МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»
(ФГБОУ ВО “КубГУ”)

Факультет компьютерных технологий и прикладной математики
Кафедра прикладной математики

УТВЕРЖДАЮ:
Проректор по научной работе и инновациям
_____ Барышев М.Г.
подпись
«__30__» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.2.2 КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В ТЕОРИИ КОДИРОВАНИЯ И КРИПТОГРАФИИ

Направление подготовки 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

ПРОФИЛЬ 05.13.18 Математическое моделирование, численные методы и комплексы программ

Форма обучения Очная и заочная

Краснодар 2018

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:
д.ф.-м.н., профессор М.Х. Уртенов

Рабочая программа обсуждена на заседании кафедры прикладной математики протокол № 7 «18» апреля 2018г.

Заведующий кафедрой прикладной математики
д.ф.-м.н., профессор М.Х. Уртенов

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 1 «20» апреля 2018г.

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

Рецензенты:

Шапошникова Татьяна Леонидовна.
Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Директор института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.
Доктор технических наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».
КубГТУ

1. Цели и задачи учебной дисциплины

1.1 Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО 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.

1.2 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.

1.3МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

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

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 ООП аспирантуры.

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

1.4 Компетенции аспиранта, формируемые в резуль- тате 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
ОПК-2	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
ОПК-7	основными методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности	владеть методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности	способность ю владеть методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности
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

УК-4	как использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	Готовностью использовать современные методы и технологии научной коммуникации на государственном и иностранном языках

2. Объем дисциплины и виды учебной работы

Для ОФО:

Вид работы	Трудоемкость, часов
	3 курс
Общая трудоемкость	**108**
Аудиторная работа:	44
Лекции (Л)	8
Практические работы (ПР)	36
Лабораторные работы (ЛР)	
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

Содержание и структура учебной дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

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		8	16

2.	Теоретико-числовые методы криптографии. Распределение простых чисел	26	10	2		8	16
3.	Алгебраические системы с условиями конечности, бернсайдовы группы	26	10	2		8	16
4.	Пакеты компьютерной алгебры на открытом коде. Проект Sage	30	14	2		12	16
	Итого:	108	44	8		36	64

Для ЗФО:

Вид работы	Трудоемкость, часов	
	3 курс	4 курс
Общая трудоемкость	**108**	
Аудиторная работа:		
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.)	46	18
Подготовка и сдача экзамена		
Вид итогового контроля	зачет	

Содержание и структура учебной дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Учебно-тематический план заочной 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			16

2.	Теоретико-числовые методы криптографии. Распределение простых чисел	26	10	2			16
3.	Алгебраические системы с условиями конечности, бернсайдовы группы	26	10	2	6	6	16
4.	Пакеты компьютерной алгебры на открытом коде. Проект Sage	30	14	2	12	12	16
	Итого:	108	44	8	18	18	64

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 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, 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

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.

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.

3. Образовательные технологии

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.

4. 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).

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

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 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. Адаменко, М.В. Основы классической криптологии : секреты шифров и кодов [Электронный ресурс] / М.В. Адаменко. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 256 с. — Режим доступа: https://e.lanbook.com/book/9123. — Загл. с экрана.

Дополнительная литература:

1. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351

2. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=229582

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронно-библиотечная система Издательство «Лань». http://e.lanbook.com
2. Network Workbench [Электронный ресурс]. – Режим доступа: http://nwb.cns.iu.edu/
3. SciMAT – Science Mapping Analysis Tool [Электронный ресурс]. – Режим доступа: http://sci2s.ugr.es/scimat
4. Science & Engineering Indicators www.nsf.gov
5. International Mathematical Union http://www.imu.org

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

Перечень необходимого программного обеспечения

1. Операционная система MS Windows (разделы 2, 3, 5 дисциплины).
2. Интегрированное офисное приложение MS Office (разделы 2, 3, 5 дисциплины).
3. Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет (разделы 2, 3, 5 дисциплины).
4. Математические пакеты Matlab, COMSOL Multiphysics
5. Python 3.5

Перечень необходимых информационных справочных систем

1. Википедия, свободная энциклопедия. [Электронный ресурс]. – Wikipedia http://ru.wikipedia.org
2. Электронная библиотека КубГУ

8. Материально-техническое обеспечение учебной дисциплины

В качестве материально-технического обеспечения дисциплины используются - проекционное оборудование (цифровой проектор, экран, ноутбук).

№	Наименование специальных* помещений и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения
1.	Аудитория, для лекционных занятий	Учебная мебель, компьютерная техника, стационарное или переносное мультимедийное оборудование (129, 131, 133, А305, А307, А508, 239А)
2.	Аудитория, для лабораторных занятий	Аудитория для семинарских занятий, укомплектованная необходимой мебелью (доска, столы, стулья) компьютерами с лицензионным программным обеспечением и выходом в интернет (106, 106а, А301, А504, 239А)
3.	Аудитория, для практических занятий	Аудитория для семинарских занятий, укомплектованная необходимой мебелью (доска, столы, стулья), презентационной техникой (аудитории: 129, 131, А305, А307, 239А) или переносным демонстрационным оборудованием (аудитории: 133,147, 148, 149, 150, 100С, А301б, А512, А508, 239А)
4.	Аудитория для групповых и индивидуальных консультаций	Аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета, лицензионное программное обеспечение (А504, А506, 239А)
5.	Текущий контроль, промежуточная аттестация	Аудитория для семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованная необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307, 147, 148, 149, 150, 100С, А301б, А512, А508), компьютерами с лицензионным программным обеспечением и выходом в интернет (106, 106а, А301, А504, 239А)

6.	Аудитория для самостоятельной работы	Аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета, лицензионное программное обеспечение (А 504, 102А)