

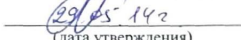
Белорусский государственный университет

УТВЕРЖДАЮ

Декан гуманитарного факультета

 В.Е. Гурский

(подпись)

 29.05.14

(дата утверждения)

Регистрационный № УД-2014-1689/р.

Теория информации

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:

1-31 03 07

Прикладная информатика (по направлениям)

Факультет Гуманитарный

Кафедра Информационных технологий

Курс (курсы) 3

Семестр (семестры) 6

Лекции 20

Экзамен

Практические (семинарские)
занятия

Зачет 6

Лабораторные
занятия 14

Курсовая работа (проект)

Аудиторных часов по
учебной дисциплине 34

Всего часов по
учебной дисциплине 52

Форма получения
высшего образования очное

Составил(а) А.В. Овсянников, кандидат технических наук, доцент

2014 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Теория информации» разработана для специальности 1-31 03-07 «Прикладная информатика (по направлениям)» высших учебных заведений.

Целью изучения дисциплины является:

- ознакомить студентов с основными положениями теории информации и кодированием, являющимися необходимым компонентом математического образования и освоение которых обеспечит осознанное понимание многих разделов специальных дисциплин.
- сформировать умения грамотно анализировать основные проблемы, возникающие в практической деятельности специалиста информационного профиля;
- научить будущих специалистов информационного профиля применять полученные знания по теории информации и кодирование в практической деятельности;
- привить умение самостоятельно, посредством математического аппарата, осваивать реальные, характерные для специальности задачи;
- развить логическое мышление, аналитические способности, интеллект, необходимые для решения научных и практических задач информационного профиля.

Основными задачами дисциплины являются:

- обеспечение овладения студентами теоретических основ данного курса, добиться четкого знания определений и основных теорем изучаемых разделов курса.
- выработка четкого овладения основными методами решения задач;
- выработка умения формулировать задачи информационного профиля в точных и строгих соотношениях с использованием соответствующих математических символов;
- выработка понимания универсальности математических методов в задачах описания явлений и процессов в разных областях практической деятельности;
- формирование у студентов научного мировоззрения, рассмотрения предметов и явлений во всей их определенности, без искажений;
- подготовка высококвалифицированного специалиста, развитие его интеллекта и способностей к логическому и алгоритмическому мышлению.

Цели и основные задачи дисциплины достигаются

- проведением всех видов учебных занятий;
- осуществлением эффективного текущего и итогового контроля занятий и навыков студентов;
- организацией самостоятельной работы студентов.

Предшествующими данной дисциплине являются: «Математический анализ», «Алгебра и теория чисел», «Программирование» (I курс), «Дифференциальные уравнения», «Теория вероятностей и математическая статистика», «Теория графов», «Методы вычислений» (II курс), которые закладывают фундаментальные математико-логические понятия, на которых базируется теоретическая и прикладная основа курса «Теория информации». Дисциплина «Теория информации» формирует новые знания и умения необходимые для освоения дисциплин входящих в учебные планы 4 курса, в частности, «Математическое моделирование», а также ее знания и умения могут использоваться в ходе дипломного проектирования.

В результате освоения курса «Теория информации и кодирование» студент должен:

знать:

- методологические основы теории информации, включающие следующие понятия: количество информации, энтропия и ее виды, представление и виды информации, измерение и преобразования информации;
- элементы и методики информационного анализа;
- модели технических дискретных и непрерывных каналов связи;
- теоретические основы дискретных и непрерывных систем передачи информации;
- алгоритмы кодирования информации;
- алгоритмы сжатия данных;
- алгоритмы цифровой подписи;
- криптографические методы защиты информации;
- алгоритмы шифрования данных;

уметь:

- применять методологические основы информации в практической деятельности;
- применять алгоритмы кодирования в практической деятельности;
- применять алгоритмы сжатия данных в практической деятельности;
- применять цифровую подпись в практической деятельности;
- использовать криптографические методы в решении важных прикладных задач;
- ориентироваться в имеющейся литературе по теории информации и кодированию;
- самостоятельно расширять круг математических знаний по теории информации и кодированию, используя необходимую научную, учебную и справочную литературу.

приобрести навыки:

- самостоятельного решения практических задач связанных с применением знаний полученных при изучении дисциплины;
- самостоятельного расширения круга математических знаний по теории информации и кодированию, используя необходимую научную, учебную и справочную литературу.

Изучение курса «Теория информации» рассчитано на 52 часа, в том числе 34 часов аудиторных занятий.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1.

Введение. Базовые понятия и определения теории информации

Определение информации. Классификация информации. Качества информации относительно ее неопределенности. Цели и задачи теории информации. Хронологические даты в развитии теории информации. Количество информации. Подходы к измерению количества информации. Мощность системы счисления и количество информации. Энтропия. Аддитивные и неаддитивные формы энтропии. К-энтропия.

Универсальная схема передачи информации и ее основные элементы. Источники сообщений и их классификация. Каналы связи, характеристики и классификация. Помехи систем передачи информации.

Информационные системы (ИС). Классификация ИС. Свойства ИС. Жизненный цикл и процессы в ИС. Эффективности функционирования ИС.

Тема 2.

Информационный анализ

Понятие информационного анализа. Характеристики информированности. Задача классификации и ранжирования ситуации. Задача информационного анализа в условиях динамики изменения информированности. Экспертные оценки определения весовых коэффициентов параметров информированности.

Тема 3.

Каналы связи систем передачи информации

Классификация информационных каналов. Технические характеристики современных каналов связи систем передачи информации. Математические модели дискретных каналов связи с помехами без памяти и с памятью. Математические модели непрерывных каналов связи.

Тема 4.

Дискретные систем передачи информации

Преобразование непрерывных сигналов в дискретные. Дискретизация непрерывного сигнала по времени. Теорема Котельникова. Квантование сигнала по уровню. Источник дискретных сообщений (ИДС). Классификация, свойства и характеристики ИДС. Избыточность ИДС. Избыточность языка. Относительные частоты появления символов в тексте. Скорость создания сообщений.

Марковские модели ИДС. Энтропия на одну букву последовательности длиной N . Влияние статистической связи на избыточность.

Информационные характеристики приема сообщения. Условная и взаимная информация. Условная энтропия. Скорость передачи информации по каналу связи. Пропускная способность канала связи.

Эффективность дискретных систем передачи информации

Тема 5.

Непрерывные систем передачи информации

Переход от дискретных к непрерывным по времени моделям характеристик теории информации. Энтропия непрерывных сообщений. Дифференциальная энтропия. Взаимная информация для непрерывных ансамблей.

Характеристики непрерывных систем передачи информации с учетом помех в канале связи. ϵ -энтропия. Скорость передачи информации по непрерывному каналу связи. Пропускная способность непрерывного канала связи. Граница Шеннона.

Тема 6.

Введение в теорию кодирования

Базовые определения и понятия теории кодирования. Цели и задачи кодирования. Общие подходы к классификации систем кодирования. Общая классификация и характеристика избыточных и неизбыточных кодов.

Равномерные неизбыточные коды: двоично-десятичные, прямого замещения, отраженные. Код Грея.

Неравномерные побуквенное кодирование. Неравенство Крафта. Прямая и обратная теоремы Шеннона для источника общего вида. Оптимальные коды и их эффективность. Коды Шеннона, Шеннона-Фано, Хаффмана. Кодовые деревья. Избыточность оптимальных кодов. Сравнение оптимальных кодов.

Тема 7.

Основы теории помехоустойчивого кодирования

Постановка задачи помехоустойчивого кодирования. Теорема о переработке информации. Неравенство Фано. Прямая и обратная теоремы кодирования.

Понятие о корректирующих кодах.

Коды с обнаружением ошибок. Код с проверкой на четность. Код с двойной проверкой на четность. Код с m -повторением. Инверсный код. Корреляционный код. Код Бергера.

Коды с обнаружением и исправлением ошибок. Код Хемминга.

Тема 8.

Принципы, методы и алгоритмы сжатия информации

Принципы сжатия данных. Характеристики алгоритмов сжатия и их применимость. Принципы энтропийного кодирования. Кодирование длин серий (RLE-алгоритм). Алгоритм LZ-77. Алгоритм LZ-78. Арифметическое сжатие. Дельта-кодирование.

Сравнение степени сжатия популярных архиваторов.

Сжатие данных с потерями. Методы сжатия изображений и видеоинформации.

Сжатие аудиоданных.

Тема 9.

Принципы, методы, алгоритмы шифрования и скрытия информации

Понятие о шифровании. Классификация шифров.

Классификация шифров по типу преобразования над открытым текстом. Шифры перестановки. Шифры замены. Шифры гаммирования.

Скремблирование. Цифровая подпись. Стеганография.

Криптоанализ и простейшие методы криптоанализа. Полный перебор (метод грубой силы) в криптоанализе. Частотный криптоанализ.

Тема 10.

Методология информационной безопасности. Принципы защиты информации

Понятие о информационной безопасности и защите информации. Виды угроз информационной безопасности. Классификация технических каналов утечки информации.

Модели информационной безопасности. Модель Белла-ЛаПадулы. Модель избирательного (дискреционного, разграничительного) управления доступом. Модель мандатного управления доступом. Модель Take-Grant. Ролевая модель управления доступом. Вероятностные модели.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов						Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Материальное обеспечение занятия	Литература занятия	
1	2	3	4	5	6	7	8	9
1	Введение. Базовые понятия и определения теории информации	2			2	Эл. през.	[1-4]	Опрос, защита л/р.
2	Информационный анализ	2				Эл. през.	[1-4]	Опрос
3	Каналы связи систем передачи информации	2				Эл. през.		Опрос
4	Дискретные систем передачи информации	2			4	Эл. през.	[1-4]	Опрос, защита л/р.
5	Непрерывные систем передачи информации	2				Эл. през.	[1-4]	Опрос
6	Введение в теорию кодирования	2				Эл. през.	[1-6]	опрос
7	Основы теории помехоустойчивого кодирования	2			4	Эл. през.	[1-8]	Опрос, защита л/р.
8	Принципы, методы и алгоритмы сжатия информации	2				Эл. през.	[1-8]	Опрос
9	Принципы, методы и алгоритмы шифрования и скрытия информации	2			4	Эл. през.	[1-8]	Опрос, защита л/р.
10	Методология информационной безопасности. Принципы защиты информации	2				Эл. през.	9	Опрос, контр. работа

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Кудряшов, Б.Д. Теория информации: Учебник для вузов. - СПб.: Питер, 2009. – 320 с.
2. Лидовский, В.В. Теория информации: Учеб.пособие. - М.: Компания Спутник+, 2004. . – 111 с.
3. Потапов, В.Н. Введение в теорию информации: Учеб.пособие. - Новосибирск: Ново-сиб. гос. ун-т., 2009. – 104 с.
4. Духин, А.А. Теория информации: Учебное пособие/А.А.Духин. - М.: Гелиос АРВ, 2007. - 248 с ,
5. Цымбал, В.П. Теория информации и кодирование: Учебник. – 4-изд. Перераб. И доп. – К.: Вища шк., 1992. – 262 с.
6. Фомичев, В.М. Дискретная математика и криптология. Курс лекций / Под общей ред. д-ра физ.-мат. н. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003. -400 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

7. Золотарёв, В. В., Овсчин, Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под. ред. чл.-кор. РАН Ю. Б. Зубарева. - М.: Горячая линия-Телеком, 2004. - 126 с.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. - М.: Мир, 1986. - 576 с.
9. Мельников, В.П. Информационная безопасность и защита информации : учеб. Пособие для студ.высш. учеб. Заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 3-е изд., стер. – М.: Издательский центр «Академия», 2008. – 336 с.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Оценка уровня знаний студента при выполнении контрольной работы производится по десятибалльной шкале в соответствии с критериями, утвержденными Министерством образования Республики Беларусь.

Оценка промежуточных учебных достижений студента также осуществляется по десятибалльной шкале.

Для оценки достижений студента используется следующий диагностический инструментарий:

- защита выполненных на лабораторных занятиях индивидуальных заданий;
- защита контрольной работы;
- проведение текущих контрольных вопросов по отдельным темам;
- выступление студента на конференции по подготовленному реферату;
- сдача зачета по дисциплине.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ РАБОТ

1. Определение наиболее мощной системы счисления для представления числовой информации. Вычисление информационных характеристик статистической совокупности.
2. Модели дискретных каналов связи с помехами с памятью и без памяти. Определение доля типичных последовательностей. Расчет характеристик источников дискретных сообщений. Расчет характеристик различных языковых систем. Расчет информационных характеристик приема сообщения. Оценка эффективности систем передачи информации.
3. Решение задач кодирования и декодирования сообщений в равномерных кодах. Решение задач кодирования и декодирования сообщений в оптимальных кодах (Шеннона, Шеннона-Фано, Хаффмана). Решение задач с кодами обнаруживающими ошибки. Решение задач с кодами обнаруживающими и исправляющими ошибки (код Хемминга).
4. Моделирование алгоритмов сжатия данных. RLE-алгоритм. LZ-77. LZ-78. Арифметическое сжатие. Дельта-кодирование. Унарное кодирование. Решение практических задач с простейшими шифрами перестановок и замены. Исследование алгоритма цифровой подписи. Решение задач частотного анализа в криптоанализе.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
(примерная форма)

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола) ²
1.			

² При наличии предложений об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на ____/____ учебный год

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (название кафедры) (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

_____ (ученая степень, ученое звание)

_____ (подпись)

_____ (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ (ученая степень, ученое звание)

_____ (подпись)

_____ (И.О.Фамилия)