

АННОТАЦИЯ
рабочей программы дисциплины
«Б1.О.15 Дополнительные главы фундаментальной математики»

Направление подготовки 02.04.01 Математика и компьютерные науки

Объем трудоемкости: 3 зач. ед.

Цель дисциплины:

Целями освоения дисциплины «Дополнительные главы фундаментальной математики» являются формирование математической культуры студентов; формирование способностей к алгоритмическому и логическому мышлению, овладение современным аппаратом дифференциальных уравнений для дальнейшего использования в других областях математического знания и дисциплинах естественнонаучного содержания; более углубленное изучение алгоритмической математики, освоение приложений теории алгоритмов алгебры в различных областях математики, информатики и защиты информации; творческое овладение основными методами теории алгебраических вычислений.

Задачи дисциплины:

Дать студентам знания о различных подходах к построению алгебраических и теоретико-числовых алгоритмов, об основных понятиях теории колец и теории чисел. Ознакомить студентов современными математическими методами в фундаментальных и прикладных задачах анализа и применения алгоритмов.

Место дисциплины в структуре ООП ВО

Дисциплина «Дополнительные главы фундаментальной математики» включена в обязательную часть Блока 1. Дисциплины и модули. и является обязательной дисциплиной для направления 02.04.01. «Математика и компьютерные науки».

Для успешного освоения дисциплины обучающийся должен владеть знаниями, умениями и навыками по программе дисциплин «Алгебра», «Теория алгоритмов». Дисциплина изучается в 4 семестре.

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: ОПК-2, ПК-1.

Основные разделы дисциплины: Разделы дисциплины, изучаемые в 4 семестре:

Кольца вычетов. Китайская теорема об остатках.

Решение уравнений в кольцах матриц над полем и в кольце целых чисел.

Регистры сдвига с обратной связью.

Поля Галуа. Структура полей.

Неприводимые многочлены над полями Галуа.

Эллиптические кривые.

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: экзамен

Основная литература.

1. Мартынов Л.М. Алгебра и теория чисел для криптографии: учебное пособие [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/140740>

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/reader/book/68466/>

Дополнительная литература.

1. Виноградов И.М. Основы теории чисел. 14-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/139285>
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: <https://e.lanbook.com/reader/book/70724>

Автор РПД

Рожков А.В., доктор физ.-мат. наук, профессор.