

АННОТАЦИЯ
дисциплины «ФТД.01 ЭКСПЕРИМЕНТАЛЬНАЯ ТЕОРИЯ ЧИСЕЛ»

Объем трудоемкости: 2 зачетные единицы (72 часа, из них – 32,2 часа контактной работы (16 часов лекций, 16 часов практических занятий, 0,2 часа ИКР); 39,8 часа самостоятельной работы).

Цель дисциплины:

Цель освоения дисциплины – рассмотрение задач информатизации и научного программирования. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины:

Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах символьных математических вычислений. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации. А также при анализе структур информационных систем и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра и численный анализ. Элементы теории сложности алгоритмов. Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.

Место дисциплины в структуре ООП ВО

Дисциплина «Экспериментальная теория чисел» является факультативом.

Данная дисциплина, как алгоритмическая основа криптографии, криптоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотек алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины:

№ раз- дела	Наименование разделов	Количество часов			
		Всего	Аудиторная ра- бота		Самостоя- тельная ра- бота (срс+ксп)
			Л	Пр	
1	2	3	4	5	6
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	14	4	4	6
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	18	4	4	10
3	LISP-машины. Целочисленная арифметика. Полиномиальная арифметика.	18	4	4	10
4	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	21,8	4	4	13,8
Итого:			16	16	39,8

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Бухштаб А.А. Теория чисел, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: <https://e.lanbook.com/book/65053>
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: <https://e.lanbook.com/book/68466>

Дополнительная литература:

1. Конова Е.А., Поллак Г.А. Алгоритмы и программы. Язык C++, 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2018. – URL: <https://e.lanbook.com/book/103905>
2. Окулов С.М. Программирование в алгоритмах, 6-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2017. – URL: <https://e.lanbook.com/book/94140>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

1. Пакет компьютерной алгебры Sage 8.3. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r9p3. Официальный сайт <http://www.gap-system.org/>
3. Клиентская ОС Debian 9.5. Официальный сайт <https://www.debian.org/>
4. Система аудита и обнаружения вторжений Kali Linux 2018.2. Официальный сайт <http://www.kali.org/>

Автор РПД, д.ф.-м.н., профессор

Рожков А.В.