

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

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

20 мая 2025 г.

Рабочая программа дисциплины

Теория кодирования

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем (в сфере информационных технологий)»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 15.04.2025, протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 05.05.2025

1. Цели освоения дисциплины

Целями освоения дисциплины "Теория кодирования" являются: формирование математической культуры студента, фундаментальная подготовка по одному из основных разделов дискретной математики, овладение современным математическим аппаратом для дальнейшего использования при решении теоретических и прикладных задач.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы и является элективной дисциплиной. Для успешного изучения этой дисциплины необходимы знания и умения, приобретенные в результате освоения школьного курса математики, а также некоторых разделов из математического анализа и алгебры.

Теория кодирования относится к числу основных разделов современной прикладной математики. Знание основ теории кодирования является важной составляющей общей математической культуры выпускника. Эти знания необходимы как при проведении теоретических исследований в различных областях математики, так и при решении практических задач из разнообразных прикладных областей, таких как информатика, программирование, обработка и передача данных, криптография и др.

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)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Универсальные компетенции		
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	И-УК-1.5 Способен осуществлять анализ с позиций алгебраического подхода, формализацию задач и на этой основе вырабатывать стратегию действий	Знать: основные алгебраические модели и конструкции. Уметь: решать системы линейных уравнений Владеть навыками: вычислений в основных алгебраических системах
Общепрофессиональные компетенции		
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	И-ОПК-3.4 Способность разрабатывать и анализировать математические модели механизмов защиты информации	Знать: основные методы и формулировки результатов, использующихся в защите информации Уметь: обосновывать алгоритмы защиты информации Владеть навыками: быстрых вычислений в основных алгебраических системах

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетные единицы, **108** 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.	4	2	1				2	
2	Основные понятия теории кодов.	4	2	1				2	
3	Сжатие информации.	4	2	1				8	Задания для самостоятельной работы
4	Алгебраические конструкции.	4	2	1		1		8	Задания для самостоятельной работы
5	Основные матричные коды.	4	2	1		1		8	Задания для самостоятельной работы
6	Поля Галуа.	4	2	1		1		4	Контрольная работа 1
7	Циклические коды.	4	4	2		1		2	
8	Квадратично вычетные коды.	4	2	1				2	
9	Схемная реализация циклических кодов.	4	2	1		1		2	
10	БЧХ-коды.	4	4	2				2	
11	Границы возможного.	4	2	1				2	
12	Коды и обработка сигналов.	4	2	1				2	
13	Рекурренты и коды.	4	2	1		1		4	Контрольная работа 2
14	Квантовые коды.	4	2	1				2	
							0,3	3,7	зачет
	Всего		32	16		6	0,3	53,7	

Содержание разделов дисциплины:

1. Вводная лекция.

1.1. Предмет и методы современной прикладной алгебры. Взаимодействие «чистой» и «прикладной» математики. Некоторые модельные задачи.

2. Основные понятия теории кодов.

2.1. Дискретный канал связи. Основные понятия теории кодов.

2.2. Простейшие двоичные коды. Недвоичное кодирование. Расстояние Хэмминга и расстояние Ли

3. Сжатие информации.

3.1. Представление информации, сжатие и восстановление информации. Код Фано.

3.2. Префиксные коды. Неравенство Крафта.

3.3. Код Хаффмена. Методы сжатия информации..

4. Алгебраические конструкции.

4.1. Необходимые алгебраические конструкции. Группы, кольца, поля, линейные векторные пространства, линейные операторы, тензорное произведение пространств и Кронекеровское произведение матриц

5. Основные матричные коды.

5.1. Линейные блочные коды. Структура линейных кодов. Матричное описание. Стандартное расположение кода.

5.2. Коды Хэмминга. Совершенные и квазисовершенные коды. Простые преобразования линейного кода.

5.3. Коды Рида – Маллера.

6. Поля Галуа.

6.1. Арифметика полей Галуа. Кольцо целых чисел. Конечные поля. Кольца многочленов и поля, основанные на кольцах многочленов. Примитивные элементы. Строение конечного поля.

7. Циклические коды.

7.1. Циклические коды. Код с точки зрения расширения поля. Матричное описание циклических кодов.

7.2. Коды Хэмминга как циклические коды. Циклические коды, исправляющие пакеты ошибок.

8. Квадратично вычетные коды

8.1. Двоичный код Голея. Квадратично вычетные коды.

9. Схемная реализация циклических кодов.

9.1. Схемная реализация циклического кодирования. Логические цепи для арифметики конечного поля. Цифровые фильтры. Кодеры и декодеры на регистрах сдвига. Декодер Меггита. Вылавливание ошибок. Укороченные коды. Декодер для кода Голея.

10. БЧХ-коды

10.1. БЧХ – коды. Определение БЧХ-кодов. Декодер Питерсона – Горенштейна –Цирлера.

10.2. Коды Рида – Соломона.

10.3. Декодирование двоичных БЧХ-кодов.

11. Границы возможного.

11.1. Границы в теории кодирования. Граница Хэмминга, Граница Варшамова – Гильберта. Граница Плоткина.

11.2. Орбитные коды и коды на Евклидовой сфере.

12. Коды и обработка сигналов.

12.1. Латинские квадраты и коды. Мажоритарное декодирование.

12.2. Матрицы Адамара и преобразования Адамара – Уолша в обработке сигналов

13. Рекурренты и коды.

13.1. Линейные рекуррентные последовательности и разностные коды. Радар.

13.2. Псевдослучайные последовательности на регистрах сдвига.

13.3. Усложнение простых рекуррент.

14. Квантовые коды.

14.1. Понятие о квантовых кодах. Аналогии кодов Рида – Маллера для квантового канала. Некоторые хорошие коды. Связь с алгебро-геометрическим подходом

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 используется:

- 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» <https://www.studentlibrary.ru>

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: учебник для вузов. / М. Вернер; пер. с нем. ; ИППИ РАН - М.: Техносфера, 2004. - 286 с.
2. Белоногов В.А. Теория кодирования: учебное пособие. - Екатеринбург: УГТУ-УПИ, 2009.
3. Л. С. Казарин, М. А. Заводчиков Введение в теорию кодирования, сжатия и восстановления информации - Ярославль: ЯрГУ, 2020.
<http://www.lib.uniyar.ac.ru/edocs/iuni/20200206.pdf>

б) дополнительная литература

1. М. В. Краснов Методы сжатия информации - Ярославль, ЯрГУ, 2014.
<http://www.lib.uniyar.ac.ru/edocs/iuni/20140407.pdf>
2. Сэломон Д. Сжатие данных, изображений и звука, М.: Техносфера, 2006.
3. Березкин Е. Ф. Основы теории информации и кодирования: учебное пособие — Санкт-Петербург: Лань, 2018. <https://e.lanbook.com/book/108326>

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 и 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 в электронную информационно-образовательную среду организации.

Автор:

Зав. кафедрой алгебры и математической логики, профессор

Л. С. Казарин

**Приложение №1 к рабочей программе дисциплины
«Теория кодирования»**

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

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

Задания по теме №1 «Введение»

Раздел 1.1. Упражнения из пособия Белоногова В.А.

Задания по теме №2. Основные понятия теории кодов.

Раздел 2.1 Пособие Упражнения из пособия Белоногова В.А.

Раздел 2.2. Пособие Упражнения из пособия Белоногова В.А.

Задания по теме №3. Сжатие информации.

Разделы 3.1.- 3.3. Пособие Белоногова В.А., книга Вернера М.

Задания по теме №4. Алгебраические конструкции.

Раздел 4.1 Пособие Белоногова В.А., книга Вернера М.

Задания по теме №5. Основные матричные коды.

Разделы 5.1 – 5.3 Пособие Белоногова В.А., книга Вернера М.

Задания по теме №6. Поля Галуа.

Раздел 6.1 Пособие Белоногова В.А., книга Вернера М.

Задания по теме №7. Циклические коды.

Разделы 7.1. – 7.2. Пособие Белоногова В.А., книга Вернера М..

Задания по теме №8. Квадратично вычетные коды

Раздел 8.1. Пособие Белоногова В.А., книга Вернера М.

Задания по теме №9. Пособие Белоногова В.А., книга Вернера М.

Задания по теме №10. БЧХ-коды

Разделы 10.1.- 10.3 Пособие Белоногова В.А., книга Вернера М.

Задания по теме №11. Продвинутое алгоритмы кодирования

Разделы 11.1 – 11.3 Пособие Белоногова В.А., книга Вернера М.

Задания по теме №12. Границы возможного

Раздел 12.1. Пособие Белоногова В.А., книга Вернера М.

Задания по теме №13. Границы возможного

Разделы 13.1 -13.2. Пособие Белоногова В.А., книга Вернера М., пособие Казарина Л.С.

Задания по теме №14. Рекурренты и коды.

Разделы 14.1 Пособие Белоногова В.А.

Контрольная работа № 1 (один из вариантов)

1. Разложить двоичный многочлен на множители.
2. Дана проверочная матрица линейного кода. Найти кодирующую матрицу.
3. Существует ли квадратично-вычетный код длины 2011?

4. Найти порождающий многочлен кода Рида-Соломона, исправляющего 2 ошибки, основываясь на поле $GF(16)$.
5. Телеграмма на русском языке содержит не более 100 букв. Требуется построить код, исправляющий 5 ошибок
6. Найти порождающий многочлен $(63,55)$ -кода над $GF(8)$.
7. Пусть $(1, 1, 0, 1, 0, 1, 1)$ и $(1,1, 0,0, 1,1,1, 1)$ – искаженные слова расширенных (по-разному) кодов Хэмминга. Какое из этих слов содержит одиночную ошибку? Исправить.

Контрольная работа № 2 (один из вариантов)

1. Сколько существует неприводимых многочленов степени 4 над полем из 3 элементов?
2. Какова должна быть вероятность q ошибки при передаче по двоичному симметричному каналу блока из 8 символов, чтобы не менее половины из них была принята правильно с вероятностью не менее 0.99?
3. Для кода Рида – Маллера первого порядка исправить или обнаружить ошибки в заданных преподавателем словах.
4. Как определяются энтропия и избыточность языка?
5. Написать программу вычисления НОД двух многочленов над полем из 3 элементов..
6. Найти преобразование Фурье последовательности из 16 элементов в конечном поле.
7. Построить декодер для кода с перемежением, позволяющий исправлять все пакеты длины 2.

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

Вопросы к зачету

- Дискретный канал связи. Основная модель теории кодирования, контролирующего ошибки. Основные понятия теории кодов. Простейшие двоичные коды. Недвоичное кодирование.
- Информация одного события. Энтропия и избыточность. Дискретный канал связи без памяти.
- Теорема кодирования источников. Префиксные коды. Неравенства Крафта и Мак-Миллана.
- Код Фано. Коды Хаффмана.
- Энтропия связанных источников. Взаимная и условная информация.
- Совместная и условная энтропия. Примеры вычислений.
- Теорема кодирования стационарного дискретного источника с памятью.
- Энтропия стационарного марковского источника. Кодирование стационарных марковских источников.
- Передача информации по дискретному симметричному каналу. Пропускная способность канала.
- Пропускная способность двоичного симметричного канала со стираниями. Теорема кодирования Шеннона. Непрерывные источники и каналы.
- Структура линейных блочных кодов. Матричное описание линейных блочных кодов.
- Стандартное расположение. Коды Хэмминга. Совершенные и квазисовершенные коды.
- Простые преобразования линейного кода. Коды Рида – Маллера.
- Код с точки зрения расширения поля. Полиномиальное описание циклических кодов. Матричное описание циклических кодов.
- Коды Хэмминга как циклические коды.

- Циклические коды, исправляющие две ошибки.
- Циклические коды, исправляющие пакеты ошибок. Двоичный код Голея.
- 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.
- Определение БЧХ-кодов. Декодер Питерсона – Горенштейна –Цирлера.
- Коды Рида – Соломона.
- Декодирование двоичных БЧХ-кодов.
- 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

Некоторые дополнительные задания для зачета

- 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».
- 4 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.
- 5 Написать схему декодера, для кода, исправляющего 2 ошибки.
- 6 Предложить схему рекуррентной последовательности, имеющей период не менее 1000.

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»

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 объёме 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.

Описание процедуры выставления оценки

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.

Приложение №2 к рабочей программе дисциплины «Теория кодирования»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Теория кодирования» являются лекции и практические занятия, причем в достаточно большом объеме. Это связано с тем, что теория кодирования представляет собой особый математический аппарат, важную роль в котором играет алгебра, с помощью которого математика решает довольно сложные и нетривиальные задачи. По всем темам предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с математическим аппаратом теории кодирования и сжатия информации.

Особенность дисциплины состоит в ее существенно более абстрактный характер по сравнению с другими дисциплинами и явно выраженный прикладной аспект. Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. В течение всего обучения на лекциях предлагаются нестандартные задачи, решая которые студент может повысить свой уровень освоения теоретического материала. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы теории. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с аппаратом алгебры в течение обучения проводятся мероприятия текущей аттестации в виде 2 контрольных и 2 самостоятельных работ. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце изучения дисциплины студенты сдают зачет. Оценка выставляется по итогам тестирования и краткого собеседования по его результатам.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Теория кодирования» самостоятельно студенту крайне сложно. Это связано со сложностью и абстрактностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым. Без упорных и регулярных занятий в течение семестра сдать зачет по итогам изучения дисциплины в каждом семестре студенту практически невозможно.