МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

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

ЭЛЕМЕНТЫ Р-АДИЧЕСКОГО АНАЛИЗА И ЕГО ПРИЛОЖЕНИЯ К КРИПТОГРАФИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Прикладная математика

Уровень квалификации выпускника - бакалавр

Форма обучения - очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

ЭЛЕМЕНТЫ Р-АДИЧЕСКОГО АНАЛИЗА И ЕГО ПРИЛОЖЕНИЯ К КРИПТОГРАФИИ
Рабочая программа дисциплины

Составители:
Д. пед. н., профессор, зав. кафедрой фундаментальной и прикладной математики
В.К. Жаров
Д. ф.-м. н., профессор, профессор кафедры фундаментальной и прикладной математики
В.М. Максимов

УТВЕРЖДЕНО
Протокол заседания кафедры
фундаментальной и прикладной математики
№ 14 от 20.06.2017

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: изучение класса р-адическозначных функций, специальных классам Т-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 р-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. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Коды компе-тенций	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ПК-10	готовность применять математический аппарат для решения поставленных задач, способность применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов	*Знать:* о применении конечных полей в моделировании; *Уметь*: применять полученные знания в решении задач организации математических моделей; *Владеть:* достаточными представлениями о типах моделей, о способах реализации современными методами в компьютерных системах

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Элементы р-адического анализа и его приложения к криптографии» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин (модулей): «Общая алгебра и теория чисел», «Математический анализ».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Теория кодирования».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 42ч., промежуточная аттестация 18ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная		Промежуточная аттестация	Самостоятельная работа	
			Лекции	Практические занятия			
1	Конечные поля: основные понятия	8	2	4		8	

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная		Промежуточная аттестация	Самостоятельная работа	
			Лекции	Практические занятия			
2	Поле p-адических чисел	8	4	4		8	Расчетно-графическая работа (РГР)
3	Алгебраические свойства целых p-адических чисел	8	4	4		8	Опрос. Контрольная работа
4	Топология пространства	8	2	4		8	Доклады
5	Введение в математический анализ	8	4	4		8	Защита расчетно-графической работы (РГР)
6	p-адические функции и их применение в теории кодирования	8	2	4		8	Доклады
7	**Экзамен**	8			18		Экзамен по билетам
	Итого:		**18**	**24**	**18**	**48**	

3. Содержание дисциплины

Тема 1. **Конечные поля: основные понятия**
Понятие пополнения. Нормированные поля. Построение пополнения нормированного поля. Нормирования поля рациональных чисел. Нормирование алгебраических расширений.

Тема 2. Поле p-адических чисел
Арифметические операции в поле. p-адические разложения рациональных чисел. Лемма Гензеля.

Тема 3. Алгебраические свойства целых p-адических чисел
Нормирование алгебраических полей: общий случай. Нормирование полей алгебраических чисел. Теорема Островского.

Тема 4. Топология пространства
Основные топологические свойства. Канторово множество.

Тема 5. Введение в математический анализ
Последовательности и ряды. p-адические степенные ряды. Некоторые p-адические элементарные функции. Разложение в ряд по p–адическим экспонентам, и логарифмам.

Тема 6. p-адические функции и их применение в теории кодирования
Локально постоянные функции. Непрерывные и равномерно непрерывные функции. Дифференцируемость p-адический функций. p-адическое интерполирование. Пример p-адического кода.

4. Образовательные технологии

№	Наименование раздела	Виды учебных	Образовательные технологии

п/п		занятий	
1	2	3	4
1	Конечные поля: основные понятия	Лекции Практическое занятие Самостоятельная работа	Вводная лекция с использованием видеоматериалов Решение и обсуждение вопросов и задач Консультирование и проверка домашних заданий посредством электронной почты
2	Поле р-адических чисел	Лекции Практическое занятие Самостоятельная работа	Лекция-визуализация с применением слайд-проектора. Решение и обсуждение вопросов и задач Подготовка к занятию с использованием электронного курса лекций, решение задач подобных задачам РГР
3	Алгебраические свойства целых р-адических чисел	Лекция Практическое занятие Самостоятельная работа	Лекции беседы, с разбором теоретических задач Решение и обсуждение вопросов и задач Подготовка к занятию с использованием электронного курса лекций
4	Топология пространства	Лекция Практическое занятие Самостоятельная работа	Проблемные лекции Решение и обсуждение вопросов и задач Консультирование и проверка домашних заданий посредством электронной почты
5	Введение в математический анализ	Лекция Практическое занятие Самостоятельная работа	Лекции беседы, с разбором теоретических задач Решение и обсуждение вопросов и задач Подготовка к занятию с использованием электронного курса лекций
6	Р-адические функции и их применение в теории кодирования	Лекция Практическое занятие Самостоятельная работа	Лекции беседы, с разбором теоретических задач Решение и обсуждение вопросов и задач Подготовка к занятию с использованием электронного курса лекций

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - опрос	10 баллов	10 баллов

- доклад - Расчетно-графическая работа (РГР) - Контрольная работа	10 баллов 25 баллов 15 баллов	10 баллов 25 баллов 15 баллов
Промежуточная аттестация (Экзамен по билетам)		40 баллов
Итого за семестр (дисциплину) Экзамен		100 баллов

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»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	«удовлетвори-тельно»	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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворител ьно»	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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Текущий контроль

Примерные темы докладов:

1. Первые идеи криптографии на кольцах.
2. p-адические многообразия.
3. Конечные поля и криптография. Примеры шифров и их развитие в истории.
4. Лемма Цорна.
5. Сходимость p-адических разложений.
6. Непрерывность степенных рядов $f(x)=\sum_{n=0}^{\infty} a_n x^n$, где $a_n \in Q_p$, $x-$ переменная, p-адический степенной ряд.
7. История возникновения p-адических чисел.
8. Об обобщенном признаке неразложимости Эйзенштейна.
9. Непрерывные дроби в полных полях.

Примерный вариант контрольной работы:

1. Докажите, что рационально число тогда и только тогда, когда представляется бесконечной десятичной периодической дробью.
2. Докажите, что если в евклидовом пространстве над множеством рациональных чисел определять расстояние между точками, то она может быть представлено десятичным разложением в ряд по степеням десяти.
3. Докажите, что следующие метрические пространства не являются полными и постройте их пополнение: 1) R с расстоянием $d(x,y)=|arctgx-arctgy|$; 2) R с расстоянием $d(x,y)=|e^x-e^y|$

Примерные задания для расчетно-графической работы (РГР):

1. Записать -1 и 3 с помощью 3-адических канонических степенных рядов.
2. Разрешимо ли уравнение $x^3-1=0$ в поле Z_7.
3. Исследовать разложение рациональных неразложимого многочлена в поле 3-адических чисел.
4. Пусть функция $f: Z_p \to Q_p$ определяется следующей формулой:

$f(x)=\begin{cases}0, & x=0,\\ 1/|x|_p, & x\neq 0\end{cases}$. Верно ли, что $f(x)$ непрерывная функция, а также является псевдоконстантой на Z_p?

Промежуточная аттестация

Примерные контрольные вопросы по курсу:

1. Конечное поле: определение, примеры.
2. Понятие пополнения. Нормированные поля.
3. Построение пополнения нормированного поля.
4. Нормирования поля рациональных чисел.
5. Нормирование алгебраических расширений.
6. Арифметические операции в Q_p.
7. p-адические разложения рациональных чисел.
8. Лемма Гензеля.
9. Нормирование алгебраических полей: общий случай.
10. Нормирование полей алгебраических чисел.
11. Теорема Островского.
12. Основные топологические свойства.
13. Канторово множество.
14. Последовательности и ряды.
15. p-адические степенные ряды.
16. Некоторые p-адические элементарные функции.
17. Разложение в ряд по p–адическим экспонентам, и логарифмам.
18. Локально постоянные функции.
19. Непрерывные и равномерно непрерывные функции.
20. Дифференцируемость p-адических функций.
21. p-адическое интерполирование.
22. Пример p-адического кода.

Примерные практические задания:

1. Докажите, что метрическое пространство полно тогда и только тогда, когда любая последовательность вложенных замкнутых шаров $\{B_n\}$, $B_1 \supset B_2 \supset B_3 \supset \ldots$, радиусы которых стремятся к нулю, имеет единственную общую точку.
2. Докажите, что поле Q_p, где p – простое число, не содержит делителей нуля.
3. Докажите, что если последовательности $\{a_n\}, \{b_n\}$ являются последовательностями Коши, то $\{a_n + b_n\}$, $\{a_n - b_n\}$, $\{a_n \cdot b_n\}$ также являются последовательностями Коши.
4. Доказать, что подмножество всех рациональных чисел и подмножество всех иррациональных чисел являются всюду плотными на вещественной прямой с метрикой $d(x, y) = |x - y|$.
5. Определите, являются ли следующие функции равномерно непрерывными на Z_p или непрерывными на N: 1. $f(x) = x_0 + x_1 x_2$; 2. $f(x) = P(x_0, x_1, x_2)$, где P – многочлен с коэффициентами в Z_p.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. Коблиц Нил. Курс теории чисел и криптографии / Н. Коблиц; [пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова]. - М.: ТВП, 2001. - X, 260 с.

Дополнительная

1. Хренников А. Ю. Введение в квантовую теорию информации / А. Ю. Хренников. - М.: Физматлит, 2008. - 283 с.
2. Акивис, М. А. Тензорное исчисление: Учебное пособие/Акивис М. А., Гольдберг В. В., 3-е изд., перераб. - Москва : ФИЗМАТЛИТ, 2005. - 304 с.ISBN 5-9221-0424-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/110700

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Единое окно доступа к образовательным ресурсам: http://window.edu.ru/window/library
2. Дифференциальное исчисление: http://math.ru/lib/3
3. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС)

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press SAGE Journals Журналы Taylor and Francis
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

- учебная аудитория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук,
- программное обеспечение (ПО).

Перечень программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010 Pro	Microsoft	лицензионное
2	Windows XP или Windows 7	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

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 CE;
  - 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, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Тема 1. Конечные поля: основные понятия

Задания:

1. Опишите все решения следующих сравнений:

а) $3x = 4 \pmod 7$; г) $27x = 25 \pmod{256}$;

б) $3x = 4 \pmod{12}$; д) $27x = 72 \pmod{900}$;

в) $9x = 12 \pmod{21}$; е) $3x = 612 \pmod{676}$.

2. Какой цифрой может заканчиваться полный квадрат в шестнадцатиричной системе счисления?

3. Доказать, что в десятичной системе счисления целое число тогда и только тогда делится на 3, когда сумма его цифр делится на 3, и что число делится на 9 тогда и только тогда, когда сумма его цифр делится на 9.

Указания по выполнению заданий: познакомиться с теоретическими основами темы; вычислять арифметические задания в Q_3, Q_5.

Тема 2. Поле p-адических чисел.

Задания:

1. Доказать, что $n^5 - n$ всегда делится на 30.
2. а) Пусть m есть либо степень p^a простого числа $p > 2$, либо удвоенная степень простого нечетного числа. Доказать, что если $x^2 = 1 \pmod m$, то либо $x = 1 \pmod m$, либо $x = -1 \pmod m$.

б) Доказать, что утверждение 2: а) неверно, если m не представимо в виде p^a или $2p^n$ и $m=4$.

в) Доказать, что если m — нечетное число, которое делится на 2 различных простых числа, то сравнение $x^2 = 1 \pmod m$ имеет 2^m различных решений между 0 и m.

Указания по выполнению заданий: познакомиться с теоретическими основами темы; вычислять арифметические задания в Q_p.

Тема 3. Алгебраические свойства целых p-адических чисел.

Задания:

1. Для $p = 2,3,5,7,11,13,17$ найти наименьшее положительное целое число, которое порождает F*, и определить, сколько среди чисел 1, 2, 3,..., $p - 1$ образующих.
2. Пусть $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ обозначает множество всех обратимых (т.е. не делящихся на p) вычетов по модулю p^a. Внимание: следует различать множество вычетов $\mathbb{Z}/p^\alpha\mathbb{Z}$ (в котором $p^\alpha - p^{\alpha-1}$ обратимых элементов) и поле F_{p^α} (в котором каждый ненулевой элемент обратим). Они совпадают лишь при $\alpha = 1$.

а) Пусть $p > 2$ и q — целое число, порождающее F_p^* F*. Пусть a — любое целое число, большее 1. Показать, что либо q, либо $(p+1)q$ порождают $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Таким образом, $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ — *циклическая группа.*

б) Показать, что при $a > 2$ группа $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ *нециклическая*, однако число 5 порождает *подгруппу,* состоящую из половины ее элементов, а именно, из элементов, сравнимых с 1 по модулю 4.

Указания по выполнению заданий: познакомиться с теоретическими основами темы; вычислять арифметические задания в Z_p. Первые криптографические идеи.

Тема 4. Топология пространства Q_p.

Задания:

1.Предположим, что $\alpha \in F_{p^2}$ удовлетворяет уравнению $X^2 + aX + b = 0$, где $a, b \in F_p$.

а) Доказать, что $\alpha \in F_{p^2}$ также удовлетворяет этому уравнению.

б) Доказать, что если $\alpha \notin F_{p^2}$ то $a = -\alpha - \alpha^2$ и $b = \alpha^{p+1}$.

в) Доказать, что если $\alpha \notin F_p$, а $c,d \in F_p$, то $(\alpha c + d)^{p+1} = d^2 - acd + bc^2 \in F_p$.

г) Пусть i — квадратный корень из —1 в F_{19^2}. Использовать пункт в), чтобы найти $(2+3i)^{101}$ (т.е. представить его в виде $a + bi$, $a, b \in F_{19}$).

Указания по выполнению заданий: познакомиться с теоретическими основами темы; изучать основные понятия в топологическом пространстве Q_p.

Тема 5. Введение в р-адический математический анализ.
Задания из книги [1, осн.лит]:
Коблиц Нил. Курс теории чисел и криптографии / Н. Коблиц; [пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова]. - М.: ТВП, 2001. - С.47:
№№12, 15
Указания по выполнению заданий: использовать математические пакеты прикладных программ, обсудить возможные пакеты и сайты с преподавателем.

Тема 6. р-адические функции и их применение в теории кодирования.
Задания из книги [1, осн.лит]:
Коблиц Нил. Курс теории чисел и криптографии / Н. Коблиц; [пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова]. - М.: ТВП, 2001. - С.56:
№№ 3, 7, 15, 19
Указания по выполнению заданий: использовать математические пакеты прикладных программ, обсудить возможные пакеты и сайты с преподавателем.

Приложения

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Элементы р-адического анализа и его приложения к криптографии» реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.

Цель дисциплины: изучение класса р-адическозначных функций, специальных классам Т-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 р-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-10 - готовность применять математический аппарат для решения поставленных задач, способность применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов.

В результате освоения дисциплины обучающийся должен:

Знать: о применении конечных полей в моделировании;

Уметь: применять полученные знания в решении задач организации математических моделей;

Владеть: достаточными представлениями о типах моделей, о способах реализации современными методами в компьютерных системах.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	Приложение к листу изменений №1	20.06.18	13
2	Приложение к листу изменений №2	28.06.19	13
3	Приложение к листу изменений №3	22.06.20	13

Приложение к листу изменений №1

1. Перечень программного обеспечения (ПО) (к п.7 на 2018г.)

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010 Pro	Microsoft	лицензионное
2	Windows XP или Windows 7	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (к п.6.2 на 2018г.)

Таблица 2

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Приложение к листу изменений №2

1. Перечень программного обеспечения (ПО) (к п.7 на 2019г.)

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010 Pro	Microsoft	лицензионное
2	Windows XP/ Windows 7 / Windows 10	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (к п.6.2 на 2019г.)

Таблица 2

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press SAGE Journals Журналы Taylor and Francis
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Приложение к листу изменений №3

1. Образовательные технологии (к п.4 на 2020г.)

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.

2. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (к п. 6.2 на 2020г.)

Таблица 1

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press SAGE Journals Журналы Taylor and Francis
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

3. Перечень программного обеспечения (ПО) (к п.7 на 2020г.)

Таблица 2

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010 Pro	Microsoft	лицензионное
2	Windows XP/ Windows 7 / Windows 10	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Zoom	Zoom	лицензионное