

## **АННОТАЦИЯ рабочей программы дисциплины «ФТД.01 Экспериментальная теория чисел»**

**Направление подготовки/специальность 01.04.01 Математика**

**Объем трудоемкости:** 2 зач. ед.

### **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: ПК-4.

### **Основные разделы дисциплины:**

Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.

Структуры данных в компьютерной алгебре. Техника символьных вычислений.

LISP-машины. Целочисленная арифметика. Полиномиальная арифметика.

Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.

**Курсовые работы:** не предусмотрены.

**Форма проведения аттестации по дисциплине:** зачет

Автор РПД, д.ф.-м.н., профессор

Рожков А.В.