

МИНОБРНАУКИ РОССИИ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ИНФОРМАТИКИ

УТВЕРЖДАЮ

Декан факультета, профессор

С.П. Сущенко

« 29 » декабря 2011 г.

**Рабочая программа дисциплины
ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЕ**

Направление подготовки

010300 Фундаментальная информатика и информационные технологии

Наименование магистерской программы

Управление проектами по разработке программного обеспечения

Квалификация (степень) выпускника

Магистр

Форма обучения

Очная

Томск
2011

1. Цели освоения дисциплины

Целями освоения дисциплины «Теория информации и кодирование» являются углубление фундаментальных знаний в области современных информационных технологий, в частности, формирование основ знаний по теории информации, принципам кодирования, изучение важнейших алгоритмов в этой области, овладение средствами разработки и исследования таких алгоритмов.

2. Место дисциплины в структуре ООП магистратуры

Данная учебная дисциплина входит в раздел «М.2. Общенаучный цикл. Вариативная часть. Курс по выбору студента» ООП по направлению подготовки 010300 – Фундаментальная информатика и информационные технологии.

Для изучения дисциплины необходимы компетенции, сформированные у обучающихся в результате освоения дисциплин «дискретная математика», «основы программирования», «алгоритмы и анализ сложности», «теория вероятностей и математическая статистика» ООП подготовки бакалавра.

Для того чтобы приступить к изучению дисциплины «Теория информации и кодирование», студент должен обладать следующими знаниями и умениями:

- знать основы компьютерных технологий и языков программирования;
- иметь твердые знания основных структур данных в программировании;
- знать основы теории вероятностей и математической статистики;
- уметь строить алгоритмы решения поставленных задач;
- уметь разрабатывать программы для ЭВМ;
- уметь выполнять анализ сложности алгоритмов и программ.

Данная учебная дисциплина входит в набор дисциплин ориентированных на изучение методов и моделей разработки программного обеспечения. Данная дисциплина предваряет дисциплину «Математические основы защиты информации и информационной безопасности» и производственную практику по профилю «Управление проектами по разработке программного обеспечения».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Теория информации и кодирование»

Данная дисциплина способствует формированию следующих компетенций, предусмотренных ФГОС-3 по направлению подготовки ВПО 010300 – Фундаментальная информатика и информационные технологии:

- «способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий (ПК-1)» в части применения языков программирования для разработки программного обеспечения;
- «способность профессионально решать задачи производственной и технологической деятельности с учетом современных достижений науки и техники, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования; разработку математических, информационных и имитационных моделей по тематике выполняемых исследований; создание информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных; разработку тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям; разработку эргономичных человеко-машинных интерфейсов (ПК-2)» в части разработки и исследования алгоритмов кодирования;
- «способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математике, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в

области информационных технологий, а также знания, которые находятся на передовом рубеже данной науки (ПК-5)» в части разработки программных средств для решения задач сжатия данных, помехоустойчивого кодирования и реализации вычислений с сверхдлинными числами.

В результате освоения дисциплины обучающийся должен:

- Знать: основные понятия теории информации, принципы разработки эффективных алгоритмов кодирования и обработки информации, методы исследования этих алгоритмов.

- Уметь: разрабатывать и реализовывать в виде программ эффективные алгоритмы, доказывать корректность алгоритмов, анализировать временную и пространственную сложность алгоритмов кодирования и обработки информации.

- Владеть: способами разработки эффективных алгоритмов кодирования и обработки информации, методами доказательства корректности алгоритмов, методами исследования временной и пространственной сложности алгоритмов кодирования и обработки информации.

4. Структура и содержание дисциплины «Теория информации и кодирование»

Общая трудоемкость дисциплины составляет 5 зачетные единицы, 180 часа, из них лекции – 32 часов, лабораторные работы – 32 часа, самостоятельная работа – 116 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
				Лекции	Лабораторные работы	Самостоятельные работы	
1	Коды, информация, энтропия	1	1-5	8	8	20	Контроль реализации программ. Письменный контроль по теории.
2	Помехоустойчивое кодирование	1	6-10	8	8	20	Контроль реализации программ. Письменный контроль по теории.
3	Случайные числа	1	11-15	8	8	20	Контроль реализации программ/ Письменный контроль по теории.
4	Алгоритмы над сверхдлинными числами	1	15-20	8	8	20	Контроль реализации программ
5	Промежуточная аттестация	1	21			36	Письменный экзамен

1. Коды, информация, энтропия

Канал связи и сообщение. Информация дискретного сообщения. Энтропия. Свойства информации и энтропии. Кодирование равномерным кодом. Избыточность. Кодирование Хаффмана. Оптимальность кодирования. Влияние корреляции частей сообщения на избыточность. Эвристические методы кодирования сообщений со сжатием без потерь информации.

2. Помехоустойчивое кодирование

Избыточное кодирование. Кодирование с проверкой четности. Кодовое расстояние по Хеммингу. Граница Хемминга. Обнаруживающая и исправляющая способность кода. Линейные коды, кодирование и декодирование, синдром. Свойства линейных кодов. Вычисление минимального кодового расстояния по порождающей матрице. Код Хемминга. Расширенный код Хемминга. Полиномиальная арифметика в поле чисел $(0,1)$. Неприводимые полиномы. Циклические коды, кодирование и декодирование, синдром. Построение матрицы линейного кода по порождающему полиному. Циклический код Хемминга. Свойства циклических кодов.

3. Случайные числа

Линейная конгруэнтная последовательность Лемера. Параметры для достижения максимального периода последовательности. Свойства последовательности в случае составного модуля, в частности в виде степени 2. Последовательность в случае модуля – простого числа. Малая теорема Ферма. Вычисление первообразного корня по модулю простого числа. Мощность датчика последовательности. Дважды случайный датчик из двух различных последовательностей, ее период. Статистические методы проверки последовательности на случайность. Генерирование последовательности с заданным законом распределения. Генерирование последовательности с нормальным распределением.

4. Алгоритмы над сверхдлинными числами

Прямое двоичное представление в памяти компьютера сверхдлинных чисел. Сравнение, сложение и вычитание «в столбик» сверхдлинных целых. Умножение «в столбик». Деление «русским крестьянским методом». Деление «в столбик». Трудоемкость алгоритмов «в столбик». Простейший быстрый алгоритм умножения рекурсивным методом «разделяй и властвуй», его трудоемкость. Итерационный метод деления, его трудоемкость. Модулярная арифметика, ее применимость. Трудоемкость операций сложения, вычитания и умножения. Переход от прямого к модулярному представлению чисел. Переход от модулярного представления чисел к прямому методом Гарнера. Вычисление обратных по модулю величин обобщенным алгоритмом Евклида.

Лабораторный практикум

Все лабораторные работы выполняются в виде разработки архитектуры программ, реализации на одном из языков программирования (например, Паскаль, Делфи, Си) и их тестирования на специально подготовленных тестах.

1. Построение кода Хаффмана для символов конкретного текста.
2. Кодирование и декодирование текста заданным неравномерным кодом.
3. Построение кода со сжатием повторяющихся символов. Кодирование и декодирование для этого кода.
4. Линейный случайный датчик и его исследование.
5. Дважды случайный датчик.
6. Датчик для битовых последовательностей.
7. Кодирование и декодирование кодом Хемминга.
8. Кодирование и декодирование циклическим кодом.

9. Деление длинных чисел "в столбик".
10. Быстрое возведение в степень длинных чисел.
11. Быстрое возведение в степень длинных чисел по модулю.
12. Быстрое умножение длинных чисел рекурсивным разрезанием пополам.
13. Обобщенный алгоритм Евклида для коротких чисел.
14. Проверка делимости сверхдлинного числа на короткие простые числа.
15. Реализация алгоритма Гарнера восстановления чисел по остаткам.

5. Образовательные технологии

В ходе преподавания дисциплины используются следующие образовательные технологии:

- лекции в сопровождении иллюстративного материала в форме презентаций,
- лабораторные занятия в компьютерном классе,
- самостоятельная работа студентов,
- активные и интерактивные формы занятий:
- лекции-консультации,
- лекции с разбором конкретных ситуаций,
- самостоятельное проектирование и программирование алгоритмов кодирования,
- мастер-классы экспертов.

Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 30% аудиторных занятий.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Виды самостоятельной работы студентов:

- 1) повторение и самостоятельное изучение основного теоретического материала и ознакомление с дополнительной литературой, интернет-ресурсами;
- 2) выполнение индивидуальных проектов, разработка программ, реализующих отдельные алгоритмы в соответствии с заданием преподавателя.

В качестве учебно-методического обеспечения самостоятельной работы используется основная и дополнительная литература по предмету, Интернет-ресурсы, материал лекций, указания, выданные преподавателем при проведении лабораторных работ.

Темы индивидуальных лабораторных заданий имеют общий шаблон: разработать и реализовать программу, выполняющую некоторый алгоритм по заданию преподавателя. При этом некоторые из программ (требующие наибольших временных затрат от студентов) должны выполняться небольшими группами студентов (по 2-3 человека) с самостоятельным планированием и распределением работы внутри группы.

Пример задания для самостоятельной работы:

Реализовать алгоритмы помехоустойчивого кодирования и декодирования произвольного файла расширенным кодом Хемминга с кодовым расстоянием 4.

Задание на СРС:

1. Спроектировать программу кодирования, на вход которой поступает имя файла, который требуется закодировать. Программа должна закодировать входной файл. На выходе программы – закодированный файл.
2. Спроектировать программу декодирования, на вход которой поступает имя файла, который требуется декодировать. Программа должна декодировать входной файл. На выходе программы – декодированный файл.
3. Запрограммировать протестировать и отладить программы кодирования и декодирования. Для этого подготовить тестовые файлы с различным содержимым. На

основе тестов показать, что однократные ошибки в файле успешно исправляются, а двукратные – обнаруживаются.

Контроль самостоятельной работы студентов.

Текущий контроль – еженедельный контроль по реализации отдельных алгоритмов.

Промежуточная аттестация.

Промежуточная аттестация по итогам освоения дисциплины – не менее 3-х раз в течение семестра в виде письменного ответа на теоретические вопросы по содержанию дисциплины и итоговый письменный экзамен.

Общая оценка составляется на основе результатов текущего контроля и итогового письменного экзамена.

Вопросы и задания для промежуточной аттестации:

1. Связь между информацией и энтропией.
2. Соотношения, связывающие условную и безусловную энтропию и информацию.
3. Оптимальность кодирования методом Шеннона-Фано-Хаффмана.
4. Свойства индивидуальной и средней энтропии.
5. Свойства индивидуальной и средней информации.
6. Эвристические методы сжатия данных.
7. Свойства линейных и циклических кодов, связь между ними.
8. Линейные коды. Кодирование и декодирование. Синдром.
9. Корректирующая и обнаруживающая способность кода в зависимости от минимального кодового расстояния. Граница Хэмминга.
10. Вычисление минимального кодового расстояния по матрице кодирования.
11. Полиномы в поле $(0,1)$, операции над ними. Неприводимые полиномы.
12. Циклические коды. Кодирование и декодирование. Синдром.
13. Построение матрицы линейного кода по порождающему полиному.
14. Циклический код Хемминга.
15. Свойства циклических кодов, обнаружение пачек ошибок.
16. Условия при которых период последовательности максимальный.
17. Линейная конгруэнтная последовательность с модулем m – простым числом.
18. Условия, при которых период последовательности равен $m - 1$.
19. Малая теорема Ферма. Первообразный корень по модулю.
20. Генерация чисел с нормальным распределением при заданном среднем и среднеквадратичном отклонении.
21. Генерация чисел с произвольным заданным распределением.
22. Дважды случайная последовательность, алгоритм генерации. Период последовательности.
23. Мощность датчика случайных чисел.
24. Линейная конгруэнтная последовательность с модулем $m = 2k$. Ее свойства.
25. Прямое представление сверхдлинных чисел.
26. Алгоритм алгебраического сложения-вычитания. Трудоемкость.
27. Умножение «в столбик» сверхдлинных чисел. Трудоемкость.
28. Быстрое умножение сверхдлинных чисел методом разделяй и властвуй. Трудоемкость.
29. Деление русским крестьянским методом сверхдлинных чисел. Трудоемкость.
30. Деление методом «в столбик» сверхдлинных чисел. Трудоемкость.
31. Деление методом итераций сверхдлинных чисел. Трудоемкость при использовании в нем быстрого умножения.
32. Алгоритм быстрого умножения в большую степень.
32. Модульное представление сверхдлинных чисел. Китайская теорема об остатках.
33. Выполнение операций сложения, вычитания, умножения сверхдлинных чисел. Трудоемкость.
34. Обобщенный алгоритм Евклида. Трудоемкость.

35. Восстановление чисел из модульного представления в прямое. Трудоемкость.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

	<i>Список основной литературы:</i>				Электронный вариант
	Автор	Название	Изд-во	Год издания	
1.	Ахо А., Хопкрофт Дж., Ульман Дж.	Построение и анализ вычислительных алгоритмов: Пер. с англ.	М.: Мир	1979	
2	Вирт Н.	Алгоритмы + структуры данных = программы: Пер. с англ.	М.: Мир	1985	
3	Кнут Д.	Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы: Пер. с англ.	М.: Мир	1977	
4	Кормен Т., Лейзерсон Ч., Ривест Р.	Алгоритмы: построение и анализ.: Пер. с англ.	М.: МЦНМО	2000	
5	Панин В.В.	Основы теории информации.	М.: БИНОМ. Лаборатория знаний	2009	
	<i>Список дополнительной литературы</i>				
	Автор	Название	Изд-во	Год	
1	Рейнгольд Э., Нивергельд Ю., Део Н.	Комбинаторные алгоритмы. Теория и практика/ Пер. с англ.	М.: Мир	1980	
2	Вернер М.	Основы кодирования: учебник для вузов	М.: Техносфера	2006	

в) программное обеспечение и Интернет-ресурсы:

1. Транслятор с языка Си или Паскаль в операционной системе Windows или Linux.
2. Программа для проведения презентаций – Power Point или аналогичная.
3. Интернет-браузер – Microsoft Explorer или аналогичный.

8. Материально-техническое обеспечение дисциплины

Лекционная аудитория должна быть оборудована проекционным оборудованием: компьютером и проектором, а также программными средствами для их функционирования.

Компьютерный класс, компьютеры должны быть объединены в локальную сеть с выходом в Интернет.

Программа составлена в соответствии с требованиями ФГОС ВПО с учетом рекомендаций и ООП ВПО по направлению «010300 – Фундаментальная информатика и информационные технологии» и профилю подготовки «Управление проектами по разработке программного обеспечения».

Автор – д.т.н., профессор кафедры теоретических основ информатики Ю.Л. Костюк
Рецензент – к.т.н, доцент, зав. кафедрой теоретических основ информатики
А.Л. Фукс

Программа одобрена на заседании кафедры теоретических основ информатики ТГУ
от 14.12.2011 , протокол № 10/11