МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Кубанский государственный университет»
(ФГБОУ ВПО «КубГУ»)

Факультет математики и компьютерных наук
Кафедра прикладной математики

«УТВЕРЖДАЮ»
Проректор по учебной работе,
качеству образования – первый проректор,
доктор исторических наук, профессор
_____ Иванов А.Г.
«___» _____ 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.2
КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В ТЕОРИИ КОДИРОВАНИЯ И КРИПТОГРАФИИ

Направление подготовки
09.06.01 Информатика и вычислительная техника
Профиль подготовки
05.13.18 Математическое моделирование, численные методы и комплексы программ

Квалификация выпускника
кандидат физико-математических наук
Форма обучения
очная

г. Краснодар – 2015 г.

Рабочая программа дисциплины компьютерное моделирование в теории кодирования и криптографии составлена на основании федеральных государственных образовательных стандартов к основной образовательной программе высшего образования подготовки научно-педагогических кадров в аспирантуре по направлению 09.06.01 Информатика и вычислительная техника.

Программу составил: А.В. Рожков – доктор физико-математических наук, профессор кафедры функционального анализа и алгебры Куб ГУ

Заведующий кафедрой прикладной математики
д.ф.-м.н., профессор М.Х. Уртенов
«_____» _____ 2015г.

Рабочая программа обсуждена на заседании кафедры прикладной математики от «_____» _____ 2015 г., протокол № _____.

Заведующий кафедрой прикладной математики
д.ф.-м.н., профессор м.х. уртенов
«_____» _____ 2015 г.

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики от «_____» _____ 2015 г., протокол № ____.

Председатель УМК факультета компьютерных технологий и прикладной математики к.ф.-м.н., доцент К.В. Малыхин

Рецензенты:

Шапошникова Т.Л. – профессор, доктор педагогических наук, кандидат физико-математических наук, заведующая кафедрой физики КубГТУ

Видовский Л.А. – доктор технических наук, доцент, заведующий кафедрой информационных систем и программирования КубГТУ

1. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цели изучения дисциплины определены государственным образовательным стандартом высшего профессионального образования и соотнесены с общими целями ООП ВПО по направлению подготовки направлению подготовки 09.06.01 Информатика и вычислительная техника, профиль подготовки 05.13.18 Математическое моделирование, численные методы и комплексы программ, в рамках которой преподается дисциплина.

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. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Компьютерное моделирование в теории кодирования и криптографии» относится к вариативной части (В) профессионального цикла (Б1) дисциплины по выбору (ДВ), являющегося структурным элементом ООП ВПО.

Данная дисциплина тесно связана с такими дисциплинами цикла (Б1), как Математическое моделирование, Численные методы и комплексы программ, Математические методы и модели. Она направлена на формирование твердых теоретических знаний и практических навыков работы с известными математическими методами и моделями теории кодирования и криптографии.

Для её успешного усвоения необходимы знания, умения и компетенции, приобретаемые при изучении следующих дисциплин: линейная алгебра, математический анализ, дифференциальные уравнения, математическая логика, дискретная математика, языки программирования, в рамках дисциплин математического и естественнонаучного цикла ООП аспирантуры.

Изучение этой дисциплины готовит обучаемых к различным видам как практической, так и теоретической, исследовательской деятельности.

3. КОМПЕТЕНЦИИ АСПИРАНТА, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина формирует следующие компетенции, которыми должен обладать выпускник, освоивший программу аспирантуры в соответствии с задачами профессиональной деятельности и целями основной образовательной программы:

В результате освоения 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

4.ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

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 экзамена	
Вид итогового контроля	зачет

5.СОДЕРЖАНИЕ И СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

5.1.Учебно-тематический план очной формы обучения

№ п/п	**Наименование раздела, темы**	***Всего***	***Аудиторные занятия***				**СР.**
			Всего	**Л**	**ЛР**	**Пр**	
1.	Операционные системы на открытом коде и языки программирования	26	10	2	4	4	16
2.	Теоретико-числовые методы криптографии. Распределение простых чисел	26	10	2	4	4	16
3.	Алгебраические системы с условиями конечности, бернсайдовы группы	26	10	2	4	4	16
4.	Пакеты компьютерной алгебры на открытом коде. Проект Sage	30	14	2	6	6	16
	Итого:	108	44	8	18	18	64

5.2. Содержание разделов 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	Однонаправленные функции. Криптография с от-	Опрос по результатам индивиду-

	криптографии. Распределение простых чисел	крытым ключом. Ключевая система. Распределение простых чисел на прямой. Гипотеза Харди-Литтлвуда. Плотные скопления простых чисел. Численные эксперименты	ального задания
3	Алгебраические системы с условиями конечности, бернсайдовы группы	Условия конечности. Группы автоморфизмов однородных деревьев. Проблема Бернсайда. Группа конечных автоматов, АТ-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 архитектуры. 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

5.3 Лабораторные занятия

Основная цель лабораторных занятий состоит в приобретении навыков построения и анализа компьютерных моделей основных задач теории кодирования и криптографии, проведения вычислительного эксперимента, выявлении имеющихся проблем, обосновании возможных путей их решения. Самостоятельная работа аспирантов на основе изучения основной и дополнительной научной литературы позволяют закрепить полученные знания, расширить круг задач, рассмотренных на лекциях практических занятиях.

Темы лабораторных занятий

1. Установка и настройка операционной системы Debian. Установка новых пакетов. Установка пакета компьютерной алгебры Sage

2. Основы программирования на языке Python. Сравнение линеек 2.x и 3.x. простейшие символьные вычисления. Работа с циклами. Создание и отладка программы вычислений массивов простых чисел

3. Основы программирования на языке Julia. Связь с языком Python. Программирование распараллеливаемых процессов.

4. Основные структуры теории групп с условиями конечности. Продольные и корневые порождающие AT-групп. Программирование рекурсивных вычислений в теории AT-групп.

5. Проект Sage. Запуск программ, написанных на Python и Julia в Sage. Вычисление нижних рядов AT-групп над последовательностью простых чисел.

6. Вычисление метрических характеристик AT-групп. Построение систем простых чисел общего положения средствами пакета Sage на платформе Debian.

5.4. Самостоятельное изучение разделов дисциплины

Одним из главных методов изучения курса «Компьютерное моделирование в теории кодирования и криптографии» является самостоятельная работа аспирантов с учебной, научной и другой рекомендуемой преподавателем литературой.

Цель самостоятельной работы – расширение кругозора и углубление знаний в области применения компьютерных методов анализа конкретных гидродинамических задач. Самостоятельная работа ведется в двух аспектах:

1) по теоретическим вопросам:

- конспекты изученного материала,
- реферат;

2) по практическим вопросам – в электронном или на бумажном носителе отчет о выполненных лабораторных работах, расчетах, созданном программном продукте, результатах исследований.

Практическое занятие позволяет научить аспиранта применять теоретические знания при решении и исследовании конкретных задач. Это обусловлено тем, что в процессе исследования часто встречаются задачи, для которых единых подходов не существует. Каждая конкретная задача при своем исследовании имеет множество подходов, а это требует разбора и оценки целой совокупности конкретных ситуаций. Этот подход особенно широко используется при определении адекватности математической модели и результатов вычислительного эксперимента.

Задания для самостоятельной работы

Теоретические вопросы:

1. Файловая структура и базовые настройки операционной системы Debian.
2. Основные задачи теории кодирования и криптографии.
3. Группы автоморфизмов деревьев – их определение, структуры и классы.
4. Базовые конструкции языка программирования Python.
5. Базовые конструкции языка программирования Julia.

6. Применение вероятностных тестов на проверку простоты чисел при построении массивов простых чисел типа k-tuples.

Практические задания:

1. Алгоритмы проверки на простоту.
2. Эллиптические кривые над конечными полями
3. Алгоритмы вычисления в конечных полях.
4. Электронная подпись по схеме Эль Гамаля.
5. Электронная подпись на основе RSA.
6. Случайные и псевдослучайные гаммы.
7. Регистры сдвига с обратной связью.
8. Базовые команды Linux
9. Команда arch: сведения об архитектуре компьютера; Команда date: вывод даты и времени; Команда env: установка переменных окружения; Команды man и info: вывод справки.

Темы рефератов

Тема 1. Основные задачи теории кодирования и криптографии.
Тема 2. Корневая файловая система и монтирование.
Тема 3. Переход с Windows на Linux.
Тема 4. Криптосистемы с открытым ключом.

Формы контроля за выполнением самостоятельной работы

Для промежуточного контроля аспиранты предоставляют отчёт в электронном или печатном виде по результатам изучения теоретических вопросов и выполнения заданий к самостоятельной работе.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИ

Используется как традиционная информационно-объяснительная подача материала, так и интерактивная подача материала с мультимедийной системой. Компьютерные технологии в данном случае обеспечивают возможность разнопланового отображения алгоритмов и демонстрационного материала. Такое сочетание позволяет оптимально использовать отведённое время и раскрывать логику и содержание дисциплины.

Занятия в диалоговом режиме предполагают обсуждение вопросов по рекомендованной к изучению литературе и документам, а также вопросы на знание проблем и противоречий изучаемой темы, раскрывающие отношение слушателей к этим проблемам и противоречиям.

Лекции представляют собой систематические обзоры основных математических методов и моделей теории кодирования и криптографии.

Лабораторное занятие позволяет научить аспирантов применять теоретические знания при решении и исследовании конкретных задач теории кодирования и криптографии**.**

Индивидуальные задания связаны с настоящей или будущей профессиональной деятельностью аспиранта. В этом качестве могут использоваться:

задания на разработку программного продукта для решения конкретных задач теории кодирования и криптографии***;***

задания на проведение численного эксперимента и анализ конкретной гидродинамической задачи.

Семинары предполагают использование дополнительных методов освоения учебного материала, в том числе:

доклад по материалам статьи (исследования);

обзорный доклад по изучаемой проблеме.

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.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа аспирантов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе, написания рефератов и выполнения самостоятельных расчетных заданий.

Фонд оценочных средств дисциплины состоит из средств текущего контроля и итоговой аттестации (экзамена).

7.1. Примерный перечень вопросов к зачету

1. Группы обратимых элементов в кольцах.
2. Структура мультипликативной группы кольца вычетов.
3. Примитивные элементы.
4. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
5. Криптографические хеш-функции.
6. Электронная подпись.
7. Криптографические протоколы.
8. Имена файлов в Linux
9. Корневая файловая система и монтирование
10. Стандартные каталоги Linux
11. Работа с файлами
12. Работа с каталогами
13. Команды chown, chmod и chattr
14. Файловая система ext4
15. Расширения конечных полей.

16. Алгоритм шифрования AES: структура поля, нахождение обратных элементов.

Вопросы к зачету

1. Техника символьных вычислений.
2. Функциональные LISP-выражения.
3. Китайская теорема об остатках и е применение.
4. Примитивные элементы конечных полей.
5. Компьютерная алгебра в криптографии.
6. Алгоритмы быстрого умножения матриц.
7. Рюкзачные алгоритмы.
8. Извлечение квадратных корней в конечных полях.
9. Алгоритм Штрассена.
10. Алгоритм Винограда-Штрассена.
11. Обзор вероятностных алгоритмов разложения на простые множители.
12. Загрузчики Linux
13. Конфигурационные файлы GRUB и GRUB2
14. Системы инициализации Linux
15. Команды управления пользователями
16. Пользователь root

7.2. Порядок формирования оценок по дисциплине

Экзамены оцениваются по системе: неудовлетворительно, удовлетворительно, хорошо, отлично.

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/