



**Аннотация по дисциплине
Б1.В.ДВ.03.02 «ПРИКЛАДНАЯ АЛГЕБРА»**

Направление подготовки/специальность

02.03.02 Фундаментальная информатика и информационные технологии

Курс 3 Семестр 6 Количество з.е. 3

Объем трудоемкости: 3 зачетных единиц (108 часа, из них – 64 часа аудиторной нагрузки: лекционных 32 ч., лабораторных работ - 32 ч., 39,8 часов самостоятельной работы, 4 часов КСР, 0,2 часа ИКР).

Цель дисциплины:

Целью преподавания и изучения дисциплины Б1.В.ДВ.03.02 «Прикладная алгебра» является овладение студентами математическим аппаратом, применяемым в фундаментальной математике и информатике, и служащим основой для разработки информационных технологий.

При освоении дисциплины «Прикладная алгебра» вырабатывается: умение логически мыслить, проводить доказательство основных утверждений, устанавливать логические связи между понятиями.

Целью освоения прикладных разделов дисциплины является освоение студентами методов решения практически ориентированных задач в различных отраслях жизнедеятельности с использованием: кольца и поля, линейных кодов, циклических кодов, алгебраической полиграфии, элементов теории групп, блок-схем, систем Штейнера и так называемых латинских квадратов.

Задачи дисциплины.

Задачами изучения дисциплины «Прикладная алгебра» является реализация требований, установленных федеральными государственными образовательными стандартами высшего профессионального образования к уровню подготовки бакалавров по направлению «Фундаментальная информатика и информационные технологии (информатика и компьютерные науки)». Следует различать следующие задачи изучения дисциплины:

1. Дать студентам основы знаний по прикладной алгебре;
2. Научить применять алгебру в прикладных областях;
3. Показать связь прикладной алгебры с информатикой.

Место дисциплины в структуре образовательной программы

Дисциплина «Прикладная алгебра» относится к дисциплинам по выбору базовой части ООП. Для изучения дисциплины необходимо знание курсов алгебры, дискретной математики, основ программирования, курса распределенных задач и алгоритмов. Знания, получаемые при изучении курса, используются при изучении программистских дисциплин профессионального цикла учебного плана бакалавра.

Место курса в профессиональной подготовке бакалавра определяется ролью алгебры в формировании высококвалифицированного специалиста по направлению «Фундаментальные информатика и информационные технологии (вычислительные технологии)».

Результаты обучения (знания, умения, опыт, компетенции)

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине (<i>знает, умеет, владеет (навыки и/или опыт деятельности)</i>)
ПК-1. Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	
ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	Знает основы теории групп и конечных полей, линейные и циклические коды, принципы построения криптосистем.
ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	Умеет применять теорию групп и конечных полей для разработки криптографических протоколов
ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области информационных технологий.	Имеет практический опыт реализации и анализа криптографических алгоритмов
ПК-2 Способен проводить под научным руководством локальные исследования на основе существующих методов в конкретной области профессиональной деятельности	
ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке	Знает методы анализа научных источников, владеет методами подготовки научных обзоров по тематике прикладной алгебры

Код и наименование индикатора*	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-2.2 Умеет решать научные задачи в связи с поставленной целью и в соответствии с выбранной методикой	Умеет решать стандартные задачи прикладной алгебры
ПК-2.3 Имеет практический опыт выступлений и научной аргументации при анализе объекта научной и профессиональной деятельности	Имеет практический опыт выступлений и научной аргументации при анализе задач прикладной алгебры

Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 6 семестре (очная форма)

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ЛР	КСР	
1	2	3	4	5	6	7
1	Кольца и поля	14	4	4		6
2	Линейные коды	20	6	6	2	6
3	Циклические коды	14	4	4	2	4
4	Алгебраическая полиграфия	20	6	6		8
5	Элементы теории групп	12	4	4		4
6	Основы теории полей	14	4	4		6
7	Блок-схемы	13,8	4	4		5,8
	ИКР	0,2				
	Итого:	108	32	32	4	39,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, КСР – самостоятельная работа студента

Курсовые работы:

Не предусмотрены.

Вид аттестации

Зачет в шестом семестре.

Основная литература:

1. Рацеев, С. М. Реализации некоторых криптосистем и корректирующих кодов / С. М. Рацеев. — Санкт-Петербург : Лань, 2024. — 288 с. — ISBN 978-5-507-

- 47919-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/356009?category=1545>
2. Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 456 с. — ISBN 978-5-507-48774-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/362942?category=1545>
3. Введение в теоретико-числовые методы криптографии : учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 396 с. — ISBN 978-5-507-47610-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/397286?category=1545>
4. Рацеев, С. М. Элементы высшей алгебры и теории кодирования / С. М. Рацеев. — 2-е изд., испр. и доп. — Санкт-Петербург : Лань, 2023. — 684 с. — ISBN 978-5-507-47915-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/336809?category=1545>
5. Рацеев, С. М. Математические методы защиты информации и их основы. Сборник задач / С. М. Рацеев. — Санкт-Петербург : Лань, 2023. — 140 с. — ISBN 978-5-507-45198-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/292910?category=1545>