

Аннотация по дисциплине
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

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.

Место 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.

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
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	способностью владеть методами проведения патентных исследований, лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности
УК-1	фундаментальные и прикладные 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
------	---	---	---

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

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

Перечень основной учебной литературы, необходимой для освоения дисциплины

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.