МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ИЖЕВСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»

УТВЕРЖДАЮ

Проректор по учебной и воспитательной работе

_____С.Л. Воробьева

"17" 06 2019 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

Кодирование информации

Квалификация _____бакалавр

Направление подготовки 09.03.03 Прикладная информатика

Ижевск 2019

1. Цели и задачи дисциплины

Дисциплина «Кодирование информации» предполагает ознакомление с основными понятиями и теоретическими основами теории кодирования информации - методов передачи, хранения и защиты информации по различным каналам связи, а именно: теории кодов, исправляющих ошибки в каналах связи с шумами; криптологии, состоящей из криптографии и криптоанализа; а также сжатия данных (передачи информации по каналам связи без шума).

Задачи дисциплины. 1. В части курса, посвященной теории кодирования, предлагается ознакомление с базовыми понятиями теории линейных кодов (основные понятия, кодирование и декодирование линейных кодов, границы объемов кодов, методы построения кодов), а также теории циклических кодов (кольцо многочленов над полем Галуа, определение циклического кода, необходимое и достаточное условие существования циклического кода с порождающим многочленом g(x), кодирование и декодирование циклических кодов, коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона), QR-коды, коды экономических номенклатур.

2. Вторая часть курса посвящена введению в криптологию, здесь излагаются основные стандарты шифрования данных (DES, AES, российский стандарт шифрования данных ГОСТ 28147-89), теорема Шеннона о существовании совершенно секретных шифров, а также основные криптосистемы с открытыми ключами, цифровые подписи, базирующиеся на основных криптосистемах. Здесь же рассматриваются вопросы применения теории кодирования в криптографии (кодовые асимметричные криптосистемы, проблемы аутентификации, блоковые шифры, проблемы распределения секретов).

3. В третьей части курса, посвященной сжатию данных излагаются основные методы сжатия данных – методы побуквенного кодирования, критерий однозначности кодирования, теорема Шеннона; основные методы адаптивного кодирования (методы Лемпела-Зива,), сжатие аудио, видео-информации.

2. Место дисциплины в структуре ООП

Дисциплина относится к части, формируемой участниками образовательных отношений.

Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-5.

Дисциплина изучается во взаимосвязи с материалом других дисциплин по практическому решению задач на персональных компьютерах и обеспечивает внедрение информационных технологий в научно-исследовательский процесс. Умения и навыки приобретаются студентами в процессе занятий и в процессе самоподготовки.

В рамках дисциплины студенты должны освоить современные информационные технологии, базирующиеся на применении электронно-вычислительной техники, математического, программного и информационного обеспечения, а также средств и систем связи, уметь использовать электронные и сетевые ресурсы для решения прикладных пользовательских задач и проведения научных исследований.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины « Кодирование информации»

(перечень планируемых результатов обучения по дисциплине)

В процессе освоения дисциплины студент осваивает и развивает следующие компетенции:

- Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью. способностью соблюдать требования законов и иных нормативных правовых актов, нетерпимо относиться к коррупционному поведению (ПК-5);

В результате изучения дисциплины студент должен:

Иметь представление об области применимости методов передачи, хранения и защиты информации для исследования различных явлений и процессов. Знать методы теории кодирования для решения задач передачи информации по каналам связи с шумами; знать криптографические методы защиты информации от несанкционированного доступа для передачи информации с использованием как криптосистем с секретными ключами, так и криптосистем с открытыми ключами; уметь создавать цифровые подписи, используя основные криптосистемы, RSA, криптосистемы на эллиптических кривых; знать методы теории информации для решения задач передачи информации по каналам связи без шума. Уметь оценить возможности применения и применять методы передачи, хранения и защиты информации для решения конкретных прикладных задач (в частности создания цифровых подписей, защиты паролей в банках). Владеть основными методами теории помехоустойчивого кодирования для передачи информации по каналам связи с помехами такими как методы кодирования и декодирования линейных кодов, методы кодирования и декодирования циклических кодов (кодов БЧХ, Рида-Соломона); владеть основными методами теории сжатия данных – методы кодирования для стационарных источников, адаптивные методы кодирования, универсальные методы; владеть основными методами теории защиты информации от несанкционированного доступа – владеть методами защиты информации как с помощью криптосистем с секретными ключами, так и с помощью криптосистем с открытыми ключами, владеть методами построения цифровых подписей.

Уметь работать с кодами для экономических номенклатур, со штрих-кодами. Уметь разрабатывать и использовать QR-коды.

3.1 Перечень компетенций с индикаторами их достижений

Номер/индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студент должен:		
		Знать	Уметь	Владеть
ПК-5	Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.	Способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, защиты от несанкционированного доступа	Работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, приме-	Методами информационных технологий для кодирования и защиты информации

			нять в профессиональной деятельности автоматизированные информационные системы	

4. Структура и содержание дисциплины

Общая трудоемкость составляет 3 зач.ед. (108 часов).

Вид учебной работы, часов	Очная форма обучения	Заочная форма обучения
	Семестр	Семестр
	3	3
1.Аудиторная работа, всего:	42	10
Лекции	14	4
Практические занятия	28	6
2.Самостоятельная работа студентов (СРС):	66	98
-рефераты - контрольная работа -самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала, учебников и учебно-методических пособий, подготовка к практическим занятиям и пр.)	66	28 70
Итоговый контроль: экзамен		
Общая трудоемкость дисциплины	108	108

4.1 Структура дисциплины

№ п/п	Семестр	Недели семестра	Раздел дисциплины (модуля), темы раздела	Виды учебной работы, включая СРС и трудоемкость (в часах, очно/заочно))						Форма: -текущего контроля успеваемости, СРС (по неделям семестра); -промежуточной аттестации (по семестрам)
				всего	лекция	практические занятия	лаб. занятия	семинары	СРС	
1	3	1	Кодирование информации	52	6/2	18/4			28	2КР
2	3	2	Сжатие информации	18	4/2	4/2			10	СР
3	3	4	Элементы криптологии	26	2	4			20	2КР, СР
4	3	6	Цифровая подпись	12	2	2			8	СР
Итого				108	14/4	28/6			66/98	Экз.

4.3 Содержание разделов дисциплины (модуля)

№№ п/п	Название раздела	Содержание раздела в дидактических единицах
1.	Кодирование информации	Кодирование в двоичном симметричном канале - Модель канала связи, скорость кода, пропускная способность. Теорема Шеннона (без доказательства). Вероятность ошибки декодирования. Кодирование и декодирование. Коды обнаружения и исправления ошибок. Общие свойства линейных кодов. QR-коды. Коды экономических номенклатур.
2.	Сжатие информации	Сжатие информации - Разделимые и префиксные коды. Метод Хаффмена. Метод Фано. - Энтропия. Метод Шеннона для бернуллиевских источников.
3	Элементы криптологии	Элементы криптологии - Введение в криптологию. Секретность и имитостойкость. Основные идеи. Криптография и криптоанализ. - Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. - Теорема Шеннона о существовании совершенно секретных шифров. - Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES). - Криптографические системы с открытыми ключами.
4	Цифровая подпись	Цифровая подпись. Законодательство. Техническая реализация

4.5 Практические занятия

№ п/п	№ раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (час.)
1.	1.	Модель канала связи, скорость кода, пропускная способность. Стандартное расположение. Линейные коды. Кодирование и декодирование.. Методы построения новых кодов из заданных. Комбинирование кодов. Совершенные коды. Коды Хэмминга, способы задания, кодирование, декодирование. Циклические коды. Кодирование и декодирование циклических кодов.	12
2.	2.	Сжатие текстовой и графической информации. Способы сжатия. Плотность сжатия	4
3	3	Секретность и имитостойкость. Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. Криптографические системы с открытыми ключами. Криптосистема RSA.	10
4	4	Формирование и анализ цифровой подписи	2

4.6 Содержание самостоятельной работы и формы ее контроля

№ п/п	Раздел дисциплины (модуля), темы раздела	Всего часов	Содержание самостоятельной работы	Форма контроля
1.	Кодирование информации	36	Работа с учебной литературой. Решение задач и выполнение контрольной работы	2КР
2.	Сжатие информации	10	Работа с учебной литературой.	СР
3.	Элементы криптологии	14	Решение задач и выполнение контрольных работ	2КР, СР
4.	Цифровая подпись	6	Работа с учебной литературой	СР

5 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Литература

№ п/п	Наименование	Автор(ы)	Год и место издания	Количество экземпляров	
				в библиотеке	на кафедре
1	Кодирование и защита информации	Акмаров П.Б.,	Ижевская ГСХА, 2016	ЭБС «Руконт»	
2	Информатика: Учебник. - 2-е изд., перераб. и доп.	Сергеева И. И.	- М.: ИД ФОРУМ: ИНФРА-М, 2011.	ЭБС «Руконт»	

5.3 Перечень Интернет-ресурсов

1. Интернет-портал ФГБОУ ВО «Ижевская ГСХА» (http: portal/izhgsha.ru);
2. Сайт http: pravo/gov.ru

5.4 Методические указания по освоению дисциплины

Перед изучением дисциплины студенту необходимо ознакомиться с рабочей программой дисциплины, размещенной на портале и просмотреть основную литературу, приведенную в рабочей программе в разделе «Учебно-методическое и информационное обеспечение дисциплины». Книги, размещенные в электронно-библиотечных системах доступны из любой точки, где имеется выход в «Интернет», включая домашние компьютеры и устройства, позволяющие работать в сети «Интернет». Если выявили проблемы доступа к указанной литературе, обратитесь к преподавателю (либо на занятиях, либо через портал академии).

Для изучения дисциплины необходимо иметь чистую тетрадь, объемом не менее 48 листов для выполнения заданий. Перед началом занятий надо бегло повторить материал из курсов дисциплин «Информатика», «Информационные технологии в экономике». Для изучения 3-го раздела дисциплины необходимо найти в справочно-консультационной системе «Консультант-плюс» (доступ свободный с портала академии) Федеральные законы «О защите информации», «О государственной тайне» и ознакомиться с ними.

Для эффективного освоения дисциплины рекомендуется посещать все виды занятий в соответствии с расписанием и выполнять все домашние задания в установленные преподавателем сроки. В случае пропуска занятий по уважительным причинам, необходимо подойти к преподавателю и получить индивидуальное задание по пропущенной теме.

Полученные знания и умения в процессе освоения дисциплины студенту рекомендуется применять для решения своих задач, не обязательно связанных с программой дисциплины. Например, передать в закодированном виде какое-либо письмо своим друзьям по электронной почте, а потом, при необходимости, помочь раскодировать это сообщение. Также консультируйте знакомых пользователей вычислительной техники по вирусам и антивирусным программам.

Владение компетенциями дисциплины в полной мере будет подтверждаться Вашим умением ставить конкретные задачи по кодированию и защите информации, а также выявлять существующие проблемы.

Полученные при изучении дисциплины знания, умения и навыки рекомендуется использовать при выполнении курсовых и дипломных работ(проектов), а также на учебных и производственных практиках.

5.5 Перечень информационных технологий, включая перечень информационно-справочных систем (при необходимости)

1. СПС «Консультант-плюс»
2. Программы MICROSOFT OFFICE

6 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Мультимедийные лекционные аудитории, Компьютеры Pentium IV и выше, программное обеспечение MS Office, электронные таблицы MS Excel

ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Кодирование информации»

1. Методические материалы, определяющие процедуры оценивания компетенций

1.1 Описание показателей, шкал и критериев оценивания компетенций

Показателями уровня освоенности компетенций на всех этапах их формирования являются:

1-й этап (уровень знаний):

– Умение отвечать на основные вопросы и тесты на уровне понимания сути – удовлетворительно (3).

- Умение грамотно рассуждать по теме задаваемых вопросов – хорошо (4)
- Умение формулировать проблемы по сути задаваемых вопросов – отлично (5)

2-й этап (уровень умений):

- Умение решать простые задачи с незначительными ошибками - удовлетворительно (3).
- Умение решать задачи средней сложности – хорошо (4).
- Умение решать задачи повышенной сложности, самому ставить задачи – отлично (5).

3-й этап (уровень владения навыками):

- Умение формулировать и решать задачи из разных разделов с незначительными ошибками - удовлетворительно (3).
- Умение находить проблемы, решать задачи повышенной сложности – хорошо (4).
- Умение самому ставить задачи, находить недостатки и ошибки в решениях – отлично (5).

2.2 Методика оценивания уровня сформированности компетенций в целом по дисциплине

Уровень сформированности компетенций в целом по дисциплине оценивается
на основе результатов текущего контроля знаний в процессе освоения дисциплины – как средний балл результатов текущих оценочных мероприятий в течение семестра;

на основе результатов промежуточной аттестации – как средняя оценка по ответам на вопросы экзаменационных билетов и решению задач;

по результатам участия в научной работе, олимпиадах и конкурсах.

Оценка выставляется по 4-х бальной шкале – неудовлетворительно (2), удовлетворительно (3), хорошо (4), отлично (5).

2.Типовые контрольные задания тесты и вопросы

2.1Задания для текущего контроля

1. Дана кодовая таблица азбуки Морзе:

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

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

2. Закодируйте с помощью азбуки Морзе слова ИНФОРМАТИКА, ДАННЫЕ, АЛГОРИТМ.
3. Закодируйте с помощью азбуки Морзе свое имя и фамилию.
4 Мальчик заменил каждую букву своего имени ее номером в алфавите. Получилось 46151. Как зовут мальчика?
5 Зашифрованная пословица.
Чтобы рубить дрова, нужен 14, 2, 3, 2, 7, а чтобы полить огород - 10, 4, 5, 1, 6.
Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
Самый колючий зверь в лесу - это 12, 13.
А теперь прочитайте пословицу: 1, 2, 3, 4, 5, 1, 6 7, 8, 9, 10, 11 9, 4, 7, 4, 13, 12, 14
6 Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: "Я УМЕЮ КОДИРОВАТЬ ИНФОРМАЦИЮ". Что необходимо предусмотреть, чтобы зашифрованный текст был записан без пропусков?
7 Дана кодировочная таблица (первая цифра кода - номер строки, вторая - номер столбца)

	1	2	3	4	5	6	7	8	9
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	"				

Рис. 1.

. С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ! А ТЫ?
Используя кодировочную таблицу на рис. 1, расшифруйте текст: 252015383503040538351115030400 38.
8.Придумайте свою кодировочную таблицу и зашифруйте с ее помощью свой домашний адрес.
9 "Шифр Цезаря". Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется третьей после нее буквой в алфавите, который

считается написанным по кругу. Используя этот шифр, зашифруйте слова ИНФОРМАЦИЯ, КОМПЬЮТЕР, ЧЕЛОВЕК.
10. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря.
11 "Шифр Виженера". Это шифр представляет шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 31913191и т.д. Используя в качестве ключевого слово ВАГОН, закодируйте слова: АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ.
12. Слово НССРХПЛСГХСА получено с помощью шифра Виженера с ключевым словом ВАЗА. Восстановите исходное слово.
13"Шифр перестановки". Кодирование осуществляется перестановкой букв в слове по одному и тому же общему правилу. Восстановите слова и определите правило перестановки: ЛБКО, ЕРАВШН, УМЫЗАК, АШНРРИ, РКДЕТИ.
14 Зашифруйте, используя "шифр перестановки", слова ИНФОРМАЦИЯ, ПРАВИЛА, АЛГОРИТМ.
15Придумайте свой шифр перестановки и с его помощью зашифруйте свое имя и фамилию.
16Какому или каким из перечисленных ниже слов соответствует код Х0:$=+0=? Слова: орнамент, доминион, рифление, строение, смекалка.
17Правило кодирования: после каждой гласной буквы вставляется буква А, а после согласной - Т. Расшифруйте слова: иантфтоартмтааттиактаа, птртиантттеарт.
18Угадайте правило шифровки и расшифруйте слова: ткафетра, ткнитсни, тицартна, ланигиро.
19Пользуясь правилом из задачи 15 зашифруйте фразу: ИНФОРМАТИКА - ЭТО НАУКА О СПОСОБАХ ПОЛУЧЕНИЯ, НАКОПЛЕНИЯ, ОБРАБОТКИ, ПЕРЕДАЧИ И ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ.
20Определите правило шифровки и расшифруйте слова:
АКРОЛДИИТРБОФВНАЗНГИЦЕШ
ЩИКНГФЗОЕРУМЦАЫЦГИХИ
21Для точности передачи сообщений и ликвидации "шумов" в сообщениях используется принцип двукратной последовательной передачи каждого символа. В результате сбоя при передаче информации приемником принята символьная последовательность: "пррраоссптоо". Какое осмысленное сообщение передавалось?
22 Для шифрования каждой буквы используются двузначные числа. Известно, что буква «е» закодирована числом 20. Среди слов «елка», «полка», «поле», «пока», «кол» есть слова, кодируемые последовательностями цифр 11321220, 20121022. Выясните код слова «колокол».
23Для пяти букв 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	110	01	001	10

Определите, какой набор букв закодирован двоичной строкой 1100000100110.
24 Вася пригласил друга Колю в гости, но не сказал ему код подъезда, а прислал сообщение: «в последовательности цифр 8, 4, 9, 3, 6 все четные цифры разделить на два, а из всех нечетных вычесть 1, затем удалить из последовательности полученных цифр первую и третью». Выполнив действия, указанные в сообщении, какой код цифрового замка получил Коля?
25 Маша забыла пароль для входа в WINDOWS XP, но помнила алгоритм его получения из символов «КВМАМ9КВК» в строке подсказки. Если все последовательности символов «МАМ» заменить на «RP», а «КВК» на «1212», а из полу-

чившейся строки удалить 3 последних символа, то полученная последовательность будет паролем. Назовите пароль

26 Для кодирования сообщения, состоящего только из букв A, B, C, D и E, используется неравномерный по длине двоичный код:

A	B	C	D	E
000	11	01	001	10

Какое (только одно!) из четырех полученных сообщений было передано без ошибок и может быть раскодировано:

1) 110000010011110
2) 110000011011110
3) 110001001001110
4) 110000001011110

27 Для кодирования сообщения, состоящего только из букв О, К, Л, М и Б, используется неравномерный по длине двоичный код:

О	К	Л	М	Б
00	01	11	010	0110

Какое (только одно!) из четырех полученных сообщений было передано без ошибок и может быть раскодировано:

1) 110001001001110
2) 10000011000111010
3) 110001001101001
4) 1000110001100010

28 На первом месте в цепочке стоит одна из бусин А, Б, В. На втором - одна из бусин Б, В, Г. На третьем месте - одна из бусин А, В, Г, не стоящая в цепочке на первом или втором месте. Задание: выписать все такие цепочки.

29 Для составления цепочек разрешается использовать 5 бусинок, помеченных буквами А Б Е Ж И. Каждая цепочка должна состоять из 4 бусинок, при этом должны соблюдаться правила:

1) любая цепочка начинается буквой А
2) после гласной буквы не может снова идти гласная, а после согласной - согласная.
3) буквы в цепочке не должны повторяться

Задание: выписать все допустимые цепочки.

30 Для составления цепочек разрешается использовать 6 бусинок, помеченных буквами А Б Е Ж И К. Каждая цепочка должна состоять из всех 6 бусинок, при этом должны соблюдаться правила:

1) любая цепочка начинается гласной буквой
2) после гласной буквы не может снова идти гласная, а после согласной - согласная.
3) буквы в цепочке не должны повторяться

Задание: сколько всего существует таких цепочек?

31 Имеется (неизвестное нам) слово из 8 букв. Оно подвергается шифрованию по следующим правилам:

1. На 1-м этапе буквы попарно меняются местами по следующей схеме: 1«3 2«5 4«7 6«8 (то есть меняются местами 1 и 3 буквы, 2 и 5 и так далее).
2. На 2-м этапе для получившейся строки из 8 букв смотрим: если крайние буквы различны по гласности (одна из них - гласная, другая - согласная), то результат шифрования является окончательным, в противном случае получившуюся на предыдущем этапе строку преобразуем по схеме 1®2®3®4®5®6®7®8®1 (выполняем циклический сдвиг вправо, то есть первая буква ставится на место второй, вторая - на место третьей, ... последняя - на место первой), после чего снова выполняем этапы 1 - 2. Таким образом, для некоторых исходных слов этапы 1-2 могут повторяться многократно, пока на этапе 1 не получится окончательный результат

шифрования.
Задание: в результате шифрования получена строка БИЛКРАКО.
Каким было исходное слово?
32 Имеется исходный набор 8-буквенных слов:
КАРАНДАШ МАРЦИПАН МАРГАРИН МАРТЫШКА ТРЯПОЧКА
Выбрать из этого набора 8-буквенных слов два слова (по своему усмотрению) и зашифровать их по правилам, указанным в задаче 28
33. Выполнить сжатие информации методом RLE по заданию преподавателя, вычислить контрольные суммы и коэффициент сжатия.
34. Выполнить сжатие информации методом Шеннона-Фано, построить кодовое дерево и определить коэффициент сжатия методом Шеннона-Фано
35. Выполнить сжатие информации методом Хаффмана, построить кодовое дерево и определить коэффициент сжатия методом Хаффмана
36. Исследовать эффективность сжатия файлов различных форматов С помощью стандартного архиватора (WinZip, WinRar, 7-Zip и т.п.) выполнить сжатие различных документов, В качестве текстового документа нужно взять файл, который не содержит рисунков. Число символов должно быть более 3000 знаков.
37. Расшифруйте латинскую пословицу, зная, что она зашифрована шифром Цезаря с ключом $k = 5$ (пробелы и запятые - остаются без изменений):

XN ANX UFHJR, UFWF GJQQZR

38. Определите ключ шифра сдвига, которым зашифровано одно из, возможно самых знаменитых, изречений Гая Юлия Цезаря:

MVEZ MZUZ MZTZ

39. Неизвестный русский последователь Цезаря, не ищущий легких путей, использует для шифрования преобразование:

$$C_i = (M_i * k + n) \bmod 32$$

где k и n - натуральные числа, M_i и C_i - коды i-ых символов исходного текста и шифротекста соотвественно.
Шифруются только прописные русские буквы, остальные символы остаются без изменений. В частности, при k = 2 и n = 0 был получен шифротекст:
ВИДРЖ. ААИРЪЪЬК ЮАКЬВААОЬДАЪРК.
К сожалению, получатель шифротекста так и не смог **правильно** его расшифровать :(. При внимательном рассмотрении оказалось, что все дело в выборе параметра k. Найдите все значения параметра k из диапазона [1, 31], использование которых создает нерасшифровываемые шифры.
40. Шифр Цезаря.
Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.
41 Алгоритм шифрования ГОСТ 28147-89.
Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.
42. Задание №3. Алгоритм шифрования RSA.
Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.
43. Функция хеширования.

Найти хеш–образ своей Фамилии, используя хеш–функцию , где n = pq, p, q взять из Задания №3.
44. Электронная цифровая подпись.

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

45. Используя хеш-образ текстового документа не менее 10 страниц, вычислите электронную цифровую подпись по схеме RSA.

2.2 Тесты

1. Сколько существует в коде Морзе различных последовательностей из точек и тире, длина которых равна 3 символа? _____
2. В алфавите языка племени «тамба-амба» две буквы: Й и Ы.

Сколько различных 5-буквенных слов можно образовать в этом языке? ____

3. Сколько существует различных последовательностей из символов «точка» и «тире» длиной от 2 до 3 символов (включительно)? ____
4. В некоторой стране автомобильный номер длиной 5 символов составляется из заглавных букв (всего используется 5 букв) и десятичных цифр в любом порядке. Каждый символ кодируется одинаковым и минимально возможным количеством битов, а каждый номер — одинаковым и минимально возможным количеством байтов. Сколько байт памяти необходимо для хранения 40 автомобильных номеров? _____
5. Отметьте все префиксные коды (для которых выполняется условие Фано).

- А-00, Б-01, В-10, Г-11
- А-00, Б-01, В-1, Г-011
- А-0, Б-10, В-11, Г-101
- А-00, Б-10, В-110, Г-111
- А-0, Б-10, В-110, Г-111

6. Для 5 букв латинского алфавита заданы их двоичные коды: A-000, B-01, C-100, D-10, E-011 Определите, какой набор букв закодирован двоичной строкой 0110100011000 В ответе запишите цепочку символов без пробелов, например ABCDE. _____
7. Для кодирования некоторой последовательности, состоящей из букв А, Б, В, Г и Д, решили использовать неравномерный двоичный код, позволяющий однозначно декодировать двоичную последовательность, появляющуюся на приёмной стороне канала связи. Использовали код: А-111, Б-110, В-100, Г-0 Укажите, каким кодовым словом может быть закодирована буква Д. Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, укажите кратчайшее из них.

- 001
- 00
- 101
- 10

8. Для кодирования сообщений, состоящих только из букв .5 букв A, B, C, D и E, используется неравномерный код: A-00, B-11, C-01, D-010, E-0110 Определите, какое из приведённых сообщений было передано правильно и может быть декодировано.

- 110001001001110
- 10000011000111010
- 110001001101001
- 1000110001100010

9. Как называется сигнал, который в любой момент

времени может принимать любые значения в заданном диапазоне? В ответе введите прилагательное в единственном числе. _____

10. Каким термином называют представление единого объекта в виде множества отдельных элементов?_____
11. Какова основная причина перехода от аналоговых сигналов к дискретным в современной технике?

- надежность передачи данных
- экономия электроэнергии
- удобство для пользователя
- дешевизна электронных устройств
- упрощение разработки схем

12. Отметьте все правильные утверждения.
- дискретизация необходима для хранения данных в памяти компьютера
- в памяти компьютера можно хранить аналоговые данные
- при дискретизации, как правило, происходит потеря информации
- дискретизация не приводит к потере информации
- органы чувств человека воспринимают дискретные сигналы

13. Отметьте все утверждения, справедливые для алфавитного подхода к измерению количества информации.
- количество информации зависит от длины сообщения
- количество информации зависит от её новизны для получателя
- учитывается, что одни символы встречаются чаще, а другие - реже
- количество информации зависит от количества используемых символов
- чем больше мощность алфавита, тем больше количество информации

14. Слово ТОР закодировано с использованием алфавита из 256 символов. Определите количество информации в этом сообщении в байтах. _____
15. Слово КИТ закодировано с использованием алфавита из 32 символов. Определите количество информации в этом сообщении в битах. _____
16. Дан текст из 500 символов. Известно, что символы берутся из таблицы размером 16 × 16, в которой все ячейки заполнены разными символами. Определите информационный объём текста в байтах._____
17. Для кодирования секретного сообщения используются 12 специальных знаков. При этом символы кодируются одним и тем же минимально возможным количеством битов. Определите информационный объём (в байтах) сообщения длиной в 256 символов? _____

2.3 Вопросы для текущего контроля

1. Кодирование в двоичном симметричном канале - Модель канала связи, скорость кода, пропускная способность.
2. Теорема Шеннона (без доказательства).
3. Вероятность ошибки декодирования. Стандартное расположение.
4. Синдром. - Поле Галуа, его свойства, примеры полей Галуа. - Линейные коды.
5. Кодирование и декодирование.
6. Общие свойства линейных кодов.
7. Теорема о связи проверочной и порождающей матриц. - Теорема Глаголева.
8. Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшамова-Гилберта.
9. Методы построения новых кодов из заданных. Комбинирование кодов.
10. Теорема Плоткина.
11. Каскадная конструкция. - Совершенные коды.
12. Теорема о существовании совершенных кодов (без доказательства).
13. Коды Хэмминга над GF(q), способы задания, кодирование, декодирование, единственность.
14. Конструкция кодов Васильева, Оценки снизу и сверху числа совершенных кодов. - Циклические коды. Кольцо многочленов над полем Галуа.
15. Определение циклического кода.
16. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом g(x).
17. Кодирование и декодирование циклических кодов.

18. Примеры циклических кодов: коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона.
19. Сжатие информации - Разделимые и префиксные коды.
20. Стоимость кодирования. Неравенство Крафта- Макмиллана. Теорема Крафта.
21. Теорема МакМиллана. - Оптимальное кодирование.
22. Метод Хаффмена. Метод Фано. - Энтропия. Метод Шеннона для бернуллиевских источников.
23. Теорема Шеннона (с доказательством). - Критерий разделимости побуквенного кодирования.
24. Теоремы Маркова.
25. Алгоритм распознавания разделимости кода. - Универсальное кодирование, теорема Фитингофа. - Код Левенштейна.
26. Код “стопка книг”. - Адаптивные методы сжатия данных.
27. Методы Лемпела-Зива и их модификации. - Адаптивный метод Хаффмена. - Арифметический код.
28. Элементы криптологии - Введение в криптологию.
29. Секретность и имитостойкость. Основные идеи.
30. Криптография и криптоанализ.
31. Криптографические системы с секретными ключами.
32. Подстановки. Перестановки. Полиалфавитные шифры.
33. Шифр с бегущим ключом.
34. Криптографические системы коды. - Теорема
35. Шеннона о существовании совершенно секретных шифров.
36. Стандарт шифрования данных (криптосистема AES, криптосистема ГОСТ, криптосистема DES).
37. Криптографические системы с открытыми ключами.
38. Односторонняя функция с лазейкой. “Шарады” Меркля.
39. Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма. Криптосистема Шамира.
40. Криптосистема RSA и проблема разложения числа на простые сомножители. - Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца.
41. Кодирующие системы Мак Эллиса и Нидеррайтера.
42. Цифровая подпись
43. Законы и нормативно-правовые акты.
44. Антивирусы.
45. Помехозащитные коды.

Вопросы к экзаменам по дисциплине «Кодирование и защита информации»

1. Понятие кодов и кодирования информации.
2. Шифрование информации. Шифры замены и шифры перестановки.
3. Понятие криптосистемы. Симметричные и асимметричные криптосистемы.
4. Понятие информационной безопасности. Виды угроз.
5. Коды обнаружения и исправления ошибок. Основные понятия

6. Двоичный симметричный канал. Кодовое слово. Интервал Хемминга.
7. Блоковые коды. Параметры кодов, линейные и нелинейные коды.
8. Код с проверкой на четность.
9. Код с постоянным весом.
10. Корреляционный код (Код с удвоением).
11. Инверсный код.
12. Методы кодирования экономических объектов.
13. Порядково-серийный код. Избыточность кода.
14. Построение кодов обнаружения ошибок по модулю числа.
15. Код Хемминга.
16. Минимальное расстояние Хемминга и корректирующая способность кода.
17. Методы и принципы создания классификаторов.
18. Структура общероссийских классификаторов. Примеры.
19. История и особенности штрихового кодирования.
20. Одномерные и двумерные штриховые коды.
21. Структура штрих-кода EAN-13.
22. Порядок расчета контрольного разряда в EAN-13.
23. Устройства считывания штрих-кодов
24. Основы построения двумерных кодов. Многоуровневые и матричные коды.
25. Основные области применения матричных кодов.
26. QR-коды. Основные типы.
27. Структура QR –кода. Основные поля.
28. Кодирование и декодирование QR – кодов.
29. История криптографии.
30. Этапы развития криптографии.
31. Электронная цифровая подпись (ЭЦП). Основные понятия и задачи.
32. История развития ЭЦП.
33. Схемы построения ЭЦП.

34. Принципы использования электронной подписи.
35. Виды ЭЦП. Особенности квалифицированной ЭЦП.
36. Удостоверяющие центры.
37. Алгоритмы цифровой подписи.
38. Классификация компьютерных вирусов.
39. Способы защиты от компьютерных вирусов.
40. Технические способы доступа к информации.
41. Инженерная защита информации от несанкционированного доступа.
42. Активные и пассивные средства технической защиты.
43. Общая характеристика устройств хранения данных.
44. Сжатие информации. Алгоритмы сжатия.
45. Основные функции диспетчера архивов.
46. Принципы правового регулирования в сфере информации.
47. Основные права и обязанности обладателя информации.
48. Виды информации по степени открытости.
49. Порядок ограничения доступа к информации.
50. Правовое регулирование информации в сети «Интернет».
51. Регулирование доступа к информации, отнесенной к государственной тайне.