

АННОТАЦИЯ
дисциплины «Б1.В.ДВ.01.01 АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ АЛГЕБРЫ»

Объем трудоемкости: 2 зачетные единицы (72 часа, из них – 40,2 часа контактной работы (14 часов лекций, 26 часов лабораторных занятий, 0,2 часа ИКР); 31,8 часов 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 «алгоритмические проблемы алгебры» относится к блоку Б1 Дисциплины (модули) и является дисциплиной по выбору.

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-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	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.
2.	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах			

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.		4		8	8
2	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.		4		8	8
3	Целочисленная арифметика. Полиномиальная арифметика. Китайская теорема об остатках. Мультипликативные группы конечных полей.		2		4	8
4	Дискретное преобразование Фурье. Быстрое преобразование Фурье. Сложность умножения двух многочленов. Умножение матриц. Метод Штрассена.		4		6	7,8
	Итого по дисциплине:		14		26	31,8

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Шевелев Ю.П. Дискретная математика, 3-е изд. [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/book/107270>
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: <https://e.lanbook.com/book/67458>

Дополнительная литература:

1. Ерусалимский Я.М. Дискретная математика. Теория и практикум [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/book/106869>
2. Тропин М.П. Основы прикладной алгебры [Электронный ресурс]. - СПб.: Лань, 2017. - URL: <https://e.lanbook.com/book/94747>

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/>

Автор РПД, д.ф.-м.н., профессор

Рожков А.В.