

## АННОТАЦИЯ

дисциплины Б1.В.05 «АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА»

**Объем трудоемкости:** 2 зачетные единицы (72 часа, из них – 22,2 часа контактной работы (10 часа лекций, 12 часов практических занятий, 0,2 часа ИКР); 49,8 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 «Алгебраическая алгоритмика» относится к вариативной части блока Б1 Дисциплины (модули) и является обязательной дисциплиной.

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 компетенций ПК-1, ПК-4:

№ 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	Основные теоремы алгебры, теории чисел и других разделов теоретической математики	Применять стандартные алгоритмы фундаментальной и прикладной математики	Методами анализа математических Моделей, возникающих в области информационных технологий и защиты информации
2.	ПК-4	Способностью к применению методов математического и алгоритмического моделирования при решении теоретических и	О компьютерной реализации информационных объектов. Связи компьютерной ал-	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		прикладных задач	гебры и численного анализа.		области символьных вычислений.

**Основные разделы дисциплины:**

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Присваивание. Последовательность. Цикл. Альтернатива. Рекурсия. Быстрый алгоритм возведения в степень. Работа с матрицами.	21,8	4	4		13,8
2	Арифметика целых чисел. Работа с большими числами. Наибольший общий делитель. Алгоритмы факторизации.	18	2	4		12
3	Евклидовы кольца. Неприводимые многочлены. Конечные кольца.	16	2	2		12
4	Китайская теорема об остатках. Вычисления в кольцах вычетов. Функция Эйлера. Дискретное преобразование Фурье.	16	2	2		12
	<b>Итого по дисциплине:</b>	<b>22</b>	<b>10</b>	<b>12</b>		<b>49,8</b>

**Курсовые работы:** не предусмотрены.

**Форма проведения аттестации по дисциплине:** зачет

**Основная литература:**

1. Шевелев Ю.П. Дискретная математика, 6-е изд. [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/book/107270>
2. Ерусалимский Я.М. Дискретная математика. Теория и практикум [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/book/106869>

**Дополнительная литература:**

1. 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>
2. Кожухов С.Ф., Совертков П.И. Сборник задач по дискретной математике, 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/book/102606>
3. Окулов С.М. Программирование в алгоритмах, 6-е изд. [Электронный ресурс]. – М.: Бинوم. 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 8.9. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r10p2. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GT 2.11. Официальный сайт <http://pari.math.u-bordeaux.fr/>

Автор РПД

Рожков А.В.