Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ
Первый проректор
_____ /Т.Р. Змызгова /
«31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

образовательной программы высшего образования –
программы специалитета
10.05.03 - "Информационная безопасность автоматизированных систем"
Специализация (Специализация №5):
"Безопасность открытых информационных систем"

Форма обучения: очная

Курган 2023

Рабочая программа дисциплины «Основы теории защиты информации» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»), утвержденным для очной формы обучения 30.06.2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2023ода, протокол № 1.

Рабочую программу составил:
канд. пед. наук, доцент _____ /Т.А. Никифорова/

Согласовано:

Зав. кафедрой «БИАС»
канд. тех. наук, доцент _____ /Д.И. Дик/

Специалист по учебно-методической
работе учебно-методического отдела _____ /Г.В. Казанкова/

Начальник Управления
образовательной деятельности _____ /И.В. Григоренко/

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 5 зачетных единиц трудоемкости (180 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		3
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**96**	**96**
Лекции	32	32
Лабораторные работы	32	32
Практические занятия	32	32
Самостоятельная работа, всего часов в том числе:	**84**	**84**
Подготовка к дифференцироовааному зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	66	66
Вид промежуточной аттестации	**Зачет с оценкой**	**Зачет с оценкой**
	180	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы теории защиты информации» относится к базовым дисциплинам Блока дисциплин модуля «Информационная безопасность».

Изучение дисциплины «Основы теории защиты информации» основывается на базе таких дисциплин как «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Языки программирования» и «Технологии и методы программирования». Знания и навыки, полученные при изучении дисциплины «Основы теории защиты информации», широко используются студентами при изучении общепрофессиональных и специальных дисциплин, связанных с вопросами проектирования, разработки, эксплуатации и внедрения систем защиты информации.

Результаты обучения по дисциплине «Основы теории защиты информации» необходимы для изучения дисциплины «Криптографические методы защиты информации» и для выполнения курсовой работы по дисциплине «Криптографические методы защиты информации», а также выпускной квалификационной работы в части проектирования систем или модулей системы защиты информации.

Освоение следующих компетенций на уровне не ниже порогового: способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1); способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины «Основы теории защиты информации» является формирование общепрофессиональных и специальных компетентностей посредством знакомства студентов с базовыми понятиями теории информации, с основами защиты информации через помехоустойчивое кодирование информации, с основами сжатия информации, с методами оценки объема информации, а также посредством рассмотрения примеров реализации методов кодирования и сжатия информации на практике. Изучение методов защиты информации неразрывно связано с изучением алгоритмов кодирования информации и на их программной реализации.

Задачами освоения дисциплины «Основы теории защиты информации» являются:

- изучение основ системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения алгоритмов кодирования информации;
- изучение основных математических методов, используемых для защиты информации;
- изучение основных алгоритмов кодирования информации для разработки программных модулей реализации этих алгоритмов.

Компетенции, формируемые в результате освоения дисциплины «Основы теории защиты информации»:

- способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1);
- способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3);
- способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности (ОПК-4).

В результате изучения дисциплины «Основы теории защиты информации» обучающийся должен:

иметь представление:

- о месте и роли информационных процессов в обществе (для ОПК-1);
- об истории и направлениях развития понятий: информация, носитель информации, источник сообщений, количество информации (для ОПК-1, ОПК-3);

знать:

- основные понятия теории информации и информационных технологий: информация и способы ее вычисления, многообразие ее форм, основные способы представления информации (для ОПК-1);
- основные классы кодов, их параметры и способы кодирования, основные каналы связи и процесс передачи информации по каналам, их основные формально-математические модели и способы их количественного описания (для ОПК-1, ОПК-3, ОПК-4);
- математические доказательства свойств энтропии, информации дискретного и непрерывного источников; основные теоремы теории информации и кодирования (для ОПК-1, ОПК-3);
- основные принципы и способы кодирования и декодирования информации, характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования, методы исследования кодов и их применение в ЭВМ и системах защиты информации (для ОПК-1, ОПК-3, ОПК-4);
- возможности информационных технологий, направленных на защиту информации (для ОПК-3, ОПК-1);
- формулы расчета количества информации при различных способах измерения количества информации (для ОПК-3);

уметь:

- вычислять количество энтропии и информации в сообщениях дискретного источника канала связи (для ОПК-3);
- закодировать и декодировать сообщения источника одним из изученных кодов, оценить его оптимальность и помехоустойчивость, а также декодировать закодированное сообщение с обнаружением или исправлением возможных ошибок (для ОПК-1, ОПК-3, ОПК-4);
- определить основные характеристики симметричного канала связи (для ОПК-1);

владеть навыками:

- расчета количества информации, вероятности двоичной ошибки на выходе канала связи и вероятности ошибочного декодирования (для ОПК-1, ОПК-3, ОПК-4);
- построения кодирующих и декодирующих алгоритмов для линейных кодов (для ОПК-1, ОПК-3, ОПК-4).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаборатор. работы	Практич. занятия
Рубеж 1	Тема 1.	Информация. Количество информации	2	2	2
	Тема 2.	Энтропия и количество информации	2	2	4
	Тема 3.	Теория кодирования информации	8	8	6
		Рубежный контроль №1 (тестирование и защита рефератов)	1	-	-
Рубеж 2	Тема 4.	Теория помехоустойчивого кодирования информации	8	8	4
	Тема 5.	Применение кодирования для сжатия информации и криптографической защиты информации	8	2	4
	Тема 6.	Основы защиты компьютерной информации	2	8	4
	Тема 7.	Применение стеганографии для сокрытия информации	1	2	6
		Рубежный контроль №2 (решение практических работ)			2
		Всего за семестр:	**32**	**32**	**32**

4.2. Содержание лекционных занятий

ТЕМА 1. Информация. Количество информации

Информация. Различные подходы к определению понятия «информация». Понятие информации в кибернетике, в теории Шеннона. Виды информации. Непрерывная и дискретная формы представления информации. Дискретная и аналоговая информация Свойства информации.

Вопросы и задачи теории информации и кодирования. Математические основы теории информации. Общая схема передачи информации. Система передачи информации как система: ее математическая модель, состав, структура и функция. Роль теории информации и кодирования в науке и современном, информационном обществе. Теория информации и информационные технологии.

ТЕМА 2. Энтропия и количество информации

Количество информации. Различные подходы к измерению количества информации: алгоритмический, объёмный, вероятностный. Формула Шеннона. Формула Хартли. Количество информации по Хартли и Шеннону. Количество и единицы измерения информации.

Случайные дискретные ансамбли с равновероятными и не равновероятными компонентами. Понятие и вычисление энтропии. Энтропия двух и более статистически связанных ансамблей. Энтропия и информация: модель Шеннона и аксиомы

Шеннона. Энтропия объединенного ансамбля и ее свойства. Условная и частная энтропия и их свойства. Дифференциальная энтропия. Избыточность сообщений источника. Количество информации, передаваемой от источника к получателю. Основное свойство информации при ее преобразовании. Реальные и идеальные каналы связи и их характеристики: скорость создания информации, скорость информации и пропускная способность. Симметричные каналы связи и другие виды каналов связи.

ТЕМА 3. Теория кодирования информации

Первая теорема Шеннона. Кодирование в каналах без шума.

Двоичное кодирование символьной информации. Алфавитное неравномерное двоичное кодирование. Основные характеристики неравномерного кода. Условие Фано. Префиксные коды. Кодирование методом Шеннона-Фано, методом Хаффмана и др. Построение неравномерного кода с разделителями. Избыточность кодов. Алфавитное равномерное двоичное кодирование. Байтовый код. Код Морзе. Понятие разрядности кода и ее расчет. Количество и объем информации при передаче информации в равномерном коде. Определение избыточности равномерных кодов. Алфавитное кодирование с неравной длительностью элементарных сигналов. Блочное двоичное кодирование.

ТЕМА 4. Теория помехоустойчивого кодирования информации

Вторая теорема Шеннона. Каналы связи с шумом. Способы обеспечения надежности передачи информации. Принципы построения систем помехоустойчивого кодирования. Информационные и проверочные (корректирующие) биты. Расстояние Хемминга. Корректирующая способность кода. Кодовое расстояние. Относительная избыточность помехоустойчивого кода. Кратность ошибки. Связь между кодовым расстоянием и минимальной кратностью ошибки. Оценка искажения передаваемой информации.

Классификация корректирующих кодов. Коды, обнаруживающие ошибку. Коды, исправляющие коды.

Алгоритмы помехоустойчивого кодирования. Коды Хэмминга. Кодирование по методу четности-нечетности. Двоичный код с защитой сдвоенными элементами. Циклические коды. Алгоритмы кодирования и декодирования циклических кодов. Их схемная реализация.

Коды БЧХ, Рида-Соломона, свёрточные коды. Общие сведения о кодах БЧХ и Рида-Соломона.

ТЕМА 5. Применение кодирования для сжатия информации и криптографической защиты информации

Технические характеристики процессов сжатия данных. Коэффициент сжатия. Потеря качества. Скорость сжатия. Классификация алгоритмов сжатия данных.

Адаптивные алгоритмы сжатия. Кодирование Хаффмана. Верхняя и нижняя границы степени сжатия для кода Хаффмана. Недостатки метода. Арифметическое кодирование. Адаптивное арифметическое кодирование. Кодирование. Декодирование. Недостатки метода. Дифференциальное кодирование. Кодирование. Декодирование. Недостатки метода. Подстановочные или словарно-ориентированные алгоритмы сжатия информации. Методы Лемпела-Зива. Алгоритм LZ (Алгоритм Лемпела-Зива). Алгоритм LZW (Алгоритм Лемпела-Зива-Велча). Сжатие данных RLE. Кодирование. Декодирование. Недостатки метода.

Сжатие информации с потерями. Сжатие графики. Кодирование преобразований. Стандарт сжатия JPEG. Метод сжатия факсимильных изображений CCITT.33. Фрактальный метод сжатия. Рекурсивный (волновой) алгоритм.

Методы сжатия подвижных изображений (видео). Сжатие информации с потерями. Сжатие звука.

ТЕМА 6. Основы защиты компьютерной информации

Защита USB-носителя от компьютерных вирусов. Защита текстовых документов, данных электронных таблиц, данных из БД. Пароли. Востановление данных после удаления. Блокировка посещения сайтов от детей. Защита страницы вКонтакстe. Защита данных в популярных мессенжерах. Способы отследить местоположение смартфона и защита данных смартфона. Тестирование сети.

ТЕМА 7. Применение стеганографии для сокрытия информации

Стеганография для сокрытия информации. Методы сокрытия информации внутри документа.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
		3 семестр	
1	Информация. Количество информации	*Лабораторная работа №1.* Информация. Свойства информации.	2
2	Энтропия и количество информации	*Лабораторная работа №2.* Информация. Различные подходы к измерению количества информации.	2
3	Теория кодирования информации	*Лабораторная работа №3.* Построение двоичного кода с разделителями знаков	2
		Лабораторная работа №4. Построение кода Шеннона-Фано	2
		Лабораторная работа №5. Построение кода Хаффмана	4
4	Теория помехоустойчивого кодирования информации	*Лабораторная работа №6.* Алгоритмы помехоустойчивого кодирования. Код Хэмминга	2
		Лабораторная работа №7. Циклические коды. Алгоритмы кодирования и декодирования циклических кодов.	6
5	Применение кодирования для сжатия информации и криптографической защиты информации	*Лабораторная работа №8.* Методы сжатия информации.	2
6	Основы защиты информации	*Лабораторная работа №9.* Основы защиты информации	8
7	Применение стеганографии для сокрытия информации	*Лабораторная работа №10.* Стеганография	2
		Всего за семестр	**32**

4.4. Практические занятия

Номер темы	Наименование темы	Наименование практических работ	Норматив времени, час.
		3 семестр	
1	Информация. Количество информации	*Практическая работа №1.* Различные подходы к измерению количества информации.	2
2	Энтропия и количество информации	*Практическая работа №2.* Расчет метрик удобочитаемости текста по формулам Флеша и Флеша-Кинсайда и индекса туманности Ганнинга (или Фог-индекс).	4
3	Теория кодирования информации	*Практическая работа №3.* Расчет избыточности кода с разделителями знаков	2
		Практическая работа №4. Расчет избыточности кода Шеннона-Фано и кода Хаффмана	4
4	Теория помехоустойчивого кодирования информации	*Практическая работа №5.* Кодирование по методу четности-нечетности. Двоичный код с защитой сдвоенными элементами. Циклический код.	2
		Практическая работа №6. Относительная избыточность помехоустойчивого кода.	2
5	Применение кодирования для сжатия информации и криптографической защиты информации	*Практическая работа №7.* Сжатие информации с потерями. Сжатие графики. Кодирование преобразований. Стандарт сжатия JPEG.	4
6	Основы защиты компьютерной информации	*Практическая работа №8.* Защита компьютерной информации. Защита USB-накопителя от вирусов.	4
7	Применение стеганографии для сокрытия информации	*Практическая работа №9.* Стеганография	6
	Рубежный контроль 2 (решение практических задач)		2
Всего за семестр			**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ и лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем перед началом работы.

Преподавателем запланировано применение на практических занятиях и лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях и лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к практическим занятиям и лабораторным работам, к рубежным контролям, подготовку к диференцированному зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице.

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение разделов и тем дисциплины, не вошедших в лекционный курс, а именно: Сжатие графической информации с потерями. Фрактальный метод сжатия. Сжатие графической информации с потерями. Рекурсивный (волновой) алгоритм. Методы сжатия подвижных изображений (видео). Сжатие информации с потерями. Сжатие звука. Основы защиты компьютерной информации (Восстановление данных после форматирования, Защита USB-носителя от вирусов)	24
Подготовка к практическим занятиям и лабораторным работам (по 2 ч к каждому занятию)	38
Подготовка к рубежному контролю (по 2 ч на каждый рубеж)	4
Подготовка к диференцированному зачету	18
Всего:	**84**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Банк заданий к рубежным контролям № 1, № 2 и № 3.
5. Вопросы к дифференцированному зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	*Распределение баллов, 4 семестр*						
		Вид учебной работы:	Посещение лекций	Выполнение практических работ	Выполнение и защита лабораторных работ	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$16_б$	$2_б$ x 9 = $18_б$	$3_б$ x 10 =$33_б$	3	10	20
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и на экзамене	60 и менее баллов – неудовлетворительно; 61…73 – удовлетворительно; 74… 90 – хорошо; 91…100 – отлично						
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету) за семестр обучающийся должен набрать по итогам текущего и рубежного контролей не менее 51 балл. В случае, если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета без проведения процедуры промежуточной аттестации обучаемому необходимо набрать не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом на усмотрение преподавателя, бальная оценка может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационные испытания 0 баллов итог балльной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы..						

		Дополнительные баллы начисляются преподавателем. Максимальное количество дополнительных баллов составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачет) набрана сумма 51 балла, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежный контроль № 1 проводятся в форме письменного тестирования и защиты реферата по выбранной теме.

Перед проведением 1-го рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. На рубежный контроль студенту отводится 2 академических часа.

Рубежный контроль № 2 проводится письменно в форме контрольной работы на кодирование сжатие информации (по вариантам). На рубежный контроль студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от правильности ответов. Итоговая оценка формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты решения практических заданий каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответа на вопросы билета. Экзаменационный билет состоит из 2 теоретических вопросов и 1 практического задания. Каждый теоретический вопрос оценивается в 5 баллов, практический — 10 баллов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета с оценкой заносятся преподавателем в экзаменационную ведомость, которые сдаются в орготдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета

1-ый рубежный контроль

1. Какое количество информации по Хартли может содержать система, информационная емкость которой определяется десятичным числом 1250.
2. Найти среднее количество информации по Шеннону в системе со следующим вероятностным распределением $\vec{p}\,(1/2;1/4;1/4)$.
3. Какое максимальное количество информации по Шеннону содержит система со следующим вероятностным распределением $\vec{p}\,(0{,}2;0{,}8)$.
4. Сравните условную и безусловную энтропии системы.

Варианты ответов:

a) $H_Y(X) \geq H(X)$;

b) $H_Y(X) \leq H(X)$.

5. Определить дифференциальную энтропию системы с заданной плотностью распределения вероятностей: $f(x) = \begin{cases} x,\ x \in (0;1) \\ 0,\ x \notin (0;1) \end{cases}$.

2-ой рубежный контроль *(задания контрольной работы)*

Задание 1. Определить количество информации в сообщении и энтропию сообщения на русском языке, содержащем фамилию, имя, отчество, год, месяц и день рождения студента для следующих случаев:

1) для равновероятных символов алфавита;

2) для не равновероятных символов алфавита;

Задание 2. Посчитайте количество информации, приходящейся на один символ, в следующем тексте:

Организационно-правовые формы предприятий в своей основе определяют форму их собственности, то есть, кому принадлежит предприятие, его основные фонды, оборотные средства, материальные и денежные ресурсы. В зависимости от формы собственности в России в настоящее время различают три основные формы предпринимательской деятельности: частную, коллективную и контрактную.

Задание 3. Решите задачу о передаче информации с помощью модема *(по вариантам).*

Вариант 1. Скорость передачи данных через ADSL-соединение равна 512000 бит/с. Через данное соединение передают файл размером 1500 Кб. Определите время передачи файла в секундах.

Вариант 2. Скорость передачи данных через ADSL-соединение равна 1024000 бит/с. Через данное соединение передают файл размером 2500 Кб. Определите время передачи файла в секундах.

Задание 4. Выполнить построение кода Шеннона-Фано, Хаффмана *(по вариантам).*

p1=0,67 p2=0,03 p3=0,1 p4= 0,14 p5=0,15

Задание 5. Выполнить построение помехоустойчивого кода: код Хэмминга, циклический код, метод четности/нечетности *(по вариантам).*

0110101010101010

Примерная тематика вопросов, выносимых на зачет в 3-ом семестре

1. Понятие информации. Сообщения, каналы связи, носители информации, сигналы и данные. Шум. Свойства информации. Виды информации. Непрерывная и дискретная информация. Дискретизация. Теорема Котельникова или теорема Уитекера.
2. Различные подходы к измерению количества информации: объемный, вероятностный и алгоритмический.
3. Энтропия. Вероятностный (энтропийный) подход к измерению количества информации. Формула Хартли (с доказательством). Формула Шеннона (с доказательством). Зависимость между формулой Хартли и формулой Шеннона. Смысл энтропии Шеннона. Свойства энтропии сложных сообщений.
4. Информация и алфавит. Избыточность текстовых сообщений. Относительная избыточность языка.
5. Теория кодирования. Кодирование и декодирование. Первичный и вторичный алфавит. Код. Длина кода. Относительная избыточность кода. Задачи теории кодирования информации. Постановка задачи кодирование информации. Влияние вторичного алфавита на способ кодирования.
6. Теория кодирования. Виды кодирования.
7. Представление чисел (целых со знаком и без знака, вещественных) в памяти ЭВМ.
8. Смещённый код (Код Грея).
9. Кодирование текстовой, звуковой и графической информации.
10. Кодирование информации. Равномерные и неравномерные коды. Условие Фано. Три задачи теории кодирования.
11. Оптимальные коды. Задача оптимизации кода. Задача построения эффективного кода. Первая теорема Шеннона.
12. Префиксные коды. Построение кода Шеннона-Фано. Относительная избыточность кода.
13. Префиксные коды. Кодирование Хаффмана. Построение кода Хаффмана. Относительная избыточность кода.
14. Префиксные коды. Построение неравномерного кода с разделителями. Относительная избыточность кода.
15. Равномерное алфавитное кодирование. Байтовый код. Код Бодо. Относительная избыточность кода.
16. Алфавитное кодирование с неравной длительностью сигнала. Код Морзе. Относительная избыточность кода.
17. Блочное двоичное кодирование. Относительная избыточность кода.
18. Каналы связи с шумом. Способы обеспечения надежности передачи информации. Оценка искажения передаваемой информации.

19. Задача обеспечения надежности передачи информации по каналам связи с шумом. Вторая теорема Шеннона. Принципы построения систем помехоустойчивого кодирования.
20. Помехоустойчивый код. Информационные и проверочные (корректирующие) биты. Расстояние Хемминга. Корректирующая способность кода. Кодовое расстояние. Относительная избыточность помехоустойчивого кода. Кратность ошибки. Связь между кодовым расстоянием и минимальной кратностью ошибки.
21. Классификация корректирующих кодов.
22. Оценка минимального количества контрольных бит, достаточных для обнаружения и исправления одиночной ошибки.
23. Помехоустойчивый код. Код Хэмминга. Построение кодовой таблицы, процедура определения ошибок передачи.
24. Помехоустойчивый код. Кодирование по методу четности-нечетности.
25. Помехоустойчивый код. Двоичный код с защитой сдвоенными элементами.
26. Помехоустойчивый код. Циклические коды.
27. Сжатие данных. Технические характеристики процессов сжатия данных. Коэффициент сжатия. Потеря качества. Скорость сжатия. Классификация алгоритмов сжатия данных.
28. Сжатие данных. Адаптивные алгоритмы сжатия. Кодирование Хаффмана. Верхняя и нижняя границы степени сжатия для кода Хаффмана. Недостатки метода.
29. Сжатие данных. Арифметическое кодирование. Адаптивное арифметическое кодирование. Кодирование. Декодирование. Недостатки метода.
30. Сжатие данных. Дифференциальное кодирование. Кодирование. Декодирование. Недостатки метода.
31. Подстановочные или словарно-ориентированные алгоритмы сжатия информации. Методы Лемпела-Зива. Алгоритм LZ (Алгоритм Лемпела-Зива).
32. Сжатие данных. Алгоритм LZW (Алгоритм Лемпела-Зива-Велча).
33. Сжатие данных RLE. Кодирование. Декодирование. Недостатки метода.
34. Сжатие информации с потерями. Сжатие графики. Кодирование преобразований. Стандарт сжатия JPEG.
35. Метод сжатия факсимильных изображений CCITT.33
36. Сжатие информации с потерями. Сжатие графики. Фрактальный метод сжатия.
37. Сжатие информации с потерями. Сжатие графики. Рекурсивный (волновой) алгоритм.
38. Методы сжатия подвижных изображений (видео).
39. Сжатие информации с потерями. Сжатие звука.

Примерный список задач для зачета:

1. Чему равно количество информации, если получили сообщение о выходе из строя одного из 8 компьютеров в данном отделе?

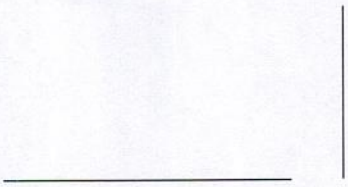
2. Алфавит состоит из букв a, b, c, d. Вероятности появления букв равны соответственно 0,25; 0,25; 0,34; 0,16. Определить количество информации, приходящееся на символ сообщения, составленного с помощью такого алфавита.
3. В корзине лежат 32 шара, среди них 4 белых, а остальные черные. Сколько битов информации содержится в сообщении о том, что из корзины вытащили белый шар?
4. В алфавите некоторого языка всего две буквы. Каждое слово этого языка состоит из m букв. Известно, что можно составить 2048 различных слов. Сколько букв в каждом слове?
5. В алфавите племени БУМ всего 4 буквы (А, У, М, Б), один знак препинания (.) и для разделения слов используется пробел. Подсчитали, что в популярном романе «МУБА» содержится 10000 знаков, из них: букв А – 4000, букв У – 1000, букв М – 2000, букв Б – 1500, точек – 500, пробелов – 1000. Найти энтропию книги.
6. Два сообщения содержат одинаковое количество символов. Количество информации в первом тексте в 1,5 раза больше, чем во втором. Сколько символов содержат алфавиты, если известно, что число символов в каждом алфавите ≤ 10 и на каждый символ приходится целое число бит.
7. Опыт имеет 2 исхода. Докажите, что энтропия такого опыта *max*, если вероятности исходов будут обе равны 0,5.
8. Сообщение состоит из последовательности двух букв А и В, вероятности появления каждой из которых не зависят от того, какая была передана раньше, и равны 0,8 и 0,2 соответственно. Произведите кодирование по методу Шеннона-Фано (по методу Хаффмана): а) отдельных букв; б) блоков, состоящих из двухбуквенных сочетаний; в) блоков, состоящих из трехбуквенных сочетаний. Сравните коды по их экономичности.
9. Первичный алфавит содержит 6 знаков с вероятностями: «пробел» – 0,3; «*» – 0,2; «+» – 0,2; «%» – 0,15; «#» – 0,1 и «!» – 0,05. Постройте неравномерный алфавитный двоичный код с разделителем знаков, префиксный код Шеннона-Фано, префиксный код Хаффмана. Найдите избыточность.
10. Декодировать сообщение методом Шенно-Фано (методом Хаффмана), используя таблицу кодов для русского алфавита: 1001110100011001001111011000101110011100101101010000110101010110000110110111
11. Код Морзе для цифр следующий:

0	– – – – –	5	· · · · ·
1	· – – – –	6	– · · · ·
2	· · – – –	7	– – · · ·
3	· · · – –	8	– – – · ·
4	· · · · –	9	– – – – ·

Считая алфавит цифр самостоятельным, а появление различных цифр равновероятным, найдите избыточность кода Морзе для цифрового алфавита.
12. Определить величину кодового расстояния между двумя комбинациями 1101101, 1001011.
13. Определить код Хемминга для данных кодовых комбинаций: 1101101001110110 и 0101010.

14. Получено машинное слово 10001011110001011001l, закодированное с использованием кода Хемминга. Устраните ошибку передачи.

15. С использованием метода *четности-нечетности* исправить ошибку в передаваемой информации:



16. Дана кодовая комбинация 0111. Поострить циклический код с d_0=3.

17. Принятая кодовая комбинация имеет вид 1111001. В качестве разрешенной кодовой комбинации взята $F(x)=x^5+x^4+x^3+1$, а $P(x)= x^3+ x^2 +1$, или в двоичном виде F(0,1)=0111001, P(x)=1101. Обнаружьте и исправьте ошибку в передаче циклического кода.

18. Закодировать сообщения «AABCDAACCCCDBB», «КИБЕРНЕТИКИ» и «СИНЯЯ СИНЕВА СИНИ», вычислить длины в битах полученных кодов, используя алгоритмы,

LZ77 (словарь — 12 байт, буфер — 4 байта),

LZ78 (словарь — 16 фраз),

LZW (словарь — ASCII+ и 16 фраз).

19. Вычислить длины кодов Хаффмана и арифметического для сообщения AAB, полученного от д. с. в. X со следующим распределением вероятностей P(X = A) = 1/3, P(X = B) = 2/3.

20. Составить арифметический код для сообщения BAABC, полученного от д.с.в. X со следующим распределением вероятностей P(X = A) = 1/4, P(X = B) = 1/2, P(X = C) = 1/4. Каков будет арифметический код для этого же сообщения, если X распределена по закону P(X = A) = 1/3, P(X = B) = 7/15, P(X = C) = 1/5?

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Гуров И.П. Основы теории информации и передачи сигналов [Электронный ресурс]: учебное пособие – С-Пб: БхВ, 2000г. – Доступ из ЭБС «znanium.com».

1. Лебедько Е.Г., Математические основы передачи информации [Электронный ресурс]. Ч.5: учеб. пособие для вузов.-СПб: СПбГУ ИТМО, 2010.-93 с. – Режим доступа: https://www.intuit.ru/studies/courses/57/57/info, свободный. – Загл. с экрана.

2. Лебедько Е.Г., Теоретические основы передачи информации: СПб [Электронный ресурс] : Лань, 2011.-352с. Ил.- (Учебники для вузов. Специальная литература). – доступ из ЭБС «Лань».

3. Лидовский В. В. Теория информации [Электронный ресурс]: Учебное пособие. М.: Компания Спутник+, 2004. – 111 с. – ISBN 5-93406-661-7. - Доступ из ЭБС «znanium.com».

7.2 Методические материалы

1. Лабораторный практикум «Теория информации» для студентов очной и очно-заочной формы обучения 10.05.03, 10.03.01 по дисциплине «Основы теории защиты информации». – Курган: КГУ, 2016. – 100 с. (на правах рукописи).

2. Методические указания к выполнению практических работ по дисциплине «Основы теории защиты информации» для студентов очной и очно-заочной формы обучения направлений (специальностей) 10.05.03, 10.03.01. – Курган: КГУ, 2016. – 96 с. (на правах рукописи)

3. Методические указания к выполнению контрольной работы по дисциплине «Основы теории защиты информации» для студентов очной и очно-заочной формы обучения направлений (специальностей) 10.05.03, 10.03.01. – Курган: КГУ, 2017. – 20 с. (на правах рукописи)

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Прохоров В.С. Теория информации - http://profbeckman.narod.ru/Informat.files/Teorinf.pdf (Обращение 20. 08.16).
2. Ватолин Д.С. Алгоритмы сжатия изображений. – М: МГУ, 1999. http://graphics.cs.msu.su/library/our_publications/index.htm.
3. Методы сжатия изображений http://www.intuit.ru/department/graphics/compression/
4. Witten I. H., Neal R. M., Cleary J. G. Arithmetic Coding for Data Compression, CACM, 1987 (доступна на http://www.compression.ru).

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, LibreOffice.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при выполнении заданий лабораторных работ: Windows XP, LibreOffice, программы, разработанные преподавателем.

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

12. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн.

Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1.

Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения.

Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Основы теории защиты информации»

образовательной программы высшего образования –
программы специалитета
10.05.03 - Информационная безопасность автоматизированных систем
Направленность: Безопасность открытых информационных систем

Форма обучения: очная

Трудоемкость дисциплины: 5 з.е. (180 академических часа)
Семестр: 3 (очная форма обучения)
Форма промежуточной аттестации: зачет с оценкой
Содержание дисциплины. Основные разделы.

Информатика и кибернетика. Основные понятия информатики как науки. Основы защиты компьютерной информации. Теория информации. Теория информации Шеннона. Теотрия кодирования информации. Кодирование информации как защита информации. Сжатие данных как защита информации. Стеганография.