

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины
Теория кодирования, сжатия и восстановления информации

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

1. Цели освоения дисциплины

Целью освоения дисциплины «Теория кодирования сжатия и восстановления информации» является обеспечение фундаментальной подготовки в одной из основных областей современной прикладной математики, освоение языка и методов раздела математики, лежащего в основе большей части теории кодирования, передачи, защиты и хранения информации, имеющего применение во многих областях новейшей вычислительной техники, ознакомление с историей развития теории кодирования и вкладом в неё российских математиков.

Основная задача дисциплины – научить студентов пониманию языка конечной алгебры и теории информации, воспитанию культуры вычислений с помощью матричной алгебры, умениям применять аппарат линейной алгебры и теории групп в различных контекстах, в частности, в полях положительной характеристики, применению основных алгоритмов сжатия и восстановления информации

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части образовательной программы и является дисциплиной специализации. Имеет разносторонние связи со всеми специальными и основными математическими дисциплинами. Полученные при её изучении знания используются в различных специальных курсах, где она зачастую выступает в качестве основы курса. Основные математические дисциплины, связанные с указанной, таковы:

1. Теория кодирования и её связь с задачами защиты информации.
2. Быстрые вычисления.
3. Теория автоматов.
4. Алгебраические основы криптографии

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Профессионально-специализированные компетенции	
ПСК-2.2 Обладает способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знать: - основные алгебраические модели и конструкции. - основные методы и формулировки результатов, использующихся в защите информации Уметь: - применять программные средства для решения профессиональных задач - анализировать и обосновывать алгоритмы защиты информации Владеть: - навыками вычислений в основных алгебраических системах - навыками быстрых вычислений в основных алгебраических системах

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **6** зачетных единиц, **216** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1.	Вводная лекция	5	2	1				5	
2	Основная проблема теории кодирования	5	4	2				5	Проверка домашних заданий
3.	Дискретные каналы без памяти и передача информации	5	6	2				5	Контрольный опрос
4.	Линейные блочные коды	5	6	2		1		5	
5.	Циклические коды	5	4	2		1		5	
6.	Схемная реализация циклического кодирования	5	4	2		2		5	Проверка домашних заданий
7.	БЧХ-коды	5	6	4				5	
8.	Другие подходы к кодированию	5	4	3		1		5	
							0,3	8,7	Зачет
	Всего за 5 семестр 108 акад. часов		36	18		5	0,3	48,7	
9	Информация, энтропия и избыточность	6	2	1		1		1	
10	Кодирование для дискретных источников без памяти	6	4	2				2	
11	Энтропия связанных источников	6	4	2		1		2	
12	Стационарные дискретные источники с памятью	6	4	2				2	
13	Сжатие данных	6	6	3		1		2	
14	Арифметическое кодирование	6	8	4		1		2	Контрольная работа
15	Адаптивное арифметическое кодирование	6	8	4		1		2	
						2	0,5	33,5	экзамен
	Всего за 6 семестр 108 акад. час.		36	18		7	0,5	46,5	экзамен
	ИТОГО		72	36		12	0.8	95.2	

Содержание разделов дисциплины:

1. Вводная лекция.

Предмет и методы современной прикладной алгебры. Некоторые проблемы. Краткий исторический очерк. Место прикладной алгебры в системе математического знания и взаимодействие «чистой» и «прикладной» математики. Алгебра и алгоритмика.

2. Основная проблема теории кодирования.

Дискретный канал связи. История кодирования, контролирующего ошибки. Основные понятия теории кодов. Простейшие двоичные коды. Недвоичное кодирование.

3. Дискретные каналы без памяти и передача информации.

Передача информации по дискретному симметричному каналу. Пропускная способность канала. Пропускная способность двоичного симметричного канала со стираниями. Теорема кодирования Шеннона. Непрерывные источники и каналы.

4. Линейные блочные коды.

Структура линейных блочных кодов. Матричное описание линейных блочных кодов. Стандартное расположение. Коды Хэмминга. Совершенные и квазисовершенные коды. Простые преобразования линейного кода. Коды Рида – Маллера.

5. Циклические коды.

Код с точки зрения расширения поля. Полиномиальное описание циклических кодов. Матричное описание циклических кодов. Коды Хэмминга как циклические коды. Циклические коды, исправляющие две ошибки.

6. Схемная реализация циклического кодирования.

Логические цепи для арифметики конечного поля. Цифровые фильтры. Кодеры и декодеры на регистрах сдвига. Декодер Меггита. Вылавливание ошибок. Укороченные циклические коды. Декодер для кода Голея.

7. БЧХ-коды.

Определение БЧХ-кодов. Декодер Питерсона – Горенштейна –Цирлера. Коды Рида – Соломона. Декодирование двоичных БЧХ-кодов.

8. Другие подходы к кодированию.

Границы в теории кодов. Латинские квадраты и коды. Мажоритарное декодирование. Матрицы Адамара. Линейные рекуррентные последовательности и радар. Орбитные коды и коды на Евклидовой сфере. Понятие о квантовых кодах и квантовых вычислениях.

9. Информация, энтропия и избыточность.

Информация одного события. Энтропия и избыточность. Дискретный канал связи без памяти.

10. Кодирование для дискретных источников без памяти.

Теорема кодирования источников. Префиксные коды. Неравенства Крафта и Мак-Миллана.

11. Энтропия связанных источников.

Взаимная и условная информация. Совместная и условная энтропия.

12. Стационарные дискретные источники с памятью.

Теорема кодирования стационарного дискретного источника с памятью. Конечные цепи Маркова. Конечные дискретные марковские источники с заданной памятью. Энтропия стационарного марковского источника. Кодирование стационарных марковских источников.

13. Сжатие данных.

Методы сжатия данных. Алгоритм Шеннона-Фэно. Код Хаффмана.

14. Арифметическое кодирование.

Кодирование Лемпеля-Зива. Алгоритм LZ77. Алгоритм LZSS. Алгоритм LZ78. Алгоритм LZW

15. Адаптивное арифметическое кодирование.

Словарные методы сжатия информации. Алгоритм RLE

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Вернер М. Основы кодирования. - М: Техносфера, 2006
https://caxapa.ru/thumbs/409009/Osnovy_kodirovaniya_M_VERNER_.pdf
2. Березкин Е. Ф. Основы теории информации и кодирования: учебное пособие — Санкт-Петербург: Лань, 2018. <https://reader.lanbook.com/book/108326>
3. Л. С. Казарин, М. А. Заводчиков Введение в теорию кодирования, сжатия и восстановления информации: учебно-методическое пособие - Ярославль: ЯрГУ, 2020. <http://www.lib.uniyar.ac.ru/edocs/iuni/20200206.pdf>

б) дополнительная литература

1. М. В. Краснов Методы сжатия информации: текст и изображение: метод. указания -Ярославль, ЯрГУ, 2014. <http://www.lib.uniyar.ac.ru/edocs/iuni/20140407.pdf>
2. Сэломон Д., Сжатие данных, изображений и звука: учеб. пособие для вузов - М., Техносфера, 2006
<https://djvu.online/file/50qPL3MaR2wkG?ysclid=lkdx1be71q590256694>
3. Чечёта С. И., Введение в дискретную теорию информации и кодирования: учеб. пособие для вузов - М., Изд-во МЦНМО, 2011

в) ресурсы сети «Интернет»

1. [http:// www.tc26.ru](http://www.tc26.ru)
2. [http:// www.nist.gov/manuscript-publication-search.cfm?pub_id=919061](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=919061)
3. <http://habrahabr.ru/post/210684/>
4. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=919061
5. <https://streebog.info>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

зав. кафедрой алгебры и математической логики ЯрГУ,
д-ф.м.н, профессор

Казарин Л.С.

**Приложение №1 к рабочей программе
«Теория кодирования, сжатия и восстановления информации»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
используемые в процессе текущей аттестации**

Задание по теме Основная проблема теории кодирования.

По книге Вернер М. Основы кодирования.

По книге Березкин Е.Ф.. Основы теории кодирования

Задание по теме Информация, энтропия и избыточность.

По книге Вернер М.В. Основы кодирования, глава 2, глава 4.

По книге Березкин Е.Ф.. Основы теории кодирования, глава 1

Задание по теме Кодирование для дискретных источников без памяти.

По книге Вернер М.В. Основы кодирования, глава 3

По книге Березкин Е.Ф.. Основы теории кодирования, глава 4

Задание по теме Энтропия связанных источников.

По книге Вернер М.В. Основы кодирования, глава 4.

По книге Березкин Е.Ф.. Основы теории кодирования, глава 6

Задание по теме Стационарные дискретные источники с памятью.

По книге Вернер М.В. Основы кодирования, глава 5.

Краснов М.В. Методы сжатия изображений (методические указания). Раздел 2.

Задание по теме Сжатие данных.

По книге Вернер М.В. Основы кодирования, глава 6.

Краснов М.В. Методы сжатия изображений (методические указания). Раздел 2.

По книге Казарин Л.С. Глава 10

Задание по теме Дискретные каналы без памяти и передача информации.

По книге Вернер М.В. Основы кодирования, глава 7.

Краснов М.В. Методы сжатия изображений (методические указания). Раздел 3.

Задание по теме Линейные блочные коды.

По книге Вернер М. Основы кодирования.

По книге Березкин Е.Ф.. Основы теории кодирования, глава 10

По книге Казарин Л.С. Глава 5.

Задание по теме Циклические коды.

По книге Вернер М. Основы кодирования.

По книге Казарин Л.С. Глава 7.

Задание по теме . Схемная реализация циклического кодирования.

По книге Вернер М. Основы кодирования

По книге Березкин Е.Ф.. Основы теории кодирования, глава 10

Задание по теме БЧХ-коды.

По книге Вернер М. Основы кодирования

По книге Березкин Е.Ф.. Основы теории кодирования, глава 10

По книге Казарин Л.С. Глава 8.

Некоторые задания для зачетной работы

1. Сжать методом Хаффмана алфавит из 6 символов с вероятностями $1/10, 2/10, 3/10, 5/100, 5/100, 3/10$.
2. Закодировать сообщение «СТУДЕНТ МАТФАКА», используя алгоритмы LZ77, LZ78, LZSS и LZW. Вычислить длины в битах полученных кодов при ограничениях на размер словаря и величину буфера.
3. Сжать с помощью арифметического кодирования строку «Жираф – длинношеее животное».

Дан марковский источник первого порядка с графом состояний из двух связанных вершин А и В, причем переходные вероятности $p(A|A)=0.9$, $p(B|B)=0.7$, $p(B|A)=0.1$ и $p(A|B)=0.3$. Найти стационарное распределение вероятностей и энтропию источника.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Зачет выставляется по итогам текущей аттестации.

Контрольная работа

1. Вычислить таблицу характеров знакопеременной группы степени 5..
2. Найти формулы для свертки двух многочленов степени 5, используя дискретное преобразование Фурье в конечном поле (в зависимости от значений коэффициентов).
3. Верно ли, что любое точное двумерное представление конечной группы над \mathbb{C} неприводимо?
4. Пусть H – подгруппа группы G и β – ее регулярный характер. Доказать, что индуцированный характер β^G является ее регулярным характером.
5. Найти все неприводимые характеры группы, являющейся прямым произведением двух групп кватернионов порядка 8.

Вопросы к зачету

1. Методы сжатия изображений.
2. Неравенство Крафта и его использование.
3. Префиксные коды. Примеры.
4. Алгоритм Хаффмана сжатия изображений
5. Взаимная и условная информация.
6. Энтропия двоичного источника.
7. Пропускная способность двоичного симметричного канала.
8. Арифметическое кодирование.
9. Кодирование Лемпеля – Зива LZ77
10. Код Шеннона.
11. Сжатие изображений и факсов.
12. Преобразования Уолша и Адамара.
13. Дискретное косинусное преобразование.
14. Сжатие изображений с потерями.
15. Преобразование кода Грея в двоичный и обратно.

16. Дискретное преобразование Фурье.
17. Преобразование Фурье и свертка в суррогатном поле.

Вопросы к экзамену

1. Дискретный канал связи. Основная модель теории кодирования, контролирующего ошибки. Основные понятия теории кодов. Простейшие двоичные коды. Недвоичное кодирование.
2. Информация одного события. Энтропия и избыточность. Дискретный канал связи без памяти.
3. Теорема кодирования источников. Префиксные коды. Неравенства Крафта и Мак-Миллана.
4. Код Фэно. Коды Хаффмана.
5. Энтропия связанных источников. Взаимная и условная информация.
6. Совместная и условная энтропия. Примеры вычислений.
7. Теорема кодирования стационарного дискретного источника с памятью.
8. Конечные цепи Маркова. Конечные дискретные марковские источники с заданной памятью.
9. Энтропия стационарного марковского источника. Кодирование стационарных марковских источников.
10. Передача информации по дискретному симметричному каналу. Пропускная способность канала.
11. Пропускная способность двоичного симметричного канала со стираниями. Теорема кодирования Шеннона. Непрерывные источники и каналы.
12. Структура линейных блочных кодов. Матричное описание линейных блочных кодов.
13. Стандартное расположение. Коды Хэмминга. Совершенные и квазисовершенные коды.
14. Простые преобразования линейного кода. Коды Рида – Маллера.
15. Код с точки зрения расширения поля. Полиномиальное описание циклических кодов. Матричное описание циклических кодов.
16. Коды Хэмминга как циклические коды.
17. Циклические коды, исправляющие две ошибки.
18. Циклические коды, исправляющие пакеты ошибок. Двоичный код Голея.
19. Логические цепи для арифметики конечного поля. Цифровые фильтры. Кодеры и декодеры на регистрах сдвига.
20. Декодер Меггита. Вылавливание ошибок.
21. Укороченные циклические коды. Декодер для кода Голея.
22. Определение БЧХ-кодов. Декодер Питерсона – Горенштейна – Цирлера.
23. Коды Рида – Соломона.
24. Декодирование двоичных БЧХ-кодов.
25. Границы в теории кодов.
26. Латинские квадраты и коды. Мажоритарное декодирование.
27. Матрицы Адамара.
28. Линейные рекуррентные последовательности и радар.
29. Орбитные коды и коды на Евклидовой сфере.
30. Понятие о квантовых кодах и квантовых вычислениях

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объеме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;

- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка («зачтено», «незачтено»), которая определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция сформирована на высоком уровне. Оценка «хорошо» выставляется студенту, у которого сформированность компетенций находится на продвинутом уровне. Оценка «удовлетворительно» выставляется студенту, компетенции которого находятся на пороговом уровне. Оценка «неудовлетворительно» выставляется студенту, обнаружившему существенные пробелы в понимании материала и его изложения, грубые ошибки, незнание ключевых понятий.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Отмечу, что в настоящем учебном плане предусмотрен зачет в зимнюю сессию и экзамен в весеннюю сессию. Во втором семестре отдельные темы поручаются для изложения студентам с целью определения сформированности компетенции способности к самообразованию. Традиционно в апреле планируются выступления студентов на студенческой научной конференции с докладами по применению алгоритмов помехоустойчивого кодирования и сжатия изображений.

Приложение №2 к рабочей программе дисциплины «Теория кодирования, сжатия и восстановления информации»

Методические указания для студентов по освоению дисциплины

Для успешного усвоения данного курса необходимо знание следующих вопросов:

- линейные операторы в конечномерном векторном пространстве,
- матрица линейного оператора, ее запись в разных базисах
- характеристический многочлен линейного оператора.;
- кольцо и поле вычетов по модулю натурального числа;
- мультипликативная группа кольца вычетов;
- строение полей Гауа;
- понятие примитивного элемента поля Гауа;

Курс «Теория кодирования» отличается высокой степенью абстрактности применяемых методов, но в то же время, один из немногих курсов, позволяющих студентам составить представление о практическом применении абстрактных конструкций. Он насыщен весьма нетривиальными теоремами и, в то же время требует от слушателя высокой алгоритмической культуры. Поэтому возможно приглашение практических работников.