

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**  
**Директор Высшей школы**  
**современной математики**  
**А.Н. Соболевский**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Теория кодирования
<b>по направлению:</b>	Математика
<b>профиль подготовки:</b>	Фундаментальная математика
	Высшая школа современной математики
	Высшая школа современной математики
<b>курс:</b>	3
<b>квалификация:</b>	бакалавр

Семестр, формы промежуточной аттестации: 5 (осенний) - Зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 42 час.

Всего часов: 72, всего зач. ед.: 2

Программу составил: М.А. Цфасман, д-р физ.-мат. наук

Программа обсуждена на заседании Высшая школа современной математики 02.09.2024

## Аннотация

В курсе излагаются в основном вопросы алгебраической теории кодирования: способам использования комбинаторных и алгебраических структур для построения схем кодирования информации, обеспечивающих устойчивость к ошибкам. Основным рассматриваемый тип ошибок — ошибки замещения с детерминированным ограничением, однако рассмотрены и некоторые другие модели и задачи. В частности, теоремы Шеннона об энтропийной оценке пропускной способности вероятностного канала связи, теорема Хафмана, коды Варшавова—Тененгольца для исправления ошибок вставки/выпадения, а также ошибки синхронизации.

### 1. Цели и задачи

#### Цель дисциплины

Формирование базовых знаний о теории помехоустойчивого кодирования.

#### Задачи дисциплины

- приобретение слушателями теоретических знаний и практических умений и навыков в области теории кодирования;
- подготовка слушателей к изучению смежных математических дисциплин.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях
ПК-3 Способен проверять корректность математического доказательства, строить логически последовательные цепочки рассуждений	ПК-3.1 Способен к формальной записи рассуждения в терминах логики предикатов
	ПК-3.2 Владеет понятием о математически строгом доказательстве, способен различать строгие и нестрогие рассуждения
	ПК-3.3 Способен выявлять использованные при доказательстве предположения и предпосылки, в том числе неявные, и контролировать их корректность

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

Основные понятия и результаты теории помехоустойчивого кодирования.

уметь:

Разбирать конкретные примеры и проводить необходимые вычисления.

владеть:

Свободно владеть техническим инструментарием, необходимым для самостоятельного анализа кодов.

#### 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

##### 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Алфавитное кодирование.	6			8
2	Коды БЧХ.	6			8
3	Линейные коды.	6			8
4	Сверточные коды.	6			8
5	Сложность задачи декодирования линейных кодов.	6			10
Итого часов		30			42
Подготовка к экзамену		0 час.			
Общая трудоёмкость		72 час., 2 зач.ед.			

##### 4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 5 (Осенний)

###### 1. Алфавитное кодирование.

Достаточные условия однозначности декодирования: равномерность, префиксность, суффиксность.

Распознавание однозначности: критерий Маркова.

Оценка длины неоднозначно декодируемого слова.

###### 2. Коды БЧХ.

Задача восстановления синхронизации.

Восстановление синхронизации для смежных классов циклических кодов.

###### 3. Линейные коды.

Определения.

Порождающая и проверочная матрицы.

Связь кодового расстояния с проверочной матрицей.

Граница Варшавова—Гилберта.

Систематическое кодирование.

Декодирование по синдрому.

Коды Хемминга.

#### 4. Сверточные коды.

Матрицы Адамара.

Конструкции Сильвестра и Пэли.

Коды на основе матриц Адамара.

#### 5. Сложность задачи декодирования линейных кодов.

Графы-расширители.

Вероятностное доказательство существования расширителей.

Коды на основе двудольных графов.

Кодовое расстояние кодов на основе расширителей.

Алгоритм декодирования Сипсера—Шпильмана.

### **5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Учебная аудитория, оснащенная мультимедиа проектором, экраном и микрофоном.

### **6. Перечень рекомендуемой литературы**

#### Основная литература

1. Заметки по теории кодирования [Текст] / А. Е. Ромащенко, А. Ю. Румянцев, А. Шен .— [Учебное изд.] .— М : МЦНМО, 2011 .— 80 с.
2. Введение в алгебраические коды [Текст] : учеб. пособие для вузов / Ю. Л. Сагалович ; М-во образования и науки Рос. Федерации, Моск. физ.-техн. ин-т (гос. ун-т), Ин-т проблем передачи информации им. А. А. Харкевича РАН .— М. : Изд-во МФТИ, 2007 .— 262 с.
3. Основы кодирования [Текст] / М. Вернер ; пер. с немец. Д. К. Зигангирова - М. Техносфера, 2004, 2006

#### Дополнительная литература

1. Дискретный анализ. Основы высшей алгебры [Текст] : учеб. пособие для вузов / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый ; М-во образования и науки Рос. Федерации, Моск. физ.-техн. ин-т (гос. ун-т) .— 2-е изд., испр. и доп. — М. : МЗ Пресс, 2007 .— 224 с.

### **7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

Не используются

### **8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)**

На лекционных и практических (семинарских) занятиях могут использоваться мультимедийные технологии, включая демонстрацию презентаций, а также технологии дистанционной аудиовидеоконференцсвязи.

### **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Методические указания приводятся в разрабатываемых аудиторных и домашних раздаточных материалах (листочках).

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**по направлению:** Математика  
**профиль подготовки:** Фундаментальная математика  
Высшая школа современной математики  
Высшая школа современной математики  
**курс:** 3  
**квалификация:** бакалавр

Семестр, формы промежуточной аттестации: 5 (осенний) - Зачет

**Разработчик:** М.А. Цфасман, д-р физ.-мат. наук

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации
	ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива
	ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях
ПК-3 Способен проверять корректность математического доказательства, строить логически последовательные цепочки рассуждений	ПК-3.1 Способен к формальной записи рассуждения в терминах логики предикатов
	ПК-3.2 Владеет понятием о математически строгом доказательстве, способен различать строгие и нестрогие рассуждения
	ПК-3.3 Способен выявлять использованные при доказательстве предположения и предпосылки, в том числе неявные, и контролировать их корректность

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Теория кодирования» обучающийся должен:

### знать:

Основные понятия и результаты теории помехоустойчивого кодирования.

### уметь:

Разбирать конкретные примеры и проводить необходимые вычисления.

### владеть:

Свободно владеть техническим инструментарием, необходимым для самостоятельного анализа кодов.

## 3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по материалу предыдущего занятия.

## 4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Алфавитное кодирование. Свойства однозначно декодируемых кодов.
2. Распознавание однозначности. Оценка длины неоднозначно декодируемого слова. Префиксные коды. Неравенство Крафта—Макмиллана.

3. Существование префиксного кода с заданным набором длин слов. Коды с мини-мальной избыточностью. Теорема Хаффмана о редукции.
4. Задача исправления и обнаружения ошибок. Типы ошибок.
5. Коды Варшавова—Тененгольца, алгоритмы исправления одиночных ошибок выпадения и вставки символов. Графовая модель канала.
6. Шенноновское произведение графов, шенноновская ёмкость. Теорема о верхней оценке шенноновской ёмкости.
7. Симметричный канал с ошибками замещения.
8. Расстояние Хемминга. Кодовое расстояние.
9. Основные задачи теории кодов, исправляющих ошибки. Границы для параметров кодов, исправляющих ошибки: границы сферической упаковки, Синглтона, Плоткина. Вложение метрических пространств.
10. Лемма о числе векторов в евклидовом пространстве. Граница Элайеса—Бассалыго.
11. Линейные коды. Определения. Порождающая и проверочная матрицы. Связь кодового расстояния с проверочной матрицей. Систематическое кодирование.
12. Декодирование по синдрому. Коды Хемминга. Граница Варшавова—Гилберта. Остаточный код, граница Грайсмера—Соломона—Штиффлера.
13. Теорема Шеннона о пропускной способности симметричного двоичного канала (вторая часть — без доказательства).
14. Асимптотические параметры семейств кодов.
15. Сложность задачи декодирования линейных кодов: задача NCP. Графы-расширители. Вероятностное доказательство существования расширителей.
16. Коды на основе двудольных графов. Кодовое расстояние кодов на основе расширителей. Алгоритм декодирования Сипсера—Шпильмана.
17. Коды Рида—Соломона. Алгоритм декодирования Берлекэмпа—Велча. Коды Рида—Маллера: кодовое расстояние, алгоритм мажоритарного декодирования.
18. Лемма Липтона—ДеМилло—Шварца—Зиппеля. Понятие об алгеброгеометрических кодах.
19. Циклические коды. Проверочный и порождающий многочлены, критерий существования кода с заданным порождающим многочленом.
20. Вид порождающей и проверочной матриц. Систематическое кодирование. Граница Боуза—Чоудхури—Хоквингема.
21. Коды БЧХ. Задача восстановления синхронизации. Восстановление синхронизации для смежных классов циклических кодов.
22. Совершенные коды. Теорема Васильева.
23. Каскадные коды. Коды Форни.
24. Свёрточные коды.
25. Коды Адамара. Понятие о локальном декодировании.
26. Понятие о списочном декодировании. Граница Джонсона.
27. Некоторые приложения теоретико-кодовых результатов и подходов в теоретической информатике и инженерии.
28. Хранение данных на CD, криптографическая система МакЭлиса, схема разделения секрета Шамира, коммуникационная сложность, дерандомизация, пороговые структуры данных.

#### Критерии оценивания

Оценка "зачтено" выставляется студентам, способным ясно и полно излагать теоретическое содержание, отвечать на дополнительные вопросы и самостоятельно разбирать конкретные примеры и проводить вычисления.

Оценка "не зачтено" выставляется студентам, у которых в результате опроса выявлены существенные пробелы в освоении материала курса или которые не способны решать упражнения на применение представленных в курсе понятий.

#### 5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Зачет проводится по итогам текущей успеваемости и сдачи заданий, предусмотренных программой дисциплины.

Во время проведения зачета обучающимся запрещается пользоваться помощью других лиц и мобильными телефонами, разрешается пользоваться программой учебной дисциплины и справочной литературой по выбору экзаменатора.