

УТВЕРЖДАЮ
Проректор по УМР

_____ Е.В. Коновалова

15 июня 2023 г., протокол УМС №5

МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНЫХ ДИСЦИПЛИН

Алгебраические структуры

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Прикладной математики
Учебный план	b010302-ТехнолПрог-23-1.plx Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА Направленность (профиль): Технологии программирования и анализ данных
Квалификация	бакалавр
Форма обучения	очная
Общая трудоемкость	4 ЗЕТ

Часов по учебному плану	144
в том числе:	
аудиторные занятия	64
самостоятельная работа	53
часов на контроль	27

Виды контроля в семестрах:
экзамены 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		Итого	
	17 2/6			
Неделя	уп	рп	уп	рп
Лекции	32	32	32	32
Практические	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	53	53	53	53
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Программу составил(и):

к.ф.-м.н., доцент, Гореликов А.В.

Рабочая программа дисциплины

Алгебраические структуры

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

Направленность (профиль): Технологии программирования и анализ данных

утвержденного учебно-методическим советом вуза от 15.06.2023 протокол № 5.

Рабочая программа одобрена на заседании кафедры

Прикладной математики

Зав. кафедрой доцент, к.ф.-м.н., Гореликов Андрей Вячеславович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Формирование у обучающихся фундаментальных знаний основ теории алгебраических структур, её методов и приложений.
1.2	Формирование у обучающихся умений и навыков применения полученных знаний при решении прикладных задач.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.О.04
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Алгоритмы и структуры данных
2.1.2	Математическая логика и теория алгоритмов
2.1.3	Комбинаторика и теория графов
2.1.4	Математический анализ
2.1.5	Алгебра и геометрия
2.1.6	Дискретная математика
2.1.7	Программирование
2.1.8	Введение в профессиональную деятельность
2.1.9	Информатика
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Базы данных
2.2.2	Численные методы
2.2.3	Искусственный интеллект
2.2.4	Методы машинного обучения
2.2.5	Учебная практика, научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
2.2.6	Анализ данных
2.2.7	Математическое моделирование
2.2.8	Методы защиты информации
2.2.9	Производственная практика, научно-исследовательская работа
2.2.10	Финансовая математика
2.2.11	Выполнение и защита выпускной квалификационной работы
2.2.12	Подготовка к сдаче и сдача государственного экзамена
2.2.13	Производственная практика, преддипломная практика
2.2.14	Теория игр и исследование операций

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-2.1: Демонстрирует знание и понимание существующих математических методов и алгоритмов решения прикладных задач

ОПК-5.1: Демонстрирует знание алгоритмов решения типовых задач, области и способов их практического применения

ОПК-5.2: Разрабатывает алгоритмы решения практических задач, при необходимости используя стандартные методы и приемы формализации и алгоритмизации

ОПК-5.3: Разрабатывает компьютерные программы, пригодные для практического применения

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Основы теории алгебраических структур, её методы и алгоритмы, области приложения и способы практического применения.
3.2	Уметь:
3.2.1	Демонстрировать знание и понимание методов и алгоритмов решения прикладных задач в рамках теории алгебраических структур.
3.2.2	Применять полученные знания при решении типовых прикладных задач теории алгебраических структур.
3.2.3	Использовать методы и приемы формализации и алгоритмизации при разработке алгоритмов решения практических задач и компьютерных программ, пригодных для практического применения.
3.3	Владеть:
3.3.1	Навыками решения типовых задач теории алгебраических структур, возникающих при разработке и реализации алгоритмов решения прикладных задач.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Введение. Алгебраические системы					
1.1	Множества и отображения. Алгебраические операции. Определение алгебраической системы. Гомоморфизм. Изоморфизм. Определения основных алгебраических структур. /Лек/	5	2	ОПК-2.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Л2.7	
1.2	Множества и отображения. Алгебраические операции. Определение алгебраической системы. Гомоморфизм. Изоморфизм. Определения основных алгебраических структур. /Пр/	5	2	ОПК-2.1	Л1.1 Л1.2 Л1.3Л2.7Л3.5 Э1 Э2	
1.3	Множества и отображения. Алгебраические операции. Определение алгебраической системы. Гомоморфизм. Изоморфизм. Определения основных алгебраических структур. /Ср/	5	3	ОПК-2.1	Л1.3Л2.3Л3.5 Э1 Э2	
	Раздел 2. Группы					
2.1	Основные свойства групп. Изоморфизм групп. Циклические группы. Группа подстановок. Автоморфизмы групп. Гомоморфизмы групп. Подгруппы. Смежные классы. Нормальные делители. Факторгруппы. Действия групп на множествах. Разрешимые группы. Произведение групп. Образующий элемент. Группы преобразований. Представления групп. /Лек/	5	10	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.3 Л2.5 Л2.6	
2.2	Основные свойства групп. Изоморфизм групп. Циклические группы. Группа подстановок. Автоморфизмы групп. Гомоморфизмы групп. Подгруппы. Смежные классы. Нормальные делители. Факторгруппы. Действия групп на множествах. Разрешимые группы. Произведение групп. Образующий элемент. Группы преобразований. Представления групп. /Пр/	5	10	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.5 Л2.6Л3.3 Л3.4 Э1 Э2	

2.3	Основные свойства групп. Изоморфизм групп. Циклические группы. Группа подстановок. Автоморфизмы групп. Гомоморфизмы групп. Подгруппы. Смежные классы. Нормальные делители. Факторгруппы. Действия групп на множествах. Разрешимые группы. Произведение групп. Образующий элемент. Группы преобразований. Представления групп. /Ср/	5	15	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Л2.5 Л2.6 Л2.7Л3.3 Л3.4 Л3.5 Э1 Э2	
Раздел 3. Кольца и поля						
3.1	Определение, свойства, примеры. Кольцо классов вычетов. Гомоморфизм и идеалы колец. Факторкольцо. Делители нуля. Поле. Характеристика поля. Поле комплексных чисел. Кольцо многочленов. Делитель. НОД и НОК. Евклидовы кольца. Корни многочленов. Формулы Виета. Симметрические многочлены. Определитель Вандермонда. Дискриминант многочлена. Результант. Алгебраическая замкнутость поля. Корни многочленов. Основная теорема алгебры. Локализация корней. Векторное пространство. Алгебры над полем. /Лек/	5	10	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Л2.5 Л2.7	
3.2	Определение, свойства, примеры. Кольцо классов вычетов. Гомоморфизм и идеалы колец. Факторкольцо. Делители нуля. Поле. Характеристика поля. Поле комплексных чисел. Кольцо многочленов. Делитель. НОД и НОК. Евклидовы кольца. Корни многочленов. Формулы Виета. Симметрические многочлены. Определитель Вандермонда. Дискриминант многочлена. Результант. Алгебраическая замкнутость поля. Корни многочленов. Основная теорема алгебры. Локализация корней. Векторное пространство. Алгебры над полем. /Пр/	5	10	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.7Л3.5 Л3.6 Э1 Э2	
3.3	Определение, свойства, примеры. Кольцо классов вычетов. Гомоморфизм и идеалы колец. Факторкольцо. Делители нуля. Поле. Характеристика поля. Поле комплексных чисел. Кольцо многочленов. Делитель. НОД и НОК. Евклидовы кольца. Корни многочленов. Формулы Виета. Симметрические многочлены. Определитель Вандермонда. Дискриминант многочлена. Результант. Алгебраическая замкнутость поля. Корни многочленов. Основная теорема алгебры. Локализация корней. Векторное пространство. Алгебры над полем. /Ср/	5	15	ОПК-2.1 ОПК-5.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.7Л3.5 Л3.6 Э1 Э2	
3.4	Группы, кольца, поля. /Контр.раб./	5	0	ОПК-2.1 ОПК-5.1		

	Раздел 4. Приложения алгебраических структур					
4.1	<p>Алгебраические структуры в криптографии.</p> <p>Основные понятия криптографии.</p> <p>Симметричные криптосистемы.</p> <p>Аффинный шифр. Шифр Хилла.</p> <p>Проблема дискретного логарифмирования. Схема Диффи-Хеллмана. Схема Эль-Гамала.Хэширование.</p> <p>Алгебраические структуры в теории кодирования.</p> <p>Схема передачи данных по каналу с шумом. Типы кодов. Проверочная матрица линейного кода.</p> <p>Порождающая матрица линейного кода.</p> <p>Минимальное расстояние линейного кода. Декодирование линейных кодов.</p> <p>Общие свойства линейных кодов. Коды Хэмминга. Дуальный код и тождество Мак-Вильямс. /Лек/</p>	5	10	ОПК-5.1 ОПК-5.2 ОПК-5.3	Л1.1 Л1.2 Л1.3Л2.5 Л2.7	
4.2	<p>Алгебраические структуры в криптографии.</p> <p>Основные понятия криптографии.</p> <p>Симметричные криптосистемы.</p> <p>Аффинный шифр. Шифр Хилла.</p> <p>Проблема дискретного логарифмирования. Схема Диффи-Хеллмана. Схема Эль-Гамала.Хэширование.</p> <p>Алгебраические структуры в теории кодирования.</p> <p>Схема передачи данных по каналу с шумом. Типы кодов. Проверочная матрица линейного кода.</p> <p>Порождающая матрица линейного кода.</p> <p>Минимальное расстояние линейного кода. Декодирование линейных кодов.</p> <p>Общие свойства линейных кодов. Коды Хэмминга. Дуальный код и тождество Мак-Вильямс. /Пр/</p>	5	10	ОПК-5.1 ОПК-5.2 ОПК-5.3	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.5 Л2.7Л3.1 Л3.2 Л3.3 Э1 Э2	
4.3	<p>Алгебраические структуры в криптографии.</p> <p>Основные понятия криптографии.</p> <p>Симметричные криптосистемы.</p> <p>Аффинный шифр. Шифр Хилла.</p> <p>Проблема дискретного логарифмирования. Схема Диффи-Хеллмана. Схема Эль-Гамала.Хэширование.</p> <p>Алгебраические структуры в теории кодирования.</p> <p>Схема передачи данных по каналу с шумом. Типы кодов. Проверочная матрица линейного кода.</p> <p>Порождающая матрица линейного кода.</p> <p>Минимальное расстояние линейного кода. Декодирование линейных кодов.</p> <p>Общие свойства линейных кодов. Коды Хэмминга. Дуальный код и тождество Мак-Вильямс. /Ср/</p>	5	20	ОПК-5.1 ОПК-5.2 ОПК-5.3	Л1.1 Л1.2 Л1.3Л2.5 Л2.7Л3.1 Л3.2	

4.4	/Экзамен/	5	27	ОПК-2.1 ОПК-5.1 ОПК-5.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Л2.5 Л2.6 Л2.7Л3.1 Л3.4 Л3.6 Э1 Э2	
-----	-----------	---	----	-------------------------------	---	--

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлены отдельным документом

5.2. Оценочные материалы для диагностического тестирования

Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Ермолаева Н. Н.	Практические занятия по алгебре. Элементы теории множеств, теории чисел, комбинаторики. Алгебраические структуры	Москва: Лань", 2014, электронный ресурс	1
Л1.2	Зяблицева Л.В., Корабельщикова С.Ю., Кузнецова И.В., Тихомиров С.А.	Алгебраические структуры и их приложения: учебное пособие	Москва: САФУ, 2015, электронный ресурс	2
Л1.3	Иванов А. Н.	Основные алгебраические структуры: учебное пособие	Москва: НИЯУ МИФИ, 2010, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Бурбаки Н.	Алгебра: Алгебраические структуры. Линейная и полилинейная алгебра	М.: Физматлит, 1962	1
Л2.2	Аграновский А. В., Хади Р. А.	Практическая криптография. Алгоритмы и их программирование: учебное пособие	Москва: СОЛОН-ПРЕСС, 2009, электронный ресурс	1
Л2.3	Лыткина Д.В., Храмова Т.В.	Алгебраические структуры: учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2016, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4	Сидельников В. М.	Теория кодирования: ВО - Бакалавриат	Москва:  издательская фирма "Физико-математическая литература" (Ф  ЗМАТЛ  Т), 2008, электронный ресурс	1
Л2.5	Ларин С. В.	Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие для вузов	Москва: Юрайт, 2022, электронный ресурс	1
Л2.6	Курош А. Г.	Теория групп	Санкт-Петербург: Лань, 2021, электронный ресурс	1
Л2.7	Ряднов А. В., Меренкова Т. В., Трубаев В. В.	Алгебраические системы: учебное пособие для студентов специальности «компьютерная безопасность»	Москва: РУТ (МИИТ), 2019, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Авдошин С.М., Набебин А.А.	Дискретная математика. Модулярная алгебра, криптография, кодирование: учебно-методическое пособие	Москва: ДМК-пресс, 2017, электронный ресурс	2
Л3.2	Бахаров, Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография): практикум	Москва: Издательский Дом МИСиС, 2019, электронный ресурс	1
Л3.3	Скворцова М. И., Ожерелкова Л. М.	Основы теории групп: учебно-методическое пособие	Москва: РТУ МИРЭА, 2020, электронный ресурс	1
Л3.4	Ряднов А. В., Меренкова Т. В., Трубаев В. В.	Теория групп: Практикум	Москва: РУТ (МИИТ), 2020, электронный ресурс	1
Л3.5	Красовская Т. Ф., Плотников П. В., Киселева А. В.	Высшая математика. Бинарные отношения. Алгебраические структуры: учебно-методическое пособие по выполнению самостоятельной работы	Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2021, электронный ресурс	1
Л3.6	Ряднов А. В., Меренкова Т. В., Булатникова М. Е.	Алгебраические системы кольца и поля: учебно-методическое пособие для студентов специальности «компьютерная безопасность»	Москва: РУТ (МИИТ), 2021, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека
Э2	Общероссийский математический портал Math-Net.Ru — современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России

6.3.1 Перечень программного обеспечения

6.3.1.1	Операционная система Microsoft Windows, пакет прикладных программ Microsoft Office.
---------	---

6.3.2 Перечень информационных справочных систем

6.3.2.1	«Национальная электронная библиотека» нэб.рф
6.3.2.2	Гарант-информационно-правовой портал. http://www.garant.ru/
6.3.2.3	КонсультантПлюс – надежная правовая поддержка. http://www.consultant.ru/
6.3.2.4	Электронные книги Springer Nature (Science, Technology and Medicine Collections) https://link.springer.com/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых и индивидуальных консультаций, укомплектованные специализированной мебелью и техническими средствами обучения (доска, экран (стационарный или переносной), проектор (стационарный или переносной)). Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечения доступа в электронную информационно- образовательную среду организации.
-----	--