АННОТАЦИЯ

Б1.В.ДВ.2 Компьютерное моделирование в теории кодирования и криптографии

1. Цель дисциплины

Цель освоения дисциплины – формирование углубленных знаний по компьютерной алгебре: алгоритмов проверки чисел на простоту, групп с условиями конечности, числовыми и метрическими характеристиками не локально конечных алгебраических объектов.

Задачи освоения дисциплины «Компьютерное моделирование в теории кодирования и криптографии»: получение базовых теоретических сведений о решении основных задач описания массивов простых чисел, востребованных в задачах криптографии, численных расчетов некоторых характеристик групп бернсайдового типа и групп автоморфизмов деревьев.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения некоторых задач теории кодирования и криптографии, описания кодирующих деревьев, структуры автоморфизмов сгущений простых чисел, метрических характеристик не локально конечных групп, задаваемых конечными автоматами. Получаемые знания лежат в основе математического образования и служат развитию навыков математического моделирования, применения численных методов и программных комплексов.

2. В результате изучения дисциплины аспирант должен:

	• **Структура компетенции**		
	• **Знать**	• **Уметь**	• **Владеть**
ОПК-8	особенности культуры научного исследования, в том числе с использованием современных информационно-коммуникационных технологий	использовать в профессиональной деятельности современные информационно-коммуникационные технологии	культурой научного исследования, в том числе с использованием современных информационно-коммуникационных технологий

УК-1	фундаментальные и прикладных разделы специальных дисциплин в области математических методов и моделей	творчески использовать в научной и производственно-технологической деятельности знания фундаментальных и прикладных разделов специальных дисциплин	Приемами и методами творческого использования в научной и производственно-технологической деятельности знания фундаментальных и прикладных разделов специальных дисциплин в области математических методов и моделей

3. Краткое содержание дисциплины:

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Операционные системы на открытом коде и языки программирования	Операционная система Debian. Современный язык научного программирования Python. Современный язык математических распределенных вычислений Julia.	Опрос по результатам индивидуального задания
2	Теоретико-числовые методы криптографии. Распределение простых чисел	Однонаправленные функции. Криптография с открытым ключом. Ключевая система. Распределение простых чисел на прямой. Гипотеза Харди-Литтлвуда. Плотные скопления простых чисел. Численные эксперименты	Опрос по результатам индивидуального задания
3	Алгебраические системы с условиями конечности, бернсайдовы группы	Условия конечности. Группы автоморфизмов однородных деревьев. Проблема Бернсайда. Группа конечных автоматов, AT-группы, ветвящиеся группы. Вычисление числовых характеристик.	Опрос по результатам индивидуального задания

4	Пакеты компьютерной алгебры на открытом коде. Проект Sage	Компьютерная алгебра и численный анализ. Точная, целочисленная и полиномиальная арифметики. Системы компьютерной алгебры. Функциональное назначение. Тип архитекту-ры. Средства реализации. Область применения. Интегральные оценки качества. Пакеты компьютерной алгебры PARI/GT, GAP, Sage. Обзор их возможностей и сравнение функционала. Объединяющая роль проекта Sage.	Проверка индивидуальных расчетных заданий

4. Объем учебной дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 108 часов.

Вид работы	Трудоемкость, часов
	3 курс
Общая трудоемкость	**108**
Аудиторная работа:	44
Лекции (Л)	8
Практические работы (ПР)	18
Лабораторные работы (ЛР)	18
Самостоятельная работа:	
Курсовой проект (КП), курсовая работа (КР)	
Расчетно-графическое задание (РГЗ)	
Реферат (Р)	
Эссе (Э)	
КСР	
Контроль (К)	
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)	64
Подготовка и сдача зачета	
Вид итогового контроля	зачет

Проведение зачета предпочтительно проводить в форме конференции аспирантов, посвященной обзору области математических методов исследования моделей алгебраических и криптографических систем и, одновременно, проектированию оригинальных инновационных решений.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ:

а) основная литература:

1. Саммерфилд М. Python на практике. Пер. с англ. Слинкин А.А. М.: ДМК Пресс. 2014. 338с. (http://e.lanbook.com/books/element.php?pl1_id=66480)
2. Музыкантский А.И., Фурин В.В. Лекции по криптографии. М.: МЦНМО (Московский центр непрерывного математического образования) 2011. 68 с. (http://e.lanbook.com/books/element.php?pl1_id=9373)
3. Торстейнсон П., Ганеш Г.А.Криптография и безопасность в технологии .NET. Спб.: Лаборатория знаний. 2013. 480 с. (http://e.lanbook.com/books/element.php?pl1_id=8767)
4. Ян, Сонг Й. Криптоанализ RSA / Ян, Сонг Й. ; С. Й. Ян ; пер. с англ. Ю. Р. Айдарова. - Москва : Регулярная и хаотическая динамика, 2011. - 285 с.
5. Крэндалл, Ричард. Простые числа: криптографические и вычислительные аспекты / Крэндалл, Ричард, Померанс, Карл ; Р. Крэндалл, К. Померанс ; под ред. и с предисл. В. Н. Чубарикова ; пер. со второго доп. англ. изд. А. В. Бегунца и др. - Москва : URSS : [Книжный дом "Либроком"], 2011. - 663 с.

б) дополнительная литература:

1. Рожков А.В., Ниссельбаум О.Н. Теоретико-числовые методы в криптографии. Учебное пособие. – Тюмень: ТюмГУ, 2007, -160 с.
2. Рожков А.В. АТ-группы. Учебное пособие. – Челябинск: Изд-во ЧелГУ, 1999, - 120 с.
3. Рожков А.В. Об условиях конечности, ослабляющих локальную конечность // Доклады РАН, 1998, Т. 362, № 4, С. 445 – 448.
4. Негус К., Каэн Ф. Ubuntu и Debian Linux для продвинутых: более 1000 незаменимых команд. - СПб.: Питер, 2011. — 352 с: ил.
5. Лутц М. Изучаем Python, 4-е изд. - Пер. с англ. - СПб.: Символ-Плюс, 2011. - 1280 с, ил.
6. Доусон М. Программируем на Python, 3-е изд. - СПб.: Питер, 2014. —416 с: ил.
7. Грошев А.С., Закляков П.В. Информатика, 3-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2015. – URL: http://e.lanbook.com/view/book/69958/
8. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: http://e.lanbook.com/view/book/67458/
9. Голубков А.Ю. Компьютерная алгебра в системе SAGE. [Электронный ресурс]. – М.: МГТУ им. Н.Э. Баумана, 2013. – URL: http://e.lanbook.com/view/book/52433/
10. Рожков А.В. Типовые курсовые работы по теоретико-числовым методам криптографии. Электронное пособие. – Челябинск: ЮУрГУ (НИУ), 2012, 60 с.

11. Рожков А.В. Решебник задач по криптографии. Электронное пособие. – Челябинск: ЮУрГУ (НИУ), 2010, 110 с.
12. Зобнин А.И. Компьютерная алгебра в системе Sage. Учебное пособие. – М.: Изд-во МГТУ им Баумана, 2011. – 55 с.

в) программное обеспечение и Интернет-ресурсы:

1. Клиентская ОС Debian 8. Официальный сайт https://www.debian.org/index.ru.html
2. Язык программирования Python. Официальный сайт https://www.python.org/
3. Пакет компьютерной алгебры на открытом коде Sage 6.9. Официальный сайт http://sagemath.org/
4. Пакет компьютерной алгебры на открытом коде Gap4r7p8. Официальный сайт http://www.gap-system.org/