

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
А. В. Замятин
« 16 » Июль 20 23 г.



Рабочая программа дисциплины

Теория кодирования

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.02.11

СОГЛАСОВАНО:

Руководитель ОП

В.Н. Тренькаев

Председатель УМК

С.П. Суценко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин.

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.

2. Задачи освоения дисциплины

- Изучить основы помехоустойчивого кодирования.
- Приобрести практические умения и навыки помехоустойчивого кодирования.
- Научиться применять понятийный аппарат помехоустойчивого кодирования для решения практических задач профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Математика».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Десятый семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам:

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:

-лекции: 32 ч.

-практические занятия: 16 ч.

в том числе практическая подготовка: 16 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в предмет теории кодирования. Коды минимальной избыточности
Основные понятия теории кодирования. Однозначность кодирования
Коды минимальной избыточности

Тема 2. Коды, исправляющие ошибки
Основные понятия помехоустойчивого кодирования. Границы для кода
Линейные коды: определение, задание, кодовое расстояние, исправление ошибок,
границы для кодового расстояния

Код Хемминга

Линейный МДР-код

Коды Рида-Маллера. Мажоритарное декодирование

Циклический код

Коды Голея

БЧХ-код

Код Рида-Соломона

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу, выполнения индивидуальных заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных практических работ.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в десятом семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из двух частей.

Первая часть представляет собой два теоретических вопроса. Ответы на вопросы даются в развернутой форме и проверяют ИОПК-3.1.

Вторая часть представляет собой практическое задание и проверяет ИОПК-3.2 и ИОПК-3.3. Ответ предполагает выбор алгоритма для решения задачи, получение решения и интерпретацию полученного результата.

Продолжительность экзамена 1,5 часа.

Примерный перечень теоретических вопросов

1. Понятие кодирования и декодирования. Математическая постановка задачи кодирования и декодирования. Алфавитное кодирование.

2. Основные требования, предъявляемые к коду.

3. Когда кодирование называется однозначным. Необходимое и достаточное условие однозначного кодирования.

4. Три достаточных условия однозначности кода.

5. Критерий однозначности алфавитного кодирования Маркова. Его геометрическая формулировка. Уметь применять геометрический критерий на практике.

6. Оценка минимальной длины неоднозначно декодируемого слова.

7. Коэффициент избыточности кода (определение). Код с минимальной избыточностью (определение).

8. Неравенство Мак-Миллана. Может ли существовать двоичный код с длинами слов 1,2,2,3,3,3 ?

9. Когда неравенства Мак-Миллана приобретает достаточный характер.

10. Алгоритм Шеннона построения кода с заданными длинами слов.

11. Свойства оптимальных кодов

12. Алгоритм Фано. Алгоритм Хаффмана.

13. Типы ошибок, которые возникают при передаче информации.

14. Понятие блочного и древовидного кода. Основные определения, связанные с блочным кодом (кодовые слова, длина кода, мощность кода)

15. Принцип максимального правдоподобия (суть), таблица кодирования (структура, принцип использования)
16. Метрическое пространство Хемминга. Вектор ошибок. Вес вектора ошибки и расстояние между принятым и переданным словом.
17. Кодовое расстояние. Связь кодового расстояния с возможностями кода исправлять и обнаруживать ошибки. Примеры.
18. Граница Хемминга.
19. Линейный код: определение, размерность линейного кода. Кодовое расстояние линейного кода. Мощность линейного кода.
20. Порождающая матрица линейного кода: определение, назначение. Проверочная матрица линейного кода: определение, назначение, определение кодового расстояния по проверочной матрице.
21. Исправление и обнаружение ошибок линейными кодами: стандартное расположение для таблицы декодирования, необходимое и достаточное условие исправления ошибки в случае стандартного расположения для таблицы декодирования.
22. Понятие синдрома вектора. Алгоритм декодирования с использованием синдрома.
23. Верхняя граница линейного кода (граница Плоткина). Может ли существовать линейный (7,4)-код, исправляющий 2 ошибки?
24. Граница Синглтона. Граница Варшамова-Гильберта.
25. Код Хемминга: с длиной кодового слова $n = 2^m - 1$, с произвольной длиной слова. Кодовое расстояние для кода Хемминга. Декодирование кода Хемминга. Кодирование кодом Хемминга.
26. Коды Рида-Маллера: построение порождающей матрицы кода Рида-Маллера r -го порядка длины 2^m , кодовое расстояние.
27. Декодирование кодов Рида-Маллера: мажоритарный принцип декодирования, порядок декодирования информационных символов, принцип построения проверочных сумм для информационных символов 1-го, 2-го и т.д. порядков.
28. Циклический код: определение, соответствие кодовое слово – многочлен, связь циклического сдвига вектора с умножением классов вычетов многочленов.
29. Описание циклических кодов с помощью многочленов: умножение (по модулю $x^n - 1$) слова циклического кода на произвольный многочлен, определение порождающего многочлена, степень порождающего многочлена, деление кодовых слов на порождающий многочлен, теорема о том, какие многочлены могут быть порождающими многочленами циклических кодов.
30. Порождающая и проверочная матрица циклического кода. Описание циклического кода посредством корней порождающего многочлена. Проверочная матрица кода в поле $GF(2^m)$ – расширении поля $GF(2)$.
31. Исправление ошибок циклическими кодами. Теорема Меггита. Алгоритм исправления ошибок, использующий теорему Меггита. Исправление пактов ошибок циклическими кодами.
32. Циклический код, исправляющий две ошибки. Теорема о границе БЧХ. БЧХ-коды. Построение порождающего многочлена БЧХ-кода.

Примеры задач:

1. Выяснить, является ли кодирование φ однозначным. Если нет, то указать слово, декодируемое неоднозначно:

$$\varphi(a_1) = ab, \quad \varphi(a_2) = ba, \quad \varphi(a_3) = cba, \quad \varphi(a_4) = cab, \quad \varphi(a_5) = acba, \\ \varphi(a_6) = abba, \quad \varphi(a_7) = cccb$$

2. Построить схему оптимального префиксного алфавитного кодирования по методу Хаффмена для распределения вероятностей P появления букв алфавита

$$V = \{a, b, c, d, e, f\}$$

в сообщении при двоичном кодировании: $P = \{0,5; 0,2; 0,1; 0,09; 0,08; 0,03\}$.

3. Найдите расстояние Хэмминга между 2-ичными последовательностями (101010) и (011100).

4. Найдите кодовое слово, в которое линейный (5,3)-код с порождающей матрицей

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

кодирует информационное слово $u=(011)$.

5. Найдите проверочную матрицу для линейного (5,3)-код с порождающей матрицей

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Проверить, являются ли кодовыми слова (01110) и (11110).

6. Закодировать (7,4)-кодом Хемминга сообщение (1101).

7. Восстановить информационное слово, если кодирование было осуществлено (10,4)-кодом Хемминга и принято слово (1001 0110 01)

8. Декодировать слово $u = (1100\ 0001\ 0111\ 1000)$, зная, что был использован $RM(2,4)$ код. (разобран на лекции).

9. Циклический (7,4) код порождается многочленом $g(x) = x^3 + x^2 + 1$. Дано двоичное представление слова «дача»:

$$(1010\ 0100\ 1010\ 0000\ 1110\ 01111\ 1010\ 0000)$$

(для двоичного представления слова «дача» использован ASCII-код). Закодируйте это слово.

10. Запишите порождающий многочлен кода БЧХ длины $n=15$, исправляющего 2 ошибки.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если:

а) студент дал полный и развернутый ответ на теоретические вопросы;

б) решение практического задания верное.

Оценка «хорошо» выставляется, если:

а) ответ студента на теоретические вопросы в целом полный, но имеются незначительные замечания;

б) решение практического задания верное или содержит арифметические ошибки, не влияющие на используемый алгоритм

Оценка «удовлетворительно» выставляется, если:

а) ответ студента на теоретические вопросы не полный;

б) решение практического задания содержит ошибки, существенно повлиявшие на результат.

Оценка «неудовлетворительно» выставляется, если:

а) ответ студента на теоретические вопросы не полный и содержит серьезные ошибки;

б) решение практического задания не доведено до конца или для его решения выбран неверный алгоритм.

Если в течение семестра студент посетил не менее 75% занятий и выполнил все индивидуальные задания на положительную оценку, то он освобождается от выполнения практической части билета.

11. Учебно-методическое обеспечение

- а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - <https://moodle.tsu.ru/course/view.php?id=12834>
- б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).
- в) План лекционных / практических занятий по дисциплине.
- г) Основная и дополнительная учебная литература.

12. Перечень учебной литературы и ресурсов сети Интернет

- а) основная литература:
 - Рацеев С. М. Элементы высшей алгебры и теории кодирования / Рацеев С. М.. – Санкт-Петербург : Лань, 2022. – 656 с.. URL: <https://e.lanbook.com/book/187575>.
 - Гуров С. И. Конечные поля и группы перестановок: приложение в теории кодирования и комбинаторике : учебное пособие / С. И. Гуров ; Моск. гос. ун-т им. М. В. Ломоносова, Фак. вычислительной математики и кибернетики. – Москва : КДУ, 2018. – 190 с.
 - Цымбал В. П. Задачник по теории информации и кодированию : [учебное пособие для студентов вузов] / В. П. Цымбал. – Изд. стер.. – Москва : Ленанд, 2020. – 273, [2] с.: ил., табл. – (Основы защиты информации ;№ 10:)
 - Колесник В. Д. Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов) : [учебное пособие для вузов по направлению "Информатика и вычислительная техника" специальности "Автоматизированные системы обработки информации и управления"] / В. Д. Колесник. – Москва : Высшая школа, 2009. – 549, [1] с.: ил. – (Для высших учебных заведений)
- б) дополнительная литература:
 - Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение : [учебное пособие для студентов, обучающихся по направлениям подготовки "Прикладные математика и физика" и "Телекоммуникации"] / Р. Морелос-Сарагоса ; пер. с англ. В. Б. Афанасьева. - М. : Техносфера, 2006. – 319 с.: рис. - (Мир связи ;IX-05:)
 - Вернер М. Основы кодирования : учебник для вузов : [по направлению "Прикладные математика и физика"] / М. Вернер ; пер. с нем. Д. К. Зигангирова. – Москва : Техносфера, 2006. – 286 с.: ил. – (Мир программирования ;VIII-03:)
 - Золотарев В. В. Помехоустойчивое кодирование. Методы и алгоритмы : справочник / В. В. Золотарев, Г. В. Овечкин. – М. : Горячая линия – Телеком, 2004. – 123 с.: ил.
 - Коды, исправляющие ошибки : учебно-методическое пособие. Ч. 1 / Том. гос. ун-т, Радифизический факультет ; сост. Н. В. Евтушенко, А. В. Коломеец. – Томск : [б. и.], 2004. – 29 с.: ил.
- в) ресурсы сети Интернет:
 - Волков А. Теория помехоустойчивого кодирования [Электронный ресурс] / Видеолекции НГУ: Теория Помехоустойчивого Кодирования, 2006 – 2016. URL: https://www.youtube.com/playlist?list=PLHKx-rx3MlyE5vjrd4bv91LAGs9_AdBCu (дата обращения: 01.06.2022)
 - Ромащенко А. Теория кодирования // Просветительский проект «Лекториум» – 2019. - URL: <https://www.lektorium.tv/course/22864> (дата обращения: 01.06.2022)
 - Скачек В. Классическая теория кодирования и новые приложения // Просветительский проект «Лекториум» – 2020. – <https://www.lektorium.tv/node/36857> (дата обращения: 01.06.2022)

- Еханин Сергей. Локальное декодирование // Просветительский проект «Лекториум» – 2019. – <https://www.lektorium.tv/course/22879> (дата обращения: 01.06.2022)
- Шень Александр. Ликбез: коды, исправляющие ошибки // Просветительский проект «Лекториум» – 2020. – <https://www.lektorium.tv/node/31751> (дата обращения: 01.09.2020)
- Общероссийская Сеть КонсультантПлюс Справочная правовая система. <http://www.consultant.ru>

13. Перечень информационных технологий

- а) лицензионное и свободно распространяемое программное обеспечение:
 - Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);
 - публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).
- б) информационные справочные системы:
 - Электронный каталог Научной библиотеки ТГУ – <http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system>
 - Электронная библиотека (репозиторий) ТГУ – <http://vital.lib.tsu.ru/vital/access/manager/Index>
 - ЭБС Лань – <http://e.lanbook.com/>
 - ЭБС Консультант студента – <http://www.studentlibrary.ru/>
 - Образовательная платформа Юрайт – <https://urait.ru/>
 - ЭБС ZNANIUM.com – <https://znanium.com/>
 - ЭБС IPRbooks – <http://www.iprbookshop.ru/>

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа, оснащенные компьютером, проектором, экраном

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Пахомова Елена Григорьевна, доцент, кандидат физ.-мат. наук, доцент кафедры компьютерной безопасности ИПМКН ТГУ.