

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
Московский государственный университет имени М.В. Ломоносова  
Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**  
декан факультета  
вычислительной математики и кибернетики



/И.А. Соколов /  
октябрь 2021г.

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины (модуля):**

**Введение в р-адический анализ и его криптографические приложения**

**Уровень высшего образования:**

**магистратура**

**Направление подготовки / специальность:**

**01.04.02 "Прикладная математика и информатика" (3++)**

**Направленность (профиль) ОПОП:**

**Искусственный интеллект в кибербезопасности**

**Форма обучения:**

**очная**

Рабочая программа рассмотрена и утверждена  
на заседании Ученого совета факультета ВМК  
(протокол № 4, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

**1. Место дисциплины (модуля) в структуре ОПОП ВО:**

Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.

**2. Входные требования для освоения дисциплины (модуля):** учащиеся должны владеть знаниями по математическому анализу, дискретной математике, алгебре, и специальными курсами в объеме, соответствующем программе второго года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки» и другим направлениям подготовки бакалавриата.

**3. Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.**

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	Индикатор (показатель) достижения компетенции	Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций
ОПК-8. Способен осуществлять эффективное управление проектами по разработке и внедрению систем искусственного интеллекта	ОПК-8.1. Исследует архитектуру информационных систем предприятий и организаций; применяет методологии и технологии реинжиниринга, проектирования и аудита информационных систем различных классов ОПК-8.2. Применяет инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью ОПК-8.3. Исследует особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; применяет системы управления качеством ОПК-8.4. Выбирает методологию и технологию проектирования информационных систем; обосновывает архитектуру информационных систем и систем искусственного интеллекта ОПК-8.5. Управляет проектами по созданию (модификации) программного обеспечения, на всех	ОПК-8.1. 3-1. Знает новые научные принципы и методы реинжиниринга, проектирования и аудита информационных систем для решения профессиональных задач ОПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-8.2. 3-1. Знает особенности модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач ОПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-8.3. 3-1. Знает особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; системы управления качеством ОПК-8.3. У-1. Умеет применять системы управления качеством ОПК-8.4. 3-1. Знает методологию и технологию

	<p>стадиях жизненного цикла, оценивает эффективность и качество проекта; применяет современные методы управления проектами по разработке и внедрению систем искусственного интеллекта</p> <p>ОПК-8.6. Использует инновационные подходы к проектированию информационных систем и систем искусственного интеллекта; принимает решения по информатизации предприятий в условиях неопределенности</p> <p>ОПК-8.7. Проводит реинжиниринг прикладных и информационных процессов</p>	<p>проектирования информационных систем</p> <p>ОПК-8.4. У-1. Умеет обосновывать архитектуру информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.5. З-1. Знает особенности управления проектами по созданию (модификации) программного обеспечения на всех стадиях жизненного цикла,</p> <p>ОПК-8.5. У-1. Умеет оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.6. З-1. Знает инновационные подходы к проектированию информационных систем и систем искусственного интеллекта</p> <p>ОПК-8.6. У-1. Умеет принимать решения по информатизации предприятий в условиях неопределенности</p> <p>ОПК-8.7. З-1. Знает особенности процессного подхода, принципы реинжиниринга прикладных и информационных процессов</p> <p>ОПК-8.7. У-1. Умеет проводить реинжиниринг прикладных и информационных процессов</p>
<p>ПК-4. Способен руководить проектами по созданию, поддержке и использованию системы искусственного интеллекта на основе нейросетевых моделей и методов</p>	<p>ПК-4.3. Руководит проектами по разработке систем искусственного интеллекта на основе моделей глубоких нейронных сетей и нечетких моделей и методов</p>	<p>ПК-4.3. З-1. Знает принципы построения моделей глубоких нейронных сетей и глубокого машинного обучения (с подкреплением и без)</p> <p>ПК-4.3. З-2. Знает подходы к применению моделей на основе нечеткой логики в системах искусственного интеллекта</p> <p>ПК-4.3. У-1. Умеет руководить выполнением коллективной проектной деятельности для создания, поддержки и использования систем искусственного интеллекта на основе моделей глубоких нейронных сетей и нечетких моделей и методов</p>

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 72 академических часов на самостоятельную работу обучающихся.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий:

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

Наименование и краткое содержание разделов и тем дисциплины (модуля),  Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	В том числе			
		Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, часы			Самостоятельная работа обучающегося, часы <i>(виды самостоятельной работы – эссе, реферат, контрольная работа и пр. – указываются при необходимости)</i>
		Занятия лекционного типа*	Занятия семинарского типа*	Всего	
1. Основные понятия и теоремы $p$ -адической арифметики.	<b>6</b>	6	0	<b>6</b>	<b>0</b>
2. Основные понятия и теоремы $p$ -адического анализа.	<b>22</b>	10	0	<b>10</b>	<b>12</b> , домашнее практическое задание №1.
3. Основные понятия и методы $p$ -адической эргодической теории.	<b>2</b>	2	0	<b>2</b>	<b>0</b>
4. Основные понятия и методы $p$ -адической эргодической теории детерминированных функций.	<b>10</b>	4	0	<b>4</b>	<b>6</b> , домашнее практическое задание № 2
5. Основные методы анализа и синтеза $T$ -функций.	<b>4</b>	4	0	<b>4</b>	<b>0</b>

6. Основные конструкции криптопримитивов на базе T-функций	<b>8</b>	2	0	<b>2</b>	<b>6</b> , домашнее практическое задание № 3
7. Основные методы синтеза детерминированных функций, имеющих заданные криптографические характеристики, с помощью методов p-адической эргодической теории.	<b>4</b>	4	0	<b>4</b>	<b>0</b>
8. Основные методы синтеза и анализа конгруэнтных генераторов.	<b>16</b>	4	0	<b>4</b>	<b>12</b> , домашнее практическое задание № 4
Промежуточная аттестация: экзамен	<b>36</b>	0	0	<b>0</b>	<b>36</b>
<b>Итого</b>	<b>108</b>	<b>36</b>	<b>0</b>	<b>36</b>	<b>72</b>

6. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Практическое задание № 1

Найти обратный к заданному целому p-адическому числу, представить рациональное число в виде p-адического, найти с заданной точностью корень заданного полинома над кольцом целых p-адических чисел.

Практическое задание № 2

Представить детерминированную функцию заданного автомата в p-адическом виде.

Практическое задание №3

Проверить на биективность/транзитивность заданную T-функцию.

Практическое задание № 4

Применить знания, полученные в области p-адической теории детерминированных функций для решения ряда задач.

Примеры задач:

1. Используя теорему о сбалансированности детерминированных функций нескольких переменных, построить мультиплексор (латинский квадрат) размера  $p^N \times p^N$ , который по модулю  $p$  (т.е., при  $N=1$ ) совпадает с заданным латинским квадратом размера  $p \times p$ .
2. Проверить, достигает ли заданный конгруэнтный генератор максимально возможного периода.

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

Вопросы к экзамену.

1. Кольцо целых  $p$ -адических чисел.
2. Каноническая форма представления целого  $p$ -адического числа.
3.  $p$ -адическая метрика и ее свойства.
4. Шары, сферы и треугольники в пространстве целых  $p$ -адических чисел.
5. Арифметика кольца целых  $p$ -адических чисел. Обратимые элементы. Рациональные числа в кольце целых  $p$ -адических чисел.
6. Предел и сходимость в кольце целых  $p$ -адических чисел.
7. Критерий сходимости рядов в кольце целых  $p$ -адических чисел.
8. Непрерывные функции на кольце целых  $p$ -адических чисел.
9. Непрерывность детерминированных функций относительно  $p$ -адической метрики.
10. Представление  $p$ -адических функций в координатной форме.
11. Критерии детерминированности  $p$ -адической функции.
12. Дифференцируемые функции на кольце целых  $p$ -адических чисел. Производные команд процессора.
13. Вероятностная мера на кольце целых  $p$ -адических чисел. Функции, сохраняющие меру и эргодические функции.
14. Основная эргодическая теорема для детерминированных функций.
15. Критерий эргодичности аффинной функции и смешанный конгруэнтный метод.
16. Критерий сохранения меры для  $T$ -функции в терминах координатных функций.
17. Критерий эргодичности для  $T$ -функции в терминах координатных функций.
18. Критерии и достаточные условия сохранения меры для детерминированных функций нескольких переменных.
19. Латинские квадраты и ортогональные латинские квадраты на базе детерминированных функций.

20. Типовые конгруэнтные генераторы на базе детерминированных функций.

Экзаменационный билет состоит из одного вопроса и одной задачи по разным частям курса, например

1. Критерий эргодичности T-функции в терминах координатных функций.
2. Проверить, эргодична ли T-функция  $f(x)=(1+x)\text{XOR}(4x^2)$ .

<b>ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)</b>				
Оценка РО и соответствующие виды оценочных средств	2	3	4	5
<b>Знания</b> <i>Экзамен</i>	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
<b>Умения</b> <i>Самостоятельные работы, практические задания</i>	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности принципиального характера)	Успешное и систематическое умение
<b>Навыки (владения, опыт деятельности)</b> <i>Экзамен</i>	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач



Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)	
Результаты обучения	Компетенция, с частичным формированием которой связано достижение результата обучения
<p><b>Знать:</b></p> <ol style="list-style-type: none"> <li>1. основы р-адического анализа;</li> <li>2. основы р-адической динамики;</li> <li>3. основные конструкции Т-функций, имеющих заданные криптографические свойства;</li> <li>4. основы р-адической теории детерминированных функций.</li> </ol> <p><b>Уметь:</b></p> <ol style="list-style-type: none"> <li>1. применять на практике полученные знания к исследованию различных криптопримитивов на базе Т-функций;</li> <li>2. строить и изучать математические модели криптоалгоритмов, используемых в их криптоанализе;</li> <li>3. решать основные задачи по применению криптографических алгоритмов в защите информации;</li> <li>4. понимать и применять на практике математические методы для решения различных задач криптографического анализа;</li> <li>5. находить, анализировать и обрабатывать научно-техническую информацию;</li> <li>6. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;</li> <li>7. демонстрировать способность к анализу и синтезу;</li> <li>8. демонстрировать способность к письменному и устному общению на русском языке.</li> </ol> <p><b>Владеть:</b></p>	СПК- рАНиКП-1.Б

- |  |  |
|--|--|
| <ol style="list-style-type: none"><li>1. навыками употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;</li><li>2. использования математического аппарата в проведении исследований;</li><li>3. пользования библиотеками прикладных программ для ЭВМ для решения прикладных задач.</li></ol> |  |
|--|--|

## 7. Ресурсное обеспечение:

### 7.1. Перечень основной и дополнительной литературы

#### Основная литература

1. Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011  
(<https://istina.msu.ru/download/8722989/1kWHXg:0y-WK9SFZmwMtvkVPLcDyYg6nOI/>).

#### Дополнительная литература

1. Кнут Д. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. - Москва–СПб–Киев: Вильямс, 2000
2. Anashin V., Khrennikov A. Applied Algebraic Dynamics, Walter de Gruyter GmbH & Co, Berlin—N.Y.,2009.
3. Anashin V. The p-adic ergodic theory and applications  
(<https://istina.msu.ru/download/294049719/1kWHfM:Z1rox82nsVkmQM-CUPaFAqK31Y8/>)
4. Коблиц Н. p-адические числа, p-адический анализ и дзета-функции. - М.: Мир, 1982.
5. Хренников А.Ю. Неархимедов анализ и его приложения. – М.: Физматлит, 2003
6. Каток С.Б. p-адический анализ в сравнении с вещественным. –М.: МЦНМО, 2004
7. Анашин В.С. Неархимедов анализ, T-функции и криптография.- М.: 2007  
(<https://istina.msu.ru/download/8722988/1kWHXg:ptg5r5DGWtVSpLKeGAZq8TjlHLY/>).
8. Анашин В.С. Введение в прикладной p-адический анализ. - М.: 2008  
([https://istina.msu.ru/download/8722987/1kWHXg:q93yFDOApSa2yhi5\\_rDm\\_yYhOoY/](https://istina.msu.ru/download/8722987/1kWHXg:q93yFDOApSa2yhi5_rDm_yYhOoY/)).

### 7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

Программное обеспечение для подготовки слайдов лекций MS PowerPoint, MS Word

Программное обеспечение для создания и просмотра pdf-документов Adobe Reader

Издательская система LaTeX

Язык программирования Python и среда разработки Jupiter Notebook (вместе с библиотеками numpy, scikit-learn, pandas)

Язык программирования R и среда разработки R Studio

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. <http://www.edu.ru> – портал Министерства образования и науки РФ
2. <http://www.ict.edu.ru> – система федеральных образовательных порталов «ИКТ в образовании»
3. <http://www.openet.ru> - Российский портал открытого образования
4. <http://www.mon.gov.ru> - Министерство образования и науки Российской Федерации
5. <http://www.fasi.gov.ru> - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.  
URL: <http://www.mathnet.ru>
2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: [www.biblioclub.ru](http://www.biblioclub.ru)
3. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.  
URL: [www.ebiblioteka.ru](http://www.ebiblioteka.ru)
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц.  
URL: [www.eLibrary.ru](http://www.eLibrary.ru)

7.5. Описание материально-технического обеспечения.

Факультет ВМК, ответственный за реализацию данной Программы, располагает соответствующей материально -технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база факультета соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

профессор факультета ВМК МГУ В.С.Анашин .

10. Язык преподавания - русский.