

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«**Российский государственный гуманитарный университет**»  
(ФГБОУ ВО «РГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
Факультет информационных систем и безопасности  
Кафедра фундаментальной и прикладной математики

## **ТЕОРИЯ КОДИРОВАНИЯ**

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

---

01.03.04 Прикладная математика

*Код и наименование направления подготовки/специальности*

---

Математика информационных сред

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *Бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2024

*ТЕОРИЯ КОДИРОВАНИЯ*

Рабочая программа дисциплины

Составители:

доктор физико-математических наук, профессор *В.М. Максимов*

УТВЕРЖДЕНО

Протокол заседания кафедры  
фундаментальной и прикладной математики  
№ 8 от 20.03.2024

## ОГЛАВЛЕНИЕ

Рабочая программа дисциплины.....	2
1. Пояснительная записка.....	4
1.1. Цель и задачи дисциплины.....	4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций.....	4
1.3. Место дисциплины в структуре образовательной программы.....	4
2. Структура дисциплины.....	4
3. Содержание дисциплины.....	5
4. Образовательные технологии.....	6
5. Оценка планируемых результатов обучения.....	6
5.1 Система оценивания.....	6
5.2 Критерии выставления оценки по дисциплине.....	6
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.....	7
6. Учебно-методическое и информационное обеспечение дисциплины.....	9
6.1 Список источников и литературы.....	9
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».....	10
6.3 Профессиональные базы данных и информационно-справочные системы.....	10
7. Материально-техническое обеспечение дисциплины.....	10
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов.....	10
9. Методические материалы.....	11
9.1 Планы практических занятий.....	11
9.2 Методические рекомендации по подготовке письменных работ.....	13
Приложение 1. Аннотация рабочей программы дисциплины.....	14

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

*Цель дисциплины:* изучение класса  $p$ -адическозначных функций, специальных классов  $T$ -функций, понятие о непрерывности и дифференцируемости, разложение в ряды и на этой основе изучение свойств криптокритериев.

*Задачи дисциплины:* ознакомление с различными направлениями и методологией анализа  $p$ -адических функций, активно развивающегося направления математики; обучение студентов теории и практике применения методов этого анализа к математическим объектам и возможных приложений в различных областях экономики и управления, психологии, физики и др.

### 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Коды компетенций	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ПК-2. Способен выделять, формулировать возникающие в результате самостоятельной научной деятельности или деятельности научных, производственных, административных учреждений задачи или подзадачи для решения текущих проблем	ПК-2.1. Владеет навыками работы с информационными системами	Знать: основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования; Уметь: использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования; Владеть: дисциплинами естественных наук в профессиональной деятельности, применять методы математического и анализа, и моделирования, теоретического и экспериментального исследования.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Теория кодирования» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: Общая алгебра и теория чисел.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения практик: Производственная практика (Проектно-технологическая практика), Производственная практика (Научно-исследовательская работа).

## 2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа.

### Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
8	Лекции	24
8	Практические занятия	32
Всего:		56

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 88 академических часов.

### 3. Содержание дисциплины

**Тема 1.** Конечные поля, их построение и основные свойства. Конечные поля, их построение и основные свойства. Поле Галуа.

**Тема 2.** Математические аспекты проблем передачи информации, вопрос о построения и кодов, исправляющих ошибки. Процедуры кодирования и декодирования. Теорема Шеннона о существовании хороших кодов.

Математические аспекты проблем передачи информации, вопрос о построения кодов, исправляющих ошибки. Процедуры кодирования и декодирования. Теорема Шеннона о существовании хороших кодов.

**Тема 3.** Линейные коды и их параметры. Спектры и двойственность. Двоичные коды Хэмминга.

Линейные коды и их параметры: Линейные коды. Кодирование и декодирование. линейных кодов. Общие свойства Спектры и двойственность. Двоичные коды Хэмминга Теорема о связи проверочной и порождающей матриц. Теорема Глаголева. Границы объема кода: граница Синглтона, граница Хэмминга, граница аршамова-Гилберта, граница Плоткина.

**Тема 4.** Коды Рида-Соломона. БЧХ-коды и рациональные коды Гоппы

Коды Рида-Соломона. БЧХ-коды и рациональные коды Гоппы. Циклические коды. Кольцо многочленов над полем Галуа. Определение циклического кода. Теорема о необходимом и достаточном условии существования циклического кода с порождающим многочленом  $g(x)$ . Кодирование и декодирование циклических кодов. Примеры циклических кодов: коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона, коды Юстесена, коды Гоппы.

**Тема 5.** Циклические и квадратично-вычетные коды. Конструкции новых кодов из уже известных.

Циклические и квадратично-вычетные коды. Конструкции новых кодов из уже известных. Теорема о существовании совершенных кодов. Коды Хемминга над  $GF(q)$ , способы задания, кодирование, декодирование, единственность. Коды Васильева. Оценки числа совершенных кодов. Коды Рида-Маллера.

**Тема 6.** Асимптотически длинные коды, границы для их параметров. Асимптотически длинные коды, границы для их параметров.

**Тема 7.** Построение асимптотически хороших кодов. Открытые проблемы.

Построение асимптотически хороших кодов. Открытые проблемы. Разделимые и префиксные коды. Стоимость кодирования. Неравенство Крафта-Макмиллана. Оптимальное кодирование. Метод Хаффмена. Метод Фано. Энтропия. Метод Шеннона для бернуллиевских источников. Теорема Шеннона для бернуллиевских источников. Критерий разделимости побуквенного кодирования. Теоремы Маркова. Алгоритм распознавания разделимости. Универсальное кодирование, теорема Фитингофа.

#### 4. Образовательные технологии

Для проведения *занятий лекционного типа* по дисциплине применяются такие образовательные технологии как лекция-визуализация с применением слайд-проектора, проблемная лекция. Для проведения *практических занятий* используются такие образовательные технологии как: решение типовых задач для закрепления и формирования знаний, умений, навыков. В рамках *самостоятельной работы* студентов проводится консультирование и проверка домашних заданий посредством электронной почты.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

#### 5. Оценка планируемых результатов обучения

##### 5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
Опрос	5 баллов	20 баллов
Доклады, рефераты	5 баллов	15 баллов
Контрольная работа	25 баллов	25 баллов
Промежуточная аттестация - экзамен (Экзамен по билетам)		40 баллов
<b>Итого за семестр</b>		<b>100 баллов</b>

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	Отлично	зачтено	A
83 – 94			B
68 – 82	Хорошо		C
56 – 67	Удовлетворительно		D
50 – 55			E
20 – 49	Неудовлетворительно	не зачтено	FX
0 – 19			F

##### 5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	отлично	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	хорошо	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	удовлетворительно	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	неудовлетворительно	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

### 5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

#### Текущий контроль

#### *Примерная тематика рефератов, докладов:*

1. Задача о назначениях: постановка, анализ и решение задачи с точки зрения: теории графов, методов оптимальных решений, теории кодирования.

2. Теория групп как необходимый аппарат в теории кодирования. Базовые представления, группы подстановок.
3. Сходство и различие кодов Хемминга и кодов Рида-Соломона.
4. Вклад Шеннона в развитие теории информации.
5. Математические исследования в теории информации.

**Примерные теоретические вопросы для контрольной работы:**

1. Геометрические свойства кодов, исправляющих ошибки, и другие подобного типа проблемы.
2. Построение сверхстойких кодов.
3. Перечислить параметры линейных кодов.
4. Указать границы для параметров асимптотически длинных кодов.
5. Указать процедуры кодирования и декодирования.
6. Привести пример кода, исправляющего ошибки.

**Примерные задания для контрольной работы:**

**Вариант 1.**

1. Построить коды с помощью проверочных матриц.

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

2. Пусть в канале связи используется код Хемминга длины 7, столбцы проверочной матрицы которого лексикографически упорядочены. Пусть на приемном конце получено слово (0 1 1 0 1 1 0). Декодировать его и найти информационный блок.

3. Для линейного кода, заданного порождающей матрицей  $H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

построить таблицу стандартного расположения. Декодировать слово (1 1 0 1 1 1) по таблице стандартного расположения и слово (1 0 1 0 1 1) с помощью синдрома.

4. Построить таблицу синдромов для расширенного кода Хемминга длины 8.

**Вариант 2.**

1. Построить коды Фано и Хаффмена найти стоимости кодирований для источников Бернулли с вероятностями букв:

- а)  $P = \{0.5; 0.2; 0.1; 0.09; 0.08; 0.03\}$ ,
- б)  $P = \{0.4; 0.2; 0.1; 0.1; 0.1; 0.1\}$ ,
- в)  $P = \{0.4; 0.3; 0.1; 0.07; 0.06; 0.04; 0.03\}$ .

2. Для заданного  $q$  указать набор вероятностей  $P$ , при котором существует  $q$ -значный префиксный код с заданным набором длин кодовых слов  $L$ , являющийся оптимальным. Построить этот код.

- а)  $q = 2, L = \{1, 2, 4, 4, 5, 5\}$ ,
- б)  $q = 2, L = \{2, 2, 2, 3, 3\}$ .

3. Построить код Шеннона для источников Бернулли с вероятностями букв:

- а)  $P = \{0.6; 0.1; 0.09; 0.08; 0.07; 0.06\}$ ,



б)  $P = \{0.4; 0.4; 0.1; 0.03; 0.03; 0.2; 0.2\}$ ,

в)  $P = \{0.34; 0.18; 0.17; 0.16; 0.15\}$ .

Найти стоимости кодирований.

4. Пусть дан монотонный источник  $A = \{a, b, c, d\}$ . Передать слово  $w$  с помощью кода «стопка книг». Декодировать полученное слово.

а)  $w = cbbaccddbb$ ;

б)  $w = ccabbaacc$ .

5. Найти код сообщения  $w$  с помощью метода Лемпела - Зива LZ78

а)  $w = babaabababaaabab$ ;

б)  $w = aaababaabaaabab$ .

## Промежуточная аттестация (экзамен)

### Контрольные вопросы по курсу:

1. Конечные поля, их построение и основные свойства
2. Математические аспекты проблем передачи информации, вопрос о построения и кодов, исправляющих ошибки.
3. Процедуры кодирования и декодирования.
4. Теорема Шеннона о существовании хороших кодов
5. Линейные коды и их параметры.
6. Спектры и двойственность. Двоичные коды Хэмминга.
7. Коды Рида-Соломона.
8. БЧХ-коды и рациональные коды Гоппы
9. Циклические и квадратично-вычетные коды.
10. Конструкции новых кодов из уже известных.
11. Асимптотически длинные коды, границы для их параметров.
12. Построение асимптотически хороших кодов.
13. Открытые проблемы.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Список источников и литературы

#### Литература

##### Основная

1. Гашков С.Б. Криптографические методы защиты информации : учеб. пособие для студентов вузов/ С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - М.: Академия, 2010. - 297 с.
2. Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).
3. Введение в криптографию / [В. В. Яценко и др.]; под ред. В. В. Яценко. - Изд. 4-е, доп. - М.: МЦНМО, 2012. - 347 с.
4. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536902> .
5. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536733> .

6. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537383> .

#### *Дополнительная*

1.Шептунов М.В. Дискретная математика для бакалавриата: учебное пособие для использования в учебном процессе образовательных организаций, реализующих программы высшего образования по направлениям подготовки 10.03.01 - "Информационная безопасность" 09.03.03 - "Прикладная информатика", 38.03.05 - "Бизнес-информатика" (уровень бакалавриата) / М. В. Шептунов. - Москва: Горячая линия-Телеком, 2017. - 114 с.

### **6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».**

1.Интернет- библиотека: <http://ilib.mccme.ru>

2.Прикладная математика. Справочник математических формул: <http://www.pm298.ru>

Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)

ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)

### **6.3 Профессиональные базы данных и информационно-справочные системы**

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

## **7. Материально-техническое обеспечение дисциплины**

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

## **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости

предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA SE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1 Планы практических занятий**

#### **Тема 1. Конечные поля, их построение и основные свойства.**

*Задания:*

Пример 2.3, гл. 2, упр.2.1,2.3, 3.7, пр. 7.1, 7.2, 7.3 из книги:

Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300

"Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел.

## **Тема 2. Математические аспекты проблем передачи информации.**

*Задания:*

Пример 2.2, 2.4, 2.6 из книги:

Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также теории информации.

## **Тема 3. Линейные коды.**

*Задания:*

Примеры 3.1, 3.2, пр.8.1 из книги:

Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).

Пример 4.4 из книги:

Шептунов М.В. Дискретная математика для бакалавриата: учебное пособие для использования в учебном процессе образовательных организаций, реализующих программы высшего образования по направлениям подготовки 10.03.01 - "Информационная безопасность" 09.03.03 - "Прикладная информатика", 38.03.05 - "Бизнес-информатика" (уровень бакалавриата) / М. В. Шептунов. - Москва: Горячая линия-Телеком, 2017. - 114 с.

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также лекций.

## **Тема 4. Коды Рида-Соломона. БЧХ-коды и рациональные коды Гоппы.**

*Задания:*

Задачи 4.2, 4.3, 4.4 из книги:

Шептунов М.В. Дискретная математика для бакалавриата: учебное пособие для использования в учебном процессе образовательных организаций, реализующих программы высшего образования по направлениям подготовки 10.03.01 - "Информационная безопасность" 09.03.03 - "Прикладная информатика", 38.03.05 - "Бизнес-информатика" (уровень бакалавриата) / М. В. Шептунов. - Москва: Горячая линия-Телеком, 2017. - 114 с.

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также лекций.

## **Тема 5. Циклические и квадратично-вычетные коды. Конструкции новых кодов из уже известных.**

*Задания:*

Пример 4.2. из книги:

Шептунов М.В. Дискретная математика для бакалавриата: учебное пособие для использования в учебном процессе образовательных организаций, реализующих программы высшего образования по направлениям подготовки 10.03.01 - "Информационная безопасность" 09.03.03 - "Прикладная информатика", 38.03.05 - "Бизнес-информатика" (уровень бакалавриата) / М. В. Шептунов. - Москва: Горячая линия-Телеком, 2017. - 114 с.

Примеры 6.1, 6.2, 6.4 из книги:

Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также лекций.

#### **Тема 6. Асимптотически длинные коды.**

*Задания:*

Примеры 6.1, 6.4 из книги:

Применко Э. А. Алгебраические основы криптографии : учеб. пособие для студентов вузов, обучающихся по направлениям ВПО 010400 "Прикладная математика и информатика" и 010300 "Фундаментальная информатика и информ. технологии" / Э. А. Применко. - М.: URSS: Либроком, 2013. - 283 с. - (Основы защиты информации).

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также лекций.

#### **Тема 7. Построение асимптотически хороших кодов. Открытые проблемы.**

*Задания:*

Примеры 4.2, 4.4 из книги:

Шептунов М.В. Дискретная математика для бакалавриата: учебное пособие для использования в учебном процессе образовательных организаций, реализующих программы высшего образования по направлениям подготовки 10.03.01 - "Информационная безопасность" 09.03.03 - "Прикладная информатика", 38.03.05 - "Бизнес-информатика" (уровень бакалавриата) / М. В. Шептунов. - Москва: Горячая линия-Телеком, 2017. - 114 с.

*Указания по выполнению задания:* вспомнить соответствующие вопросы из общей алгебры и теории чисел, а также лекций.

### **9.2 Методические рекомендации по подготовке письменных работ**

***Требования к подготовке и содержанию письменных работ (реферата, доклада):***

1. Соответствие содержания теме и плану работы.
2. Полнота и глубина раскрытия основных понятий проблемы.
3. Достаточность фактов, позволяющих проиллюстрировать актуальность избранной проблемы, способы ее решения.
4. Работа с литературой, систематизация и структурирование материала.
5. Обобщение и сопоставление различных точек зрения по рассматриваемому вопросу.
6. Наличие и четкость выводов, резюме.

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.

Цель дисциплины: изучение класса  $p$ -адическозначных функций, специальных классов  $T$ -функций, понятие о непрерывности и дифференцируемости, разложение в ряды и на этой основе изучение свойств криптокритериев.

Задачи дисциплины: ознакомление с различными направлениями и методологией анализа  $p$ -адических функций, активно развивающегося направления математики; обучение студентов теории и практике применения методов этого анализа к математическим объектам и возможных приложений в различных областях экономики и управления, психологии, физики и др.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен выделять, формулировать возникающие в результате самостоятельной научной деятельности или деятельности научных, производственных, административных учреждений задачи или подзадачи для решения текущих проблем.

В результате освоения дисциплины обучающийся должен:

Знать: основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования;

Уметь: использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования;

Владеть: дисциплинами естественных наук в профессиональной деятельности, применять методы математического анализа, и моделирования, теоретического и экспериментального исследования.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

**ЛИСТ ИЗМЕНЕНИЙ<sup>1</sup>**

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола

---

<sup>1</sup> Для ОП ВО магистратуры изменения только за 2020 г.