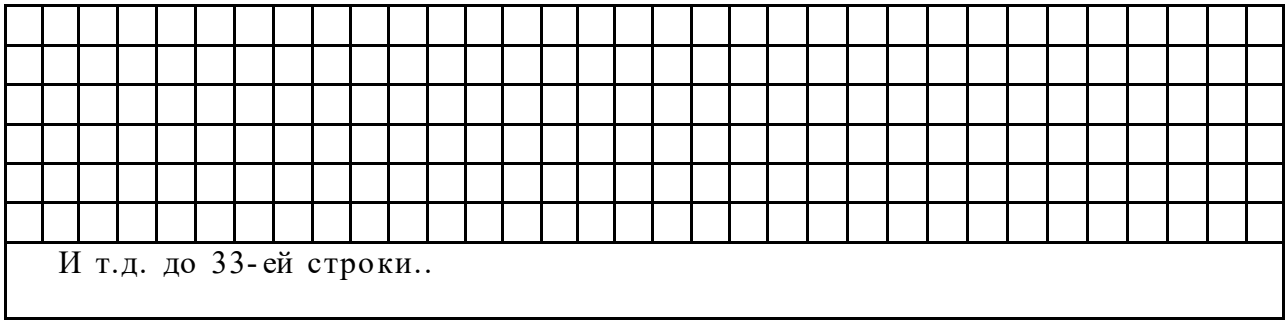


Таблица Вижинера

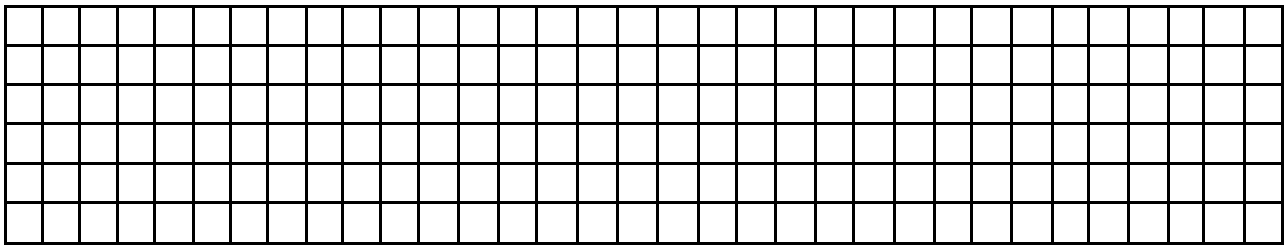
Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе шифрования. Пример такой рабочей матрицы для ключа «книга» .

Процесс шифрования осуществляется следующим образом:

1. под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз.
2. каждая буква шифруемого текста заменяется по подматрице буквами находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящимися под ними букв ключа.
3. полученный текст может разбиваться на группы по несколько знаков.

Пусть, например, требуется зашифровать сообщение: *максимально допустимой ценой является пятьсот руб. за штуку*. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

максимально допустимой ценой является пятьсот руб. за штуку
книгакнигак нигакнигак нигак нигакниг акнигак ниг ак нигак



Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (К); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (К),— в нашем примере такой буквой является Ч; выбранную таким образом букву помещаем в зашифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по таблице Вижинера эквивалентна простой

замене с циклическим изменением алфавита, т.е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т.е. число букв в ключе.

Расшифровка текста производится в следующей последовательности:

1. над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз.
2. в строке подматрицы Вижинера, соответствующей букве ключа отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста.
3. полученный текст группируется в слова по смыслу.

Нетрудно видеть, что процедуры как прямого, так и обратного преобразования являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключи с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв не имеющих смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем только некоторые из них:

- во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке.
- В качестве ключа используется случайность последовательных чисел. Из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе.

Известны также и многие другие модификации метода.

Алгоритм перестановки

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ.

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЪ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой

(например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительные изменения, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявляются серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

П У С Т Ь Б У Д Е Т Т А К К А

К М Ы Х О Т Е Л И К Л М Н О П

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-решетка, в который можно записывать исходный текст. Но тут уже потребуется предварительная договоренность между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать к нее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и по диагоналями, а для шифрования можно брать тоже различные направления.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Зашифрованное сообщение получают примерно также, как в шифре Цезаря, но используют не одно жестко заданное смещение а фрагменты ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда сообщение

С О В Е Р Ш Е Н Н О С Е К Р Е Т Н О

3 1 4 3 1 4 3 1 4 3 1 4 3 1 4 3 1 4

Ф П Ё С Ь З О С С А Х З Л Ф З У С С

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Зашифрованное сообщение получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

ПРИЕЗЖАЮ_ШЕСТОГО

АГАВААГАВААГАВАА

ПОИГЗЖЮЮЮШЕПТНГО

Такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Практическое задание

Придумайте 3 фразы, каждая минимум из 7 слов. Реализуйте шифрование этой фразы всеми перечисленными видами шифрования.

«Практика криптографической защиты информации»

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.
   Задание 1: Придумать акростих, в котором скрыто ваше имя.

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."

   Задание 2: Придумать подобное послание.

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. КРИПТОГРАФИЯ - ИПКРГРТОИЯАФ. (ИП↔ КР ГР↔ ТО ИЯ↔ АФ)

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

1. 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.

Задание 3:

1. Зашифровать:
   a) Французский математик Пьер Ферма по образованию был юрист.
   b) Леонардо Пизанского математики знают под именем "сын добряка" или Фибоначчи.
2. Дешифровать (восстановить сообщение, зная ключ) Ключ 8.
   Чинои сечем лчгмс хыеоо еаитн ккыин лтсбч втрйы еоосс ееорс неомв бадер покп.
   Примечание: АБ-дополнительные буквы.
3. Расшифровать (восстановить сообщение, не зная ключа).
   Осуз уаан евем исчи тдьм одоа ьлвь рдво быи.
4. Расшифровать:
   Етгртуой дкмиуиав цлишлаег врныинис аяоплыдб аанполбр.

2. Ключом является правило расстановки.

В О Е С М А Л А

С Р Н Е Т О

К А Т И К

Я А Ч Ш

Воесмала срнето катик яачш мея са к.

Или

Воес мала срне тока тикя ачшм еяса к.

М Е Я

С А

К

Задание 4:

1. Расшифровать фразу: Сошки ввнлы охеде нванз бркое еуквс изазх.
2. Расшифровать фразу: Леор тиюд тнет мауа ялее очнм кжхо йчей ооот лсеч и_пчс днит _киех са_чл илж_а шоо_в рп_уо_ к_ _

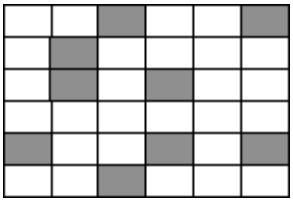
Постолбцовая транспозиция

К	А	Ш	А	Лшше ссис пссл шшао соак ааои ау.
3	1	4	2	Над столбцами записывается ключевое слово, затем в соответствии с порядком букв в алфавите столбцы
Ш	Л	А	С	нумеруются, а затем выписываются подряд: первый
А	Ш	А	П	столбец, за ним второй и т.д. Ключ здесь - "каша".
О	Ш	О	С	
С	Е	И	С	
О	С	А	Л	
А	С	У	Ш	
К	И			

Задание 5:

1. Зашифруйте фразу: Не плюй в колодец: вылетит - не поймаешь.
2. Дешифруйте старинное японское хайку: (ключом будет имя известного японского поэта "Басё") Тйдг адга лвис ыуы лояк пкшр ррув лшсс иеап пнву увет н.
3. Расшифруйте высказывание Козьмы Пруткова: Ако еаь дне дсц тан жод сск даг рео о.

Шифр "Решетка"



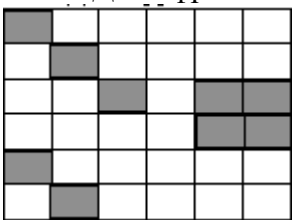
Если хочешь быть красивым поступи в гусары. (Высказывание Козьмы Пруткова)

Пьеиис влыбым тивхгь укпрос оарчсе ташуыс.

Ключом является решетка

Задание 6:

1. Придумать решетку и зашифровать фразу:
   "Евклид был древнегреческим математиком"
2. Дешифровать:

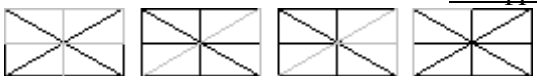


а) Сиекпе тпароо коолко йслтйс тськво нвоски.

б) Двплго раимид рувтай гуекте гньдот ыоруам.

Шифры замены

Шифр "Британский флаг"



Ответ: флаг.

Задание 7: зашифровать фразу: "ВГГУ".

Каждая буква заменяется несколькими символами

Криптография 11179161915417121932

К1К7А9К6К9К5А4К7А1Ф1А9Ю2

И2О2ИО1О4ОА3О2АУ1ИЯ

Задание 8:

1. Расшифровать: 1111712 20 111211728 201117112 11517112121228
2. Расшифровать: 11212941191517 16122812 1615 176116 111514415
3. Расшифровать: 11176191832 5157529 1815291716191832
4. Расшифровать: И1А2А5И5О4 Е3И5О4Я1О2 Я1И5О4Е3И5 И6О1И6О1О5 И3Ю1О2И5У8 И1А3И6И3Е3 А2О5А4О3И2 Е3И1О2А5Е1 Е3О3О3А5О2.

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.

Задание 9: расшифровать текст:

Сзргйзю тсуцълн Уйиефнлм цкрго, ъхс зов кргнспфхег ф зиецынсм ргзс тсзсмхл, ритулрцйзиррс тсжсесулхя с тсжзси л тсфои ахсжс туизфхгелхяфв. Рг сзрсм лк тусжцосн ср тсефхуиъго жцовбьцб ф дсосрнсм зиецынц. Тсуцълн тсзсыио н рим, трцо ии дсосрнц хгн, ъхс хг згоинс цоихиог л фнгкго:

- Рлкнс оихлх. Елзгхя, н зсйзб. Нфхгхл, угкуиылхи туизфхгелхяфв, тсуцълн Уйиефнлм.

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			

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.

Задание 10: расшифровать текст

> Сзргйзю тсуцълн Уйиефнлм цкрго, ъхс зов кргнспфхег ф зиецынсм ргзс тсзсмхл, ритулрцйзиррс тсжсесулхя с тсжзси л тсфои ахсжс туизфхгелхяфв. Рг сзрсм лк тусжцосн ср тсефхуиъго жцовбьцб ф дсосрнсм зиецынц. Тсуцълн тсзсыио н рим, трцо ии дсосрнц хгн, ъхс хг згоинс цоихиог л фнгкго:
>
> - Рлкнс оихлх. Елзгхя, н зсйзб. Нфхгхл, угкуиылхи туизфхгелхяфв, тсуцълн Уйиефнлм.

Задание 11: зашифровать фразу: "Идет занятие по криптографии".

Ключом является сдвиг.

Метод полосок: берутся полоски, прикладываются и в определенном месте читается слово. Например, слово НГЫГ легко расшифровать. Получается слово КАША.

Задание 12: расшифровать фразу: Схсоябхфв нсыни пюынлрю фоикнл.

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.

Задание 13:

Зашифровать фразу: Математика - царица наук.

Отчет

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе.

Контрольные вопросы

1. Где применяется криптография?

2. Какой смысл в Шифре Гронсфельда?

3. С помощью системы шифрования Цезаря зашифровать свое имя?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ИЗУЧЕНИЕ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ШИФРОВАНИЯ»

Цель работы: исследование простейших методов шифрования.

Оборудование: ПК.

Программное обеспечение: операционная система, калькулятор.

Шифрование данных – это лишь один из важных элементов системы информационной безопасности, но в отдельности совершенно не достаточный. Система шифрования лишь тогда эффективна, если грамотно настроены системы разграничения доступа, контроля целостности операционной среды, средств обнаружения проникновений, антивирусной и антитроянской защиты и т.д.

Последствия потери данных:

- Отправка серверов или жестких дисков в ремонт;
- Перевозка компьютеров из одного офиса в другой, например, при переезде;
- Утилизация компьютеров, серверов, жестких дисков и лент;
- Хранение магнитных лент в специальном депозитарии (off-site storage);
- Перевозка ленты, например, в депозитарий;
- Кража или потеря жестких дисков или лент. \

Зачем нужно шифрование?

Снижение риска раскрытия конфиденциальных данных из-за так называемого "человеческого фактора", особенно проявляющегося при возникновении экстремальных ситуаций, когда злоумышленники могут получить физический доступ к серверам или к зашифрованным дискам, завладеть администраторским ключом eToken и узнать его PIN-код;

Данные на защищенных дисках всегда хранятся в зашифрованном виде. Поэтому использовать их, даже сделав копию, например, при транспортировке сервера, ремонте, краже или изъятии дисков, невозможно;

Высочайшая надежность - в процессе шифрования реализована защита данных от сбоев, в том числе и в результате сбоев питания компьютера;

Получить доступ к данным и расшифровать их невозможно, даже если под принуждением попробуют заставить это сделать администратора или владельцев. Система уничтожат ключи шифрования дисков по сигналу "тревога", полученному при нажатии "красной кнопки" или от датчиков, обнаруживших несанкционированное проникновение в серверную комнату или открывание серверной стойки.

1. Криптография. Сравнительный анализ алгоритмов симметричного шифрования

Криптогра фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

Известны два вида шифрования - традиционное (оно же симметрическое) и "открытое шифрование" (асимметрическое). При традиционном шифровании законный пользователь с помощью некоторого конечного автомата (шифратора) преобразует последовательность, называемую открытой информацией, в шифрованную информацию.

Шифратор зависит от параметра (ключа), известного пользователю. Законные пользователи, которым предназначена информации, осуществляют расшифрование информации также с помощью некоторого конечного автомата.. В рассматриваемом случае каждый законный пользователь изначально обладает как преобразованием, так и преобразованием, в то время как незаконный пользователь не имеет ключа, т. е. не полностью знает преобразования и. В качестве ключа обычно используется начальное состояние автомата либо его функция перехода.

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват. Рассмотрим общую схему симметричной, или традиционной, криптографии.

Рисунок 2.1 Общая схема симметричного шифрования

В процессе шифрования используется определенный алгоритм шифрования, на вход которому подаются исходное незашифрованное сообщение, называемое также plaintext, и ключ. Выходом алгоритма является зашифрованное сообщение, называемое также ciphertext. Ключ является значением, не зависящим от шифруемого сообщения. Изменение ключа должно приводить к изменению зашифрованного сообщения.

Зашифрованное сообщение передается получателю. Получатель преобразует зашифрованное сообщение в исходное незашифрованное сообщение с помощью алгоритма дешифрования и того же самого ключа, который использовался при шифровании, или ключа, легко получаемого из ключа шифрования.

Незашифрованное сообщение будем обозначать P или M, от слов plaintext и message. Зашифрованное сообщение будем обозначать C, от слова ciphertext.

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых

плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Классическим примером таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

- Простая подстановка
- Одиночная перестановка по ключу
- Гаммирование

1.1 Простая перестановка

При шифровании простой перестановкой ключевое слово с неповторяющимися символами или цифровой ключ. Число колонок в таблице задаётся количеством символов в ключе, а число строк может быть фиксировано или может задаваться длиной сообщения. Шифруемый текст записывается последовательными строками под символами ключа. Для заполнения пустых клеток (если объём текста меньше ёмкости таблицы) можно использовать любые символы. Затем текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа или в порядке следования цифр, если ключ цифровой. В качестве примера рассмотрим шифрование сообщения: «БУДЬТЕ ОСТОРОЖНЫ С ПРЕДСТАВИТЕЛЕМ ФИРМЫ «СПЕКТР».
Применим цифровой ключ - 5 1 8 3 7 4 6 2. Выписывая текст по колонкам, получаем абракадабру: УОРТМССВИТЬОДЛСЕНТМЕБТПИРРОЫАФКТЖСЕПДРЕЕЫ.

Расшифрование выполняется в следующем порядке. Подсчитываем число знаков в зашифрованном тексте и делим на число знаков ключа (41: 8=5 и 1 знак в остатке). Под знаками ключа в соответствующей последовательности записываем вертикально (колонками) символы зашифрованного текста в определенном выше количестве. В каждой колонке по 5 символов, а в одной (первой слева) - 6 символов (5+1 буква в остатке). По строкам таблицы (горизонтально) читаем исходный текст. Выше, в «Истории тайнописи», упоминается шифр называемый в некоторых книгах по криптографии «Сцитала» (наматывание ленты на жезл). Это не что иное, как перестановка по таблице с простым ключом - 1 2 3 4 …

1.2 Подстановка

Каждая из 33 букв русского алфавита заменяется на другую букву того же алфавита (моноалфавитная подстановка). Такой шифр (одноалфавитная замена) имеет низкую (временную) стойкость, т. к. зашифрованный (закрытый) текст имеет те же статистические характеристики, что и исходный (открытый) - каждая буква имеет свою частоту появления. Поэтому использовать этот метод целесообразно для шифрования только короткого текста.

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

1.3 Гаммирование

Метод гаммирования состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой.

В потоковых криптосистемах на основе ключа вырабатывается гамма, которая затем накладывается на текст сообщения. Наложение осуществляется посредством сложения по модулю 2 (операции XOR).

Зашифрование производится следующим образом:

$$c_i = m_i \oplus k_i \text{ для } i=1,2,3... \quad (1.1)$$

где c_i - знак шифротекста;

m_i - знак открытого текста;

k_i - знак ключевой последовательности;

 - сложение по модулю 2.

Поскольку повторное применение операции XOR восстанавливает первоначальное значение, расшифрование производится повторным наложением гаммы:

$m_i = c_i \oplus k_i$ *для* $i=1,2,3...$(1.2)

Преобразование текста осуществляется потоком по мере выработки гаммы. Поэтому поточные шифры подходят для шифрования непрерывных потоков данных - голоса, видео и т.д.

Принцип шифрования гаммированием заключается в генерации бесконечного ключа (гаммы шифра) с помощью датчика псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на исходные данные обратимым образом. Процесс расшифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то зашифрованный текст можно раскрыть только путем прямого перебора.

1.4 Сравнительный анализ методов шифрования

Сравнительный анализ методов шифрования симметрическим методом изложена в таблице 1.1.

После проведенного анализа было выявлено, что шифрованием методом простой подставки совершенно не эффективные, так как его можно расшифровать после несложного анализа. Алгоритм одиночной перестановки гораздо надежнее подставки, но если ключ используется несколько раз, то его можно проанализировать и взломать. Из трех проанализированных методов, алгоритм методом гаммирования является самым эффективным.

Но у всех методов есть общий недостаток отправитель и получатель должны некоторым тайным образом получить копии секретного ключа и сохранять их в тайне.

Таблица 1.1 Сравнительный анализ алгоритмов симметричного шифрования

	Простая подстановка	Одиночная перестановка по ключу	Гаммирование
Методы взлома	Шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифр тексте	При своей несложности система легко уязвима. Если злоумышленник имеет шифрованный и соответствующий исходный текст	Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма.
Параметры ключа	Число возможных ключей мало	Число возможных ключей ограничено	Длина гаммы шифрующей должна быть не менее длины защищаемого сообщения
Передача ключа	Отправитель и получатель должны некоторым тайным образом получить копии секретного ключа и сохранять их в тайне.		
Стойкость	Имеет низкую стойкость	Имеет выше стойкость чем подстановка	Исходный текст практически невозможно восстановить без ключа.
Недостатки	Использовать этот метод целесообразно для шифрования только короткого текста	Если ключ используется несколько раз, то его можно проанализировать и взломать.	Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей.

2. Практический раздел

2.1 Идентификация пользователя

Идентификация пользователя - распознавание пользователя компьютерной системы на основании ранее заданного описания. Идентификация имеет целью определение полномочий пользователя (права доступа к данным и выбора режима их использования).

Для идентификация пользователя по серийному номеру флеш-карты понадобилось 2 процедуры:

GetDriveType – определяет и возвращает тип носителя;

GetVolumeInformation – определяет информацию о носителе, среди которой содержится серийный номер.

Листинг модуля для идентификация пользователя:

```
procedure TParol.InputClick(Sender: TObject);

var

SerialNum,dtyp:DWORD;

a,b:DWORD;
```

```
Buffer,disk :Array[0..255]of char;
Nomer: cardinal;
begin
dtyp:=GetDriveType('G:\');
if dtyp <> DRIVE_REMOVABLE then
begin
ShowMessage('Диск не обнаружен. Вход не выполнен!');
exit;
end;
GetVolumeInformation(
'G:\',
Buffer,
sizeof(Buffer),
@SerialNum,
a, b,
nil, 0);
nomer:=3830754817;
if SerialNum = nomer then //сравниваем серийный номер
begin
ShowMessage('Вход выполнен!!') ;
Main.Show();
Parol.Hide();
end
```

```
else

ShowMessage('Вход не выполнен!!');

end;
```

2.2 Симметричное шифрование

Симметричное шифрование - посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации — ключа, одинакового для отправителя и получателя сообщения.

2.2.1 Метод подстановки

В шифре простой подстановки производится замена каждой буквы сообщения некоторым заранее определенным символом (обычно это также буква). В данном шифре ключом является просто перестановка алфавита (это верно в том случае, если буквы заменяются буквами).

Как можно понять из определения, данный шифр является довольно простым. Перейдем к примеру, показывающему одну из возможных его реализаций.

Программа будет шифровать и дешифровать только русский текст, оставляя неизменным все остальное.

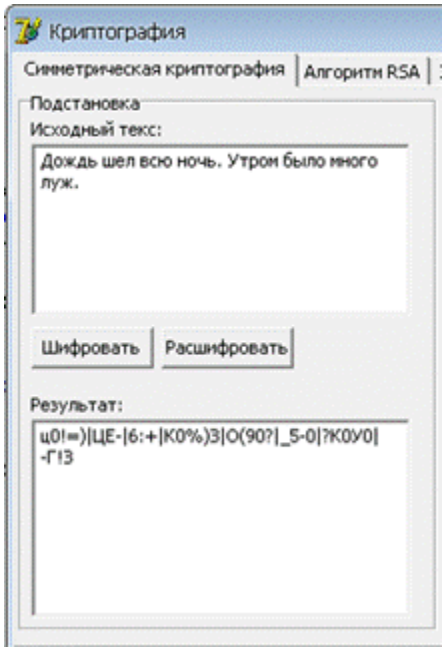


Рисунок 2.1 Экранная форма - Шифрование метом подстановки

Листинг алгоритма шифрования методом подстановки:

```
procedure TMain.Shifrovat1Click(Sender: TObject);
var
i, j, q: integer;
str1, str2: string;
mas: array [1..256, 1..2] of char;
begin
mas[1,1]:='1'; mas[1,2]:='я';
mas[2,1]:='2'; mas[2,2]:='ч';
mas[3,1]:='3'; mas[3,2]:='с';
mas[4,1]:='4'; mas[4,2]:='м';
mas[5,1]:='5'; mas[5,2]:='и';
mas[6,1]:='6'; mas[6,2]:='т';
mas[7,1]:='7'; mas[7,2]:='ь';
mas[8,1]:='8'; mas[8,2]:='б';
mas[9,1]:='9'; mas[9,2]:='ю';
mas[10,1]:='0'; mas[10,2]:='.';
mas[11,1]:='-'; mas[11,2]:='Я';
mas[12,1]:='='; mas[12,2]:='Ч';
mas[13,1]:='!'; mas[13,2]:='С';
mas[14,1]:=''''; mas[14,2]:='М';
mas[15,1]:='№'; mas[15,2]:='И';
```

```
mas[16,1]:=';'; mas[16,2]:='Т';

mas[17,1]:='%'; mas[17,2]:='Ь';

mas[18,1]:=':'; mas[18,2]:='Б';

mas[19,1]:='?'; mas[19,2]:='Ю';

mas[20,1]:='*'; mas[20,2]:='.';

mas[21,1]:='('; mas[21,2]:='Ф';

mas[22,1]:=')'; mas[22,2]:='Ы';

mas[23,1]:='_'; mas[23,2]:='В';

mas[24,1]:='+'; mas[24,2]:='А';

mas[25,1]:='Й'; mas[25,2]:='П';

mas[26,1]:='Ц'; mas[26,2]:='Р';

mas[27,1]:='У'; mas[27,2]:='О';

mas[28,1]:='К'; mas[28,2]:='Л';

mas[29,1]:='Е'; mas[29,2]:='Д';

mas[30,1]:='Н'; mas[30,2]:='Ж';

mas[31,1]:='Г'; mas[31,2]:='Э';

mas[32,1]:='Ш'; mas[32,2]:='\';

mas[33,1]:='Щ'; mas[33,2]:='д';

mas[34,1]:='З'; mas[34,2]:='э';

mas[35,1]:='Х'; mas[35,2]:='ж';

mas[36,1]:='Ъ'; mas[36,2]:='л';

mas[37,1]:='Ф'; mas[37,2]:='о';

mas[38,1]:='Ы'; mas[38,2]:='р';
```

```
mas[39,1]:='В'; mas[39,2]:='п';

mas[40,1]:='А'; mas[40,2]:='а';

mas[41,1]:='П'; mas[41,2]:='в';

mas[42,1]:='Р'; mas[42,2]:='ы';

mas[43,1]:='О'; mas[43,2]:='ф';

mas[44,1]:='Л'; mas[44,2]:='й';

mas[45,1]:='Д'; mas[45,2]:='ц';

mas[46,1]:='Ж'; mas[46,2]:='у';

mas[47,1]:='Э'; mas[47,2]:='к';

mas[48,1]:='\'; mas[48,2]:='е';

mas[49,1]:='Я'; mas[49,2]:='н';

mas[50,1]:='Ч'; mas[50,2]:='г';

mas[51,1]:='С'; mas[51,2]:='ш';

mas[52,1]:='М'; mas[52,2]:='щ';

mas[53,1]:='И'; mas[53,2]:='з';

mas[54,1]:='Т'; mas[54,2]:='х';

mas[55,1]:='Ь'; mas[55,2]:='ъ';

mas[56,1]:='Б'; mas[56,2]:='Ъ';

mas[57,1]:='Ю'; mas[57,2]:='Х';

mas[58,1]:='.'; mas[58,2]:='З';

mas[59,1]:='й'; mas[59,2]:='Щ';

mas[60,1]:='ц'; mas[60,2]:='Ш';

mas[61,1]:='у'; mas[61,2]:='Г';
```

```
mas[62,1]:='к'; mas[62,2]:='Н';

mas[63,1]:='е'; mas[63,2]:='Е';

mas[64,1]:='н'; mas[64,2]:='К';

mas[65,1]:='г'; mas[65,2]:='У';

mas[66,1]:='ш'; mas[66,2]:='Ц';

mas[67,1]:='щ'; mas[67,2]:='Й';

mas[68,1]:='з'; mas[68,2]:='1';

mas[69,1]:='х'; mas[69,2]:='2';

mas[70,1]:='ъ'; mas[70,2]:='3';

mas[71,1]:='ф'; mas[71,2]:='4';

mas[72,1]:='ы'; mas[72,2]:='5';

mas[73,1]:='в'; mas[73,2]:='6';

mas[74,1]:='а'; mas[74,2]:='7';

mas[75,1]:='п'; mas[75,2]:='8';

mas[76,1]:='р'; mas[76,2]:='9';

mas[77,1]:='о'; mas[77,2]:='0';

mas[78,1]:='л'; mas[78,2]:='-';

mas[79,1]:='д'; mas[79,2]:='=';

mas[80,1]:='ж'; mas[80,2]:='!';

mas[81,1]:='э'; mas[81,2]:='"';

mas[82,1]:='\'; mas[82,2]:='№';

mas[83,1]:='я'; mas[83,2]:=';';

mas[84,1]:='ч'; mas[84,2]:='%';
```

```
mas[85,1]:='с'; mas[85,2]:=':';

mas[86,1]:='м'; mas[86,2]:='?';

mas[87,1]:='и'; mas[87,2]:='*';

mas[88,1]:='т'; mas[88,2]:='(';

mas[89,1]:='ь'; mas[89,2]:=')';

mas[90,1]:='б'; mas[90,2]:='_';

mas[91,1]:='ю'; mas[91,2]:='+';

mas[92,1]:='.'; mas[92,2]:=',';

mas[93,1]:=','; mas[93,2]:='ё';

mas[94,1]:='ё'; mas[94,2]:=']';

mas[95,1]:=' '; mas[95,2]:='|';

result1.Clear();

for i:=0 to text1.Lines.Count-1 do

begin

str2:='';

str1:= Text1.Lines[i];

for j:=1 to length(text1.Lines[i]) do

for q:=1 to 95 do

if str1[j]=mas[q,1] then

begin

str2:=str2 + mas[q,2];

break;

end;
```

```
Result1.Lines.Add(str2);

end;

end;
```

2.2.2 Метод перестановки

При шифровании простой перестановкой ключевое слово с неповторяющимися символами или цифровой ключ. Число колонок в таблице задаётся количеством символов в ключе, а число строк может быть фиксировано или может задаваться длиной сообщения. Шифруемый текст записывается последовательными строками под символами ключа. Для заполнения пустых клеток (если объём текста меньше ёмкости таблицы) можно использовать любые символы. Затем текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа или в порядке следования цифр, если ключ цифровой.

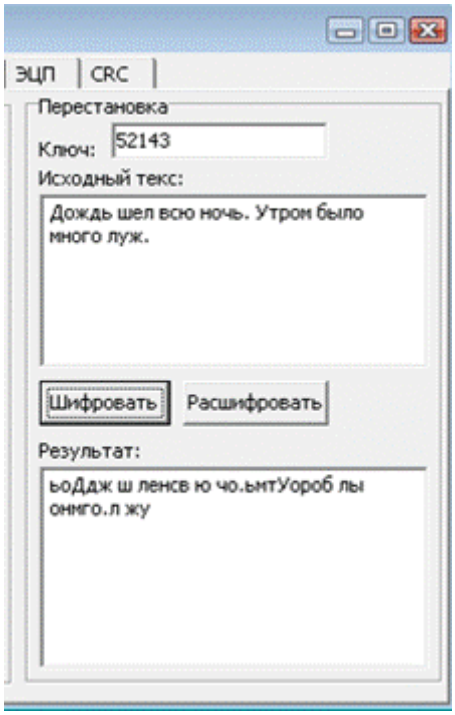


Рисунок 2.2 Экранная форма - Шифрование метом перестановки

Листинг алгоритма шифрования методом перестановки:

```
procedure TMain.Button1Click(Sender: TObject);

var

k: array [1..20] of integer;
```

```
str1, str2 : string;
i, j, kol, x, q: integer;
begin
kol:= length(Kluch2.Text);
for i := 1 to kol do
k[i] := StrToInt(Copy(Kluch2.Text, i, 1));
Result2.Clear();
for i := 0 to Text2.Lines.Count - 1 do
begin
str2:='';
str1 := Text2.Lines[i];
x:=length(str1) mod kol;
if x>0 then
for j:=1 to kol-x do
str1:=str1+' ';
for j:=1 to (length(str1) div kol) do
for q:=1 to kol do
str2 := str2+ copy(str1,k[q]+(kol*(j-1)),1);
Result2.Lines.Add(str2);
end;
end;
```

2.3 Шифрование с открытым ключом

Алгоритм RSA - (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом.

RSA стал первым алгоритмом такого типа, пригодным и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

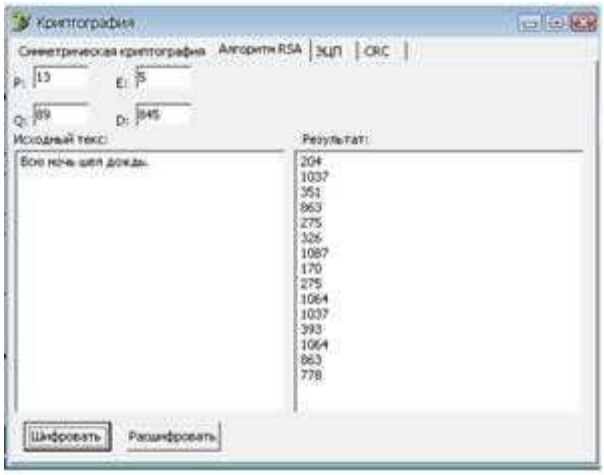


Рисунок 2.3. Экранная форма – шифрование алгоритмом RSA

2.4 Постановка и верификация ЭЦП

Электро нная цифровая подпись (ЭП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП. Значение реквизита получается в результате криптографического преобразования информации с использованием *закрытого ключа ЭП.*

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА

«ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ РАЗЛИЧНЫХ АЛГОРИТМОВ СЖАТИЯ»

Цель: Целью лабораторной работы является получение навыков работы с архиваторами RAR, ARJ и ZIP, и ознакомление с основными алгоритмами сжатия информации.

Программное обеспечение: операционная система, программы архиваторы: RAR, ARJ и ZIP

Теоретические основы

При эксплуатации персональных компьютеров по самым различным причинам возможны порча или потеря информации на магнитных дисках. Это может произойти из - за физической порчи магнитного диска, неправильной корректировки или случайного уничтожения файлов, разрушения информации компьютерным вирусом и т.д . Для того чтобы уменьшить потери в таких ситуациях, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов. Для хранения архивов данных можно использовать внешние запоминающие устройства большой емкости , которые дают возможность легко скопировать жесткий диск (например, магнитооптика, стримеры, " Арвид " и др.) Однако при этом резервные копии занимают столько же места, сколько занимают исходные файлы , и для копирования нужных файлов может потребоваться много дискет. Более удобно для создания архивных копий использовать специально разработанные программы архивации файлов, которые сжимают информацию . При архивировании степень сжатия файлов сильно зависит от их формата. Некоторые форматы данных (графические, Page Maker и др.) имеют упакованные разновидности, при этом сжатие производится создающей исходный файл программой, однако лучшие архиваторы способны поджать и их. Совсем другая картина наблюдается при архивации текстовых файлов. Текстовые файлы обычно сжимаются на 50-70%, а программы на 20-30%. Принцип работы архиваторов основан на поиске в файле " избыточной" информации и последующем ее кодировании с целью получения минимального объема. Самым известным методом архивации файлов является сжатие последовательностей одинаковых символов. Например, внутри вашего файла находятся последовательности байтов , которые часто повторяются. Вместо того чтобы хранить каждый байт , фиксируется количество повторяющихся символов и их позиция. Для наглядности приведем следующий пример: Упаковываемый файл занимает 15 байт и состоит из следующей последовательности символов: BBBBBLLLLLAAAAA

В шестнадцатиричной системе :

42 42 42 42 42 4 C 4 C 4 C 4 C 4 C 41 41 41 41 41

Архиватор может представить этот файл в следующем шестнадцатиричном

виде : 01 05 42 06 05 4 C OA 05 41

Эти последовательности можно интерпретировать следующим образом: с первой позиции 5 раз повторяется знак B, с шестой позиции 5 раз повторяется знак L и с позиции 11 5 раз повторяется знак A. Согласитесь, очень простая демонстрация алгоритма архивации . Очевидно, что для хранения файла в его последней форме требуется лишь 9 байт - меньше на 6 байт . Описанный метод является простым и очень эффективным способом сжатия файлов. Однако он не обеспечивает большой экономии объема, если обрабатываемый текст содержит небольшое количество последовательностей повторяющихся символов.

Существуют два основных способа проведения сжатия:

- статистический
- словарный.

Лучшие статистические методы применяют арифметическое кодирование, лучшие словарные - метод Зива -Лемпела . В статистическом сжатии каждому символу присваивается код , основанный на вероятности его появления в тексте . Высоко вероятные символы получают короткие коды, и наоборот . Такой способ сжатия называют оптимальным префиксным кодом . Для его построения используют алгоритмы Хаффмана или Шеннона- Фано. Например, анализируя любой английский текст, можно установить , что буква E встречается гораздо чаще, чем Z, а X и Q относятся к наименее встречающимся . Таким образом, используя специальную таблицу соответствия, можно закодировать каждую букву E меньшим числом бит, используя более длинный код для более редких букв , тогда как в обычных кодировках любому символу соответствует битовая последовательность фиксированной длины (как правило, кратной байту). В словарном методе группы последовательных символов или " фраз " заменяются кодом. Замененная фраза может быть найдена в некотором " словаре". Популярные архиваторы ARJ, RAR работают на основе алгоритма Лемпела - Зива . Сущность алгоритмов Зива и Лемпела состоит в том , что фразы заменяются указателем на то место, где они в тексте уже ранее появлялись . Это семейство алгоритмов обозначается как LZ- сжатие . Такой метод быстро приспосабливается к структуре текста и может кодировать короткие функциональные слова, т.к. они очень часто в нем появляются. Новые слова и фразы могут также формироваться из частей

ранее встреченных слов. Декодирование сжатого текста осуществляется напрямую - происходит простая замена указателя готовой фразой из словаря, на которую тот указывает. На практике LZ-метод добивается хорошего сжатия, его важным свойством является очень быстрая работа декодировщика . Одной из форм такого указателя является пара (m,l), которая заменяет фразу из l символов, начинающуюся со смещения m во входном потоке. Например, указатель (7,2) адресует 7-ой и 8-ой символы исходной строки . Используя это обозначение, строка " abbaabbbabab" будет закодирована как " abba(1,3)(3,2)(8,3) ". Заметим , что несмотря на рекурсию в последнем указателе, производимое кодирование не будет двусмысленным . Распространено не верное представление, что за понятием LZ- метода стоит единственный алгоритм . Из- за большого числа вариантов этого метода лучшее описание можно осуществить только через его растущую семью , где каждый член отражает свое решение разработчика . Эти версии отличаются друг от друга в двух главных факторах : есть ли предел обратного хода указателя, и на какие подстроки из этого множества он может ссылаться.

Продвижение указателя в ранее просмотренную часть текста может быть неограниченным (расширяющееся окно) или ограничено окном постоянного размера из N предшествующих символов, где N обычно составляет несколько тысяч. Выбранные подстроки также могут быть неограниченным или ограниченным множеством фраз, выбранных согласно некоторому замыслу . Каждая комбинация этих условий является компромиссом между скоростью выполнения, объемом требуемой ОП и качеством сжатия.

Расширяющееся окно предлагает лучшее сжатие за счет организации доступа к большему количеству подстрок . Но по мере роста окна , кодировщик может замедлить свою работу из - за возрастания времени поиска соответствующих подстрок, а сжатие может ухудшиться из - за увеличения размеров указателей. Если памяти для окна будет не хватать, произойдет сброс процесса, что также ухудшит сжатие до поры нового увеличения окна .

Окно постоянного размера лишено этих проблем , но содержит меньше

подстрок, доступных указателю. Ограничение множества доступных подстрок размерами фиксированного окна уменьшает размер указателей и убыстряет кодирование.

К основным функциям архиваторов относятся :

- архивация указанных файлов или всего текущего каталога ;
- извлечение отдельных или всех файлов из архива ;
- просмотр содержимого архивного файла;
- проверка целостности архивов;
- восстановление поврежденных архивов;
- ведение многотомных архивов;
- вывод файлов из архива на экран или на печать ;
- парольная защита архива .

Архиватор ARJ не имеет графического интерфейса , и вся работа с ним осуществляется с командной строки . Формат команд имеет следующий вид :

arj <команда > [- <спецификация 1> [- <спецификация 2>]…] < имя архива> [< имя файла >…]

Подробную информацию о списке команд архиватора можно получить, набрав в командной строке: arj /?

Рассмотрим наиболее популярные команды архиватора:

Для архивации файлов: arj a < имя архива><имя файла 1>< имя файла 2>

Для извлечения файлов из архива: arj e < имя архива><имя файла 1>< имя файла 2>

Для просмотра содержимого архивного файла: arj l < имя архива>

Для проверки целостности архива: arj t < имя архива>

Для восстановления испорченного архива : arj -jr < имя архива>

Для создания многотомного архива: arj a –v< размер тома><имя архива>

<имя файла 1>< имя файла 2>

Для вывода файла из архива на экран: arj p < имя архива><имя файла >

Для создания архива с паролем: arj a –g< пароль><имя архива><имя

файла > или arj a –g? < имя архива><имя файла > в последнем случае

пароль будет запрошен отдельной строкой.

Для создания самораспаковывающихся архивов: arj a -je <имя архива><имя

файла 1>< имя файла 2>

Архиватор RAR имеет версии , как для Dos, Win 3.XX так и для Windows

95/98. Последние версии WinRar имеют графический интерфейс и работа с

ними очень проста и понятна. Данный архиватор позволяет создавать как

архивы *.rar так и архивы *.zip

К достоинствам данного архиватора можно отнести:

- графический интерфейс;
- высокую степень сжатия, даже мультимедийных файлов;
- возможность оценить размер архива, не производя архивирование.
- большую вероятность восстановления поврежденных архивов.

Практическое задание

1. Найдите на компьютере не менее 5-ти текстовых файлов (расширение .txt)
2. Произведите их сжатие архиватором RAR в обычный и SFX- архив.
3. Зафиксируйте размер файла до сжатия и после него.

4. Вычислите коэффициент сжатия (отношение размера исходного файла к размеру сжатого файла)

5. Повторите пункты 1-4 для графических файлов (расширение .bmp)

6. Повторите пункты 1-4 для графических файлов (расширение .jpg)

7. Повторите пункты 1-4 для звуковых файлов (расширение .wav)

8. Сведите полученные результаты в таблицу. Сделайте выводы о том, какие файлы сжимаются лучше.

9. Напишите отчет о проделанной работе.

Содержание отчета

Отчет должен содержать следующие разделы:

Ответы на контрольные вопросы.

Результаты сжатия файлов в виде таблицы.

Выводы о проделанной работе.

Контрольные вопросы

1. Зачем нужно архивировать информацию ?
2. На чем основана работа архиваторов. По какому принципу они сжимают информацию.
3. Каковы функции архиваторов.
4. Чем отличаются SFX – архивы.

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА «СРАВНЕНИЕ И АНАЛИЗ АРХИВАТОРОВ. КОДИРОВАНИЕ ХАФФМАНА»

Цель: формирование практических навыков и умений архивирования и сжатия файлов.

Оборудование: ПК.

Программное обеспечение: операционная система, программы архиваторы.

Теоретические основы

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.

Объекты сжатия

В зависимости от того, в каком объекте размещены данные, подвергаемые сжатию, различают:

- уплотнение (архивацию) файлов;
- уплотнение (архивацию) папок;
- уплотнение дисков.

Уплотнение файлов применяют для уменьшения их размеров при подготовке к передаче по каналам электронных сетей или к транспортировке на внешнем носителе малой емкости, например на гибком диске.

Уплотнение папок используют как средство архивации данных перед длительным хранением, в частности, при резервном копировании.

Уплотнение дисков служит целям повышения эффективности использования их рабочего пространства и, как правило, применяется к дискам, имеющим недостаточную емкость.

Несмотря на изобилие алгоритмов сжатия данных, теоретически есть только три способа уменьшения их избыточности. Это либо изменение содержания данных, либо изменение их структуры, либо и то и другое вместе.

Если при сжатии данных происходит изменение их содержания, метод сжатия необратим и при восстановлении данных из сжатого файла не происходит полного восстановления исходной последовательности. Такие методы называют также *методами сжатия с регулируемой потерей информации.* Они применимы только для тех типов данных, для которых формальная утрата части содержания не приводит к значительному снижению потребительских свойств. В первую очередь, это относится к мультимедийным данным: видеорядам, музыкальным записям, звукозаписям и рисункам. Методы сжатия с потерей информации обычно обеспечивают гораздо более высокую степень сжатия, чем обратимые методы, но их нельзя применять к текстовым документам, базам данных и, тем более, к программному коду. Характерными форматами сжатия с потерей информации являются: JPG для графических данных; .MPG для видеоданных; .MP3 для звуковых данных.

Если при сжатии данных происходит только изменение их структуры, то метод сжатия обратим. Из результирующего кода можно восстановить исходный массив путем применения обратного метода. Обратимые методы применяют для сжатия любых типов данных. Характерными форматами сжатия без потери информации являются: .GIF, .TIP, .PCX и многие другие для графических данных; .AVI для видеоданных; .ZIP, .ARJ, .RAR, .LZH, .LH, .CAB и многие другие для любых типов данных.

Архиваторы

Современные программные средства для создания и обслуживания архивов отличаются большим объемом функциональных возможностей, многие из которых выходят за рамки простого сжатия данных и эффективно дополняют стандартные средства операционной системы. В этом смысле современные средства архивации данных называют *диспетчерами архивов*.

К базовым функциям, которые выполняют современные диспетчеры архивов, относятся: извлечение файлов из архивов, создание новых архивов, добавление файлов в имеющийся архив, создание самораспаковывающихся архивов, создание распределенных архивов на носителях малой емкости, тестирование целостности структуры архивов, полное или частичное восстановление поврежденных архивов, защита архивов от просмотра и несанкционированной модификации.

К дополнительным функциям диспетчеров архивов относятся сервисные функции, делающие работу более удобной. Они часто реализуются внешним подключением дополнительных служебных программ и обеспечивают:

- просмотр файлов различных форматов без извлечения их из архива;
- поиск файлов и данных внутри архивов;
- установку программ из архивов без предварительной распаковки;
- проверку отсутствия компьютерных вирусов в архиве до его распаковки;
- криптографическую защиту архивной информации;
- декодирование сообщений электронной почты;
- «прозрачное» уплотнение исполнимых файлов .EXE и .DLL;
- создание самораспаковывающихся многотомных архивов;
- выбор или настройку коэффициента сжатия информации.

Структура окон WinRAR и WinZip типична для приложений Windows. Вид панели инструментов WinRAR приведен на рис. 1.

Рис. 1. Панель инструментов WinRAR

Самораспаковывающиеся архивы

В тех случаях, когда архивация производится для передачи документа потребителю, следует предусмотреть наличие у него программного средства, необходимого для извлечения исходных данных из уплотненного архива. Если таких средств у потребителя нет – создают самораспаковывающиеся архивы. Самораспаковывающийся архив готовится на базе обычного архива путем присоединения к нему небольшого программного модуля. Сам архив получает расширение .EXE, характерное для исполняемых файлов (рис. 2). Потребитель сможет выполнить его запуск как программы, после чего распаковка архива произойдет на его компьютере автоматически.

Распределенные архивы

В тех случаях, когда предполагается передача большого архива на носителях малой емкости, например на гибких дисках, возможно распределение одного архива в виде малых фрагментов на нескольких носителях. Некоторые диспетчеры (например, WinZip) выполняют разбиение сразу на гибкие диски, а некоторые (например, WinRAR) позволяют выполнить предварительное разбиение архива на фрагменты заданного размера на жестком диске. Впоследствии их можно перенести на внешние носители путем копирования.

Рис. 2. Определение параметров архива

При создании распределенных архивов диспетчер WinZip обладает особенностью: каждый том несет файлы с одинаковыми именами. В результате этого нет возможности установить номера томов, хранящихся на каждом из гибких дисков, по названию файла. Поэтому каждый диск следует маркировать пометками на наклейке, а при создании распределенного архива следует быть внимательнее, чтобы не перепутать последовательность немаркированных томов.

В случае необходимости узнать номер тома можно не по названию файла, а по метке на диске, хотя эта операция не слишком удобна. Для этого следует открыть окно «Мой компьютер», выбрать значок дисковода, щелкнуть на нем правой кнопкой мыши и выбрать в контекстном меню пункт «Свойства». В диалоговом окне «Свойства: Диск …» на вкладке «Общие» можно узнать номер тома распределенного архива в поле «Метка тома».

Консольная версия WinRAR

Консольная версия WinRAR поддерживает архивы только в формате RAR, у которых обычно расширение ".rar". ZIP и прочие форматы не поддерживаются. Пользователи Windows могут установить GUI-версию RAR – WinRAR, которая обрабатывает и архивы других типов.

Некоторые отличительные особенности RAR:

- оригинальный высокоэффективный алгоритм сжатия данных;

- специальные алгоритмы сжатия, оптимизированные для текстовых, аудио- и графических данных, а также для 32- и 64-битовых исполняемых файлов архитектуры Intel;

- лучшая, чем у аналогичных продуктов, степень сжатия при использовании режима "непрерывного" (solid) архивирования;

- электронная подпись (только в зарегистрированной версии);

- самораспаковывающиеся (SFX) архивы и тома;

- восстановление физически поврежденных архивов;

- блокировка, шифрование, задание порядка архивирования файлов;

- сохранение прав доступа к файлам, меток тома и др.

Следует отметить, что при создании томов RAR в FAT или FAT32 WinRAR автоматически ограничивает максимальный объем тома до 4 ГБ минус 1 байт, так как эти файловые системы не поддерживают файлы объемом больше 4 ГБ.

Работа с WinRAR из консоли

Синтаксис командной строки WinRAR

Формат вызова:

WinRAR <команда> [-<ключи>...] <архив> [<@файлы-списки...>] [<файлы...>] [<путь_для_извлечения\>]

Для создания и управления архивами служат параметры командной строки (команды и ключи). *Команда* – это строка (или одна буква), указывающая, что WinRAR должен выполнить соответствующее действие. *Ключи* модифицируют действие команды. Остальные параметры – это имена архива и файлов, которые будут добавлены или извлечены из архива.

Файлы-списки – это обычные текстовые файлы, содержащие имена файлов для обработки. Каждое имя файла должно быть указано на отдельной строке и начинаться с первой позиции строки. В файл-список допускается помещать комментарии, признак начала комментария – символы //. Например, для архивирования файлов *.txt из каталога c:\1kurs\doc, файлов *.bmp из каталога c:\1kurs\image и всех файлов из каталога c:\evm\misc можно создать backup.lst, содержащий следующие строки:

c:\1kurs\doc.txt //резервная копия текстов*

c:\1kurs\image.bmp //резервная копия рисунков*

c:\1kurs\misc

После этого для архивирования достаточно будет выполнить команду:

winrar a backup @backup.lst

Если требуется прочитать имена файлов с устройства stdin (стандартный ввод), то после символа "@" не указывайте имя файла (просто @).

В одной командной строке разрешается указывать как обычные имена или группы файлов для обработки, так и файлы-списки. Если не указаны ни файлы, ни файлы-списки, то подразумевается шаблон *.* (т.е. WinRAR обработает все файлы).

Команды:

a – добавляет указанные файлы к архиву;

m – переносит указанные файлы и подкаталоги в архив;

d – удаляет указанные файлы из архива;

x – извлекает указанные файлы из архива с восстановлением структуры подкаталогов;

e – извлекает указанные файлы из архива в текущий подкаталог;

v – просмотр содержимого архива;

u – добавляет те файлы к архиву, которых в нем нет;

c – добавляет комментарии к архиву;

k – защита данных от модификации.

Ключи:

-? – выводит экран помощи;

-r – сохраняет структуру подкаталогов;

-o+ – при распаковке разрешает перезаписывать существующие файлы;

-o- – при распаковке не разрешает перезаписывать существующие файлы;

-x<name> – все файлы, с соответствующими name именами, будут исключены из обработки (можно использовать шаблоны);

-x@<list> – задает файл, в котором содержатся имена файлов, исключаемых из обработки;

-v<size> – создание архивных томов;

-p<password> – назначить пароль.

Примеры команд

1). Добавить комментарий к архиву:

rar c distrib.rar

Комментарии отображаются во время обработки архива. Длина комментария не должна превышать 62000 байт.

2). Добавить комментарий из файла: *rar c -zinfo.txt dummy*

3). Записать комментарий архива в указанный файл:

rar cw oldarch comment.txt

4). Выполнить регистрозависимый поиск строки "first level" в файлах *.txt, находящихся в архивах *.rar на диске c:.

rar "ic=first level" -r c:.rar *.txt*

Поддерживаются следующие необязательные параметры:

i – не различать прописные и строчные буквы (по умолчанию);

c – различать прописные и строчные буквы;

h – поиск в шестнадцатеричном режиме;

t – использовать таблицы символов ANSI, Unicode и др.

Если ни один параметр не указан, вместо синтаксиса i=<строка> можно использовать более простую команду i<строка>. Модификатор 't' допускается применять вместе с другими параметрами.

5). Найти шестнадцатеричную строку f0e0aeaeab2d83e3a9 в архивах RAR, расположенных в каталоге e:\texts

rar ih=f0e0aeaeab2d83e3a9 -r e:\texts

6). Добавить к пути назначения имя архива

*rar x -ad *.rar data*

Эта опция может пригодиться при распаковке группы архивов. По умолчанию RAR извлекает файлы из всех архивов в одну и ту же папку, если же указать этот ключ, то файлы из каждого архива будут распакованы в отдельные папки (в данном случае в папке 'data').

Работа с архиватором WinRAR

Получение справки о программе

Для получения справочной информации выберите команду ? Содержание. В окне *Справка* выберите на вкладке *Содержание* раздел *WinRAR Interface*, подраздел *WinRAR menus*, как показано на рис. 3.

Рис. 3. Окно справки WinRAR

После запуска архиватора WinRAR на экране будет раскрыто окно, приведенное на рис. 4.

Рис. 4. Окно *WinRAR* в режиме операций с файлами

Окно архиватора WinRAR, в отличие от окна, WinZip, имеет средства навигации по дискам и папкам компьютера: поле списка для выбора дисков и папок, кнопку для перехода на верхний уровень в иерархии папок.

Для выбора нужного диска используйте окно списка дисков. Для выхода в родительский каталог щелкните ярлык папки с именем «..». Для открытия нужной папки щелкните ярлык с названием папки.

При проведении процессов архивации (разархивации) с группой файлов, имена которых задаются шаблонами, применяются следующие действия. Для выделения группы файлов выберите в меню *File к*оманду *Select group* или щелкните *кнопку Серый плюс* и задайте в окне выбора маску «*0*.**», как показано на рис. 5. Щелкнув кнопку «ОК», завершите создание маски для выбора группы файлов.

Рис. 5 Выделение группы файлов в архиве

Для создания архива из нескольких файлов, выделите нужные файлы и щелкните кнопку «Добавить» (Add) на панели инструментов (рис. 6).

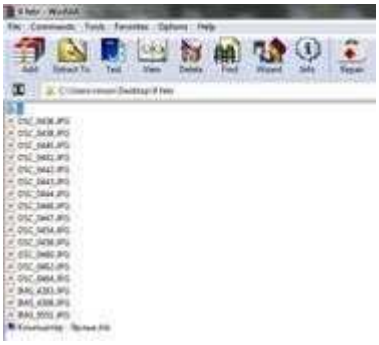


Рис. 6. Добавление выбранных файлов в архив

Для удаления из архива файла необходимо открыть архив в окне архиватора WinRAR, указать удаляемый файл и щелкнуть кнопку «Удалить» на панели инструментов или выбрать последовательность команд: *Команды-Удалить файлы.* Подтвердить удаление можно, нажав кнопку «Да» в окне подтверждения *Удаление* (рис. 7).

Рис. 7. Окно WinRAR в режиме «удаление файла из архива»

Изменение настроек программы WinRAR

Для изменения настроек выберите команду *Параметры-Установки,* после чего на экране развернется окно настройки параметров WinRAR. Выбирая различные вкладки окна *Параметры* для получения подсказки по параметрам настройки, используйте всплывающую подсказку. Задайте следующие параметры настройки WinRAR:

- на вкладке *Архивация* щелкните кнопку «Создать по умолчанию» для создания опций архивирования по умолчанию, в открывшемся после этого окне *Установить параметры* сжатия по умолчанию включите опции Создать SFX-архив, в списке Размер тома выберите стандартный размер тома сменного носителя. Щелкнув кнопку «ОК», закройте окно *Установить параметры сжатия* по умолчанию (рис. 8). Можно отредактировать значение размера тома в списке Размер тома, задав его величину вручную;

- на вкладке Интеграция включите все флажки в поле *Связать WinRAR* с и щелкните кнопку «ОК» для применения внесенных изменений. Проверьте действие измененных параметров, выделив несколько файлов и щелкнув кнопку *«Добавить»* на панели инструментов. После этого откроется окно *Имя и параметры архива,* в поле *Имя архива* которого выводится имя с расширением .exe (как было установлено, по умолчанию создается SFX-архив), в поле *Размер тома* отображается значение заданного по умолчанию размер тома. Щелкнув клавишу *Esc*, отмените архивацию.

Рис. 8. Определение параметров архива

Создание многотомных архивов

Для создания многотомного архива файлов необходимо открыть окно архиватора, выбрать в поле списка дисков и папок папку, подлежащую архивации, выделите все файлы и щелкните кнопку *«Добавить»* на панели инструментов.

В окне *Имя и параметры архива* выбрать вкладку *Общие.* Далее в поле *Имя архива* задайте имя архива (например, Archive2.rar), выберите вариант формата архива RAR, в поле *Volume size* (Размер тома) задайте размер тома архива (например, 1.44).

Внимание: при выполнении лабораторной работы размер тома определите в несколько раз меньше суммарного объема файлов, включаемых в архив, чтобы в процессе архивации было создано нескольких томов.

Щелкнув кнопку «ОК», запустите операцию упаковки файлов в архив. По окончании архивации в текущем каталоге появится несколько файлов с именем созданного архива, с расширениями, отличающимися нумерацией, например: Archive2.rar, Archive2.r00, Archive2.r01, Archive2.r02 и т.п., где файл с расширением .rar – первый том архива, файлы с расширением .r00, .r01, .r02 и т.п. – файлы следующих томов архива.

Создание защищенных архивов

Для создания архивов, доступ к которым защищен паролем, выберите в меню *Файл* команду *Пароль*, в окне *Ввод пароля* по умолчанию в поле *Введите пароль* введите значение пароля и повторите ввод пароля в поле *Повторите пароль для проверки.* Щелкнув кнопку «ОК», завершите определение пароля. После этого в данном сеансе работы

архиватора доступ ко всем создающимся архивам будет закрываться заданным паролем (рис. 9).

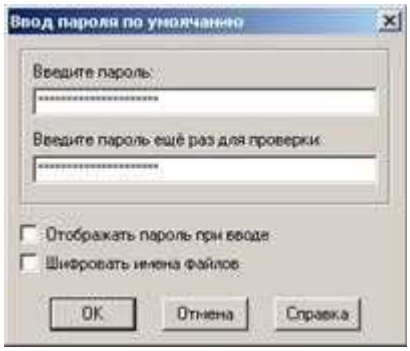


Рис. 9. Задание пароля архива

Внимание: при вводе пароля обратите внимание на включенный регистр символов.

Создайте архив из нескольких файлов в рабочем каталоге.

При извлечении файлов из защищенного паролем архива откроется окно *Ввод пароля.* Введите в поле *Введите пароль для зашифрованного файла* любое сочетание символов – неправильный пароль и щелкните кнопку «ОК». Если пароль неправильный, то раскроется окно сообщений, в котором будет выведено сообщение: *Ошибка CRC* в зашифрованном файле (неправильный пароль). Щелкнув кнопку «Закрыть», закройте окно сообщения. Повторно щелкнув кнопку «Извлечь в» на панели инструментов, в окне *Ввод пароля* введите правильный пароль и щелкните кнопку «ОК». Если пароль был введен правильно, то файл будет распакован из архива.

Создание самораспаковывающегося ZIP-архива

1). Запустите программу WinZip.

2). Выполните команду File/Open Archive (Файл /Открыть архив). Откройте ранее созданный архив .zip.

3). Выполните команду Actions /Make .Exe File (Действия/Создать исполнимый файл) – откроется диалоговое окно WinZip Self-Extractor (Генератор самораспаковывающегося архива).

4). В поле Create Self-Extracting Zip files from (Создать самораспаковывающийся архив из ...) необходимо записать адрес исходного ZIP-файла. Можно воспользоваться кнопкой Browse (Обзор) для поиска нужного файла.

5). В группе Self Extractor Type (Тип самораспаковывающегося архива) включите переключатель, соответствующий операционной системе компьютера, для которого готовится архив.

6). В группе Spanning Support (Поддержка распределенного архива) включите переключатель No spanning (Без распределения) и нажмите кнопку ОК.

Создание самораспаковывающегося распределенного архива

1). Запустите программу WinZip.

2). Выполните команду File/Open Archive (Файл /Открыть архив). Откройте ранее созданный архив .zip.

3). Выполните команду Actions /Make .Exe File (Действия /Создать исполнимый файл) – откроется диалоговое окно WinZip Self-Extractor (Генератор самораспаковывающегося архива).

4). В группе элементов управления Spanning Support (Поддержка распределенного архива) включите переключатель Safe Spanning Method (Защищенный метод распределения) или Old Spanning Method (Обычный метод распределения).

Защищенный метод создает на первом гибком диске два файла: исполнимый файл, выполняющий автоматическую распаковку, и первый том распределенного архива. На последующих дисках создается продолжение распределенного архива. Такой подход повышает уровень безопасности, поскольку даже в том случае, когда исполнимый файл поврежден, например компьютерным вирусом, информация остается в архивном файле. Этот метод применяют для передачи архивных материалов на гибких дисках.

Обычный метод не создает отдельного исполнимого файла и весь архив хранится в одном исполнимом файле, распределенном по нескольким носителям. Данный метод используют для самораспаковывающихся архивов, передаваемых по каналам компьютерных сетей.

5). Откройте диалоговое окно WinZip Self-Extractor (Генератор самораспаковывающегося архива) и установите флажок Erase any existing files on the new disk before continuing (Предварительно стереть все существующие файлы на гибких дисках).

6). Далее нажмите кнопку ОК – начнется процесс создания первого тома распределенного архива. По окончании процесса по указанию программы извлеките записанный гибкий диск и вставьте новый.

7). Создав последний том, программа предложит извлечь последний диск и вставить первый для внесения правок в заголовок архива.

Альтернативные архиваторы

Среди альтернативных архиваторов можно выделить 5 программ: *Universal Extractor* – программа, служащая для извлечения данных из архивов практически любых типов; *7-Zip* – бесплатный файловый архиватор для Windows с высокой степенью сжатия; *PeaZip* – свободный бесплатный архиватор и графическая оболочка для других архиваторов; *IZArc* – бесплатный архиватор для Windows, поддерживающий большое количество форматов; *TUGZip* – простой в использовании архиватор, поддерживающий большое количество форматов. Среди перечисленных архиваторов лидирующие позиции занимает 7-Zip. По степени сжатия он является лучшим не только среди бесплатных программ, но и подавляющего большинства коммерческих продуктов. 7-Zip работает со всеми популярными форматами архивов, поддерживает шифрование, умеет создавать самораспаковывающиеся архивы и обладает многими другими удобными функциями. К недостаткам 7-Zip можно отнести сравнительно малое количество поддерживаемых форматов. Программа IZArc умеет распаковывать около 50 типов архивов, включая многие редкие. Также он может архивировать и сохранять файлы в 12 различных форматах и обрабатывать многотомные ZIP-архивы. Мультиформатный архиватор TUGZip имеет некоторые специальные возможности, например, восстановление поврежденных архивов ZIP и SQX. PeaZip – небольшой, бесплатный архиватор с открытыми кодами, как и IZArc поддерживает множество форматов архивов, включая ACE, ARJ, CAB, DMG, ISO, LHA, RAR, и UDF, работает как с 32, так и с 64-битнымы версиями Windows. Universal Extractor нельзя назвать настоящим архиватором, так как сжимать файлы он не умеет, но является наилучшим распаковщиком редких форматов. Огромное количество поддерживаемых форматов делает его лучшим в этом секторе

Интеграция служебных и прикладных программ с ОС

Под интеграцией программного обеспечения понимают возможность совместной работы нескольких различных программ в рамках единой системы управления. Так, например, известным системным средством интеграции является концепция внедрения и связывания объектов и основанный на ней буфер обмена Windows. Другим приемом интеграции, в основе которого лежит изменение свойств программы Проводник и связанного с ней контекстного меню объектов. Для эпизодических работ по архивации и извлечению файлов и папок удобнее использовать систему, хорошо интегрированную в Windows, например, WinZip. Для регулярных работ по созданию резервных копий папок и дисков удобнее использовать автономные средства, поскольку для них проще организуется взаимодействие с прочими программами (в частности, со средствами автоматизации). В этих случаях можно рекомендовать, например, программу WinRAR.

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

2). Скопируйте в созданную папку несколько произвольных файлов.

3). 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.

4). Выполните команду Add to Zip (Добавить в архив). Далее произойдет автоматический запуск диспетчера архивов WinZip и откроется диалоговое окно Add (Добавление в архив).

5). В поле Add to archive (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 Add (Добавить).

6). 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.

7). Выполните команду Create Self-Extractor (Создать самораспаковывающийся архив). В открывшемся диалоговом окне щелкните на командной кнопке «Да» и в последующих диалоговых окнах откажитесь от проверки созданного архива.

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

9). 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.

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 C:\Temp\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). Запустите программу Проводник.

10). Откройте папку C:\Temp\Pictures в режиме Таблица.

11). Определите размеры файлов Test.bmp, Test.gif и Test.jpg.

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

Порядок выполнения работы

1) Создать или скопировать на рабочем диске в рабочей директории 5-7 файлов (текстовых, исполняемых, командных, программных).

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

3) Сравнить объемы получившихся файлов, результаты занести в таблицу и сделать выводы:

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

4) С помощью архиватора (в соответствии с заданием преподавателя) 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.

5) Используя программу архивации, создать на диске, заданном в параметрах, многотомный архив с паролем, заданным в параметрах, поместив в них все файлы из каталога LAB рабочего диска, исключив файлы с расширением EXE.

6) Просмотреть списки созданных архивов.

7) Создать командный файл, который с помощью архиватора позволяет расположить файлы в архиве в заданном порядке, просмотреть архив, извлечь файлы из архива в заранее созданный каталог.

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

9) Создать самораспаковывающиеся распределенные архивы RAR- и ZIP-архивы.

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

11) Исследуйте свойства форматов сжатия графических данных (файлы .bmp, .gif, .jpg). Результаты занесите в таблицу:

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

12) Используя программу, например, Excel, построить диаграммы по результатам, приведенным в таблицах, и сделать выводы.

Содержание отчета

Отчет должен содержать следующие разделы:

Ответы на контрольные вопросы.

Результаты сжатия файлов в виде таблицы.

Выводы о проделанной работе.

Контрольные вопросы

1. Для чего необходимо создавать архив?
2. Поясните основные алгоритмы архивации.
3. Как можно упаковать информацию при хранении на диске?
4. Приведите команды упаковки данных в архив и распаковки данных из архива для архиватора Winrar.exe в консольном режиме.
5. Как создать защищенный архив?
6. Приведите команды упаковки данных в архив Winzip.exe и распаковки данных из архива.
7. Как создать многотомный архив?

8. Укажите расширение имен файлов продолжения архива.

9. Как получить полную справку по всем возможным режимам работы программы-архиватора?

10. Как создать самораспаковывающий архив?

11. Приведите примеры альтернативных программ архивации.

12. В чем особенность альтернативных программ архивации.

13. Что понимается под интеграцией служебных и прикладных программ с ОС?

Критерии оценивания практической работы:

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

4. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Предметом оценки являются умения и знания. Контроль и оценка дисциплины ОП.12. Основы теории информации осуществляются через экзамен с использованием следующих форм и методов:

1) До экзамена допускаются студенты в полном объеме выполнившие практические работы.

2) Теоретические вопросы на экзамен:

1. Теория информации – дочерняя наука кибернетики.
2. Основные понятия об информации.
3. Основные понятия о канале связи
4. Шум
5. Кодирование.
6. Принципы хранения, измерения информации.
7. Принципы обработки и передачи информации
8. Измерение количества информации,
9. Единицы измерения информации,
10. Носители информации.
11. Передача информации.
12. Скорость передачи информации
13. Вероятностный подход к измерению дискретной информации Клода Шеннона.
14. Вероятностный подход к измерению непрерывной информации Клода Шеннона.
15. Теория вероятности
16. Функция распределения.
17. Дисперсия случайной величины
18. Теорема отсчетов Котельникова и Найквиста — Шеннона
19. Математическая модель системы передачи информации
20. Понятие энтропии.
21. Формула Хартли.
22. Виды условной энтропии.

23. Энтропия объединения двух источников.
24. Статистический подход к измерению информации.
25. Закон аддитивности информации.
26. Формула Шеннона
27. Простейшие алгоритмы сжатия информации.
28. Методы Лемпела-Зива
29. Архиваторы и их виды.
30. Особенности программ архиваторов
31. Помехоустойчивое кодирование.
32. Адаптивное арифметическое кодирование.
33. Цифровое кодирование.
34. Аналоговое кодирование
35. Таблично-символьное кодирование
36. Числовое кодирование
37. Понятие криптографии.
38. Использование криптографии на практике.
39. Различные методы криптографии, их свойства
40. Методы шифрования
41. Криптография с симметричным ключом
42. Криптография с открытым ключом.
43. Шифрование с использованием перестановок.
44. Шифрование с использованием замен.

Из представленных вопросов формируется 25 билетов, по два теоретических вопроса в билете.

Критерии оценки экзамена:

5 «отлично» выставляется, если студент:

- полностью раскрыл содержание материала в объеме, предусмотренном программой и учебником, правильно решил практическое задание;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил практическое задание, сопутствующие ответу;
- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя (возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя).

4 «хорошо» выставляется, если:

ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

3 «удовлетворительно» выставляется, если:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись

затруднения или допущены ошибки в определении понятий, использовании терминологии, практике и выкладках, исправленные после нескольких наводящих вопросов преподавателя;

- студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме;
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

2 «неудовлетворительно» выставляется, если:

- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;
- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя;
- студент обнаружил полное незнание и непонимание изучаемого учебного материала или не смог ответить ни на один из поставленных вопросов по изучаемому материалу.