

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»

Физико-математический факультет
Кафедра алгебры и геометрии

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев
«30» апреля 2025 г., протокол № 8

Рабочая программа дисциплины

Прикладная алгебра

(наименование дисциплины (модуля))

Направление подготовки

01.03.02 «Прикладная математика и информатика»

(шифр, название направления)

Направленность (профиль):

«Общий профиль: прикладная математика и информатика»

Квалификация выпускника

бакалавр

Форма обучения

очная

Год начала подготовки - **2023**

Программу составила: канд. физ.-мат. наук, доцент кафедры алгебры и геометрии
Кубекова Б.С.

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденным приказом Министерства образования и науки Российской Федерации от 10.01.2018 № 9 с изменениями и дополнениями от 26.11.2020 г., №1456, 8.02.2021 г., №83, образовательной программой высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика, направленность (профиль): «Общий профиль: прикладная математика и информатика»; локальными актами КЧГУ.

Рабочая программа рассмотрена и утверждена на заседании кафедры алгебры и геометрии на 2025-2026 учебный год, протокол **№ 8 от 10 апреля 2025г.**

Оглавление

1. Наименование дисциплины (модуля).....	4
2. Место дисциплины (модуля) в структуре образовательной программы.....	4
3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.....	4
4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.....	5
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	6
6. Основные формы учебной работы и образовательные технологии, используемые при реализации образовательной программы.....	8
7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю).....	9
7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.....	9
7.2. Перевод балльно-рейтинговых показателей оценки качества подготовки обучающихся в отметки традиционной системы оценивания	11
7.3. Типовые контрольные вопросы и задания, необходимые для оценивания сформированности компетенций в процессе освоения учебной дисциплины	11
7.3.1. Примерные вопросы к итоговой аттестации (экзамен).....	11
7.3.2. Тестовые задания для проверки знаний студентов.....	13
7.3.3. Типовые задания к контрольным работам.....	13
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).....	14
8.1. Основная литература	14
8.2. Дополнительная литература	14
9. Требования к условиям реализации рабочей программы дисциплины (модуля).....	15
9.1. Общесистемные требования	15
9.2. Материально-техническое и учебно-методическое обеспечение дисциплины.....	16
9.3. Необходимый комплект лицензионного программного обеспечения	16
9.4. Современные профессиональные базы данных и информационные справочные системы	16
10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья.....	17
11. Лист регистрации изменений.....	18

1. Наименование дисциплины (модуля)

Прикладная алгебра

Целью изучения дисциплины является формирование систематизированных знаний в области алгебры и ее приложения. Теоретическое освоение обучающимися основных разделов алгебры, необходимых для понимания ее роли в профессиональной деятельности; формирования культуры мышления, способности к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения; освоения основных методов алгебры, применяемых в решении профессиональных задач и научно-исследовательской деятельности. Одной из основных целей курса является знакомство студентов с основными конструкциями абстрактной алгебры, теории кодирования и криптографии.

Для достижения цели ставятся задачи:

1. получить представление о роли математики в профессиональной деятельности;
2. изучить необходимый понятийный аппарат дисциплины;
3. сформировать умения доказывать теоремы;
4. получить необходимые знания из области алгебры для дальнейшего самостоятельного освоения научно-технической информации.
5. получить представление об основных алгебраических структурах, используемых в перечислительных и алгоритмических задачах, в том числе о конечных группах.
6. изучить конструкции основных типов линейных кодов и знать алгоритмы декодирования некоторых кодов.
7. изучить понятие группы точек эллиптической кривой и понимать, как эта группа используется в криптографии.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.ДВ.12.01 «Прикладная алгебра» относится к дисциплинам по выбору и изучается на 4 курсе в 7 семестре.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО	
Индекс	Б1.В.ДВ.12.01
Требования к предварительной подготовке обучающегося:	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по элементарной математике, алгебре, функциональному анализу.	
Знания полученные по дисциплине используются в последующих курсах. На основе знания, умения и владения прикладной алгеброй студенты изучают математические дисциплины в магистратуре.	

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций обучающегося

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ ОП ВО	Индикаторы достижения компетенций
-----------------	--	-----------------------------------

УК-1.	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности УК-1.3. Владеет навыками работы с информационными объектами и сетью Интернет, опытом научного поиска, опытом библиографического поиска
ПК-2.	Способен понимать, совершенствовать и применять современный математический аппарат	ПК-2.1. Знает принципы построения и методы исследования математических моделей объектов различной природы. ПК-2.2. Умеет использовать и модифицировать существующие математические методы для решения прикладных задач. ПК-2.3. Владеет навыками использования математического аппарата при решении прикладных задач.

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины (модуля) составляет 4 зачетные единицы (ЗЕТ), 144 академических часа.

Объем дисциплины	Всего часов	
	для очной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	144	-
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)		
Аудиторная работа (всего):	72	
в том числе:		
лекции	36	
семинары, практические занятия	36	
практикумы		
лабораторные работы		
Внеаудиторная работа:		
В том числе, индивидуальная работа обучающихся с преподавателем:		
курсовое проектирование		
Консультация перед экзаменом		
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем, творческую работу (эссе), рефераты, контрольные работы и др.		
Самостоятельная работа обучающихся (всего)	72	
Контроль самостоятельной работы		
Вид промежуточной аттестации обучающегося (зачет / экзамен)	Экзамен	

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

Очная форма обучения

№ п/п	Раздел дисциплины	Об- щая тру- доем- кость (в ча- сах)	Виды учебных занятий, включая самостоятель- ную работу обучаю- щихся и трудоемкость (в часах)			
			Аудиторные уч. занятия			Самост. работа
			Лек	Пр	Лаб	
	Раздел 1. Группы, кольца, поля.					
1.1	<i>Группы</i> Определения и свойства. Симметрическая группа Группы симметрии Подгруппы и Смежные классы Изоморфизмы групп Теорема Кэли Циклические группы и их свойства Теорема Лагранжа и следствия из нее.	7	2	2		3
1.2	<i>Кольца и поля</i> Кольца. Определение и свойства Ассоциативные кольца Изоморфизмы колец Идеалы кольца и факторкольца Класс вычетов по модулю идеала кольца Евклидовы кольца. Поле, свойства поля	7	2	2		3
	Раздел 2. Конечные поля					
2.1	<i>Поля вычетов.</i> Характеристика поля. Мультипликативная группа и примитивный элемент конечного поля. Деление в кольце многочленов.	7	2	2		3
2.2	<i>Неприводимые многочлены.</i> Теорема о существовании неприводимых многочле- нов. Расширения простых полей	7	2	2		3
2.3	<i>Вычисления в конечных полях</i> Алгоритм Евклида. Расширенный алгоритм Евклида	7	2	2		3
2.4	<i>Алгебра векторов над конечным полем</i> Векторное пространство Представление элементов конечных полей	7	2	2		3
2.5	<i>Минимальные и примитивные многочлены</i> Минимальный многочлен. Примитивные многочлены. Свойства минимальных многочленов.	7	2	2		3
2.6	<i>Корни многочленов над конечным полем</i> Свойства многочленов над конечным полем.	7	2	2		3

	Нахождение корней неприводимого многочлена					
2.7	Вычисления в мультипликативной группе. Вычисления в мультипликативной группе расширения поля Нахождение минимальных многочленов	7	2	2		3
2.8	Существование и единственность поля $GF(p^n)$ Существование и единственность поля $GF(p^n)$ для всех p Среднее число неприводимых нормированных многочленов Функция Мебиуса	7	2	2		3
2.9	Циклические пространства Нормированный делитель порождающего элемента идеала Циклическое пространство. Примитивные корни, т.е. корни из 1.	7	2	2		3
	Раздел 3 Коды, исправляющие ошибки					
3.1	Блочное кодирование. Задача помехоустойчивого кодирования Понятия, связанные с булевым кубом Кодовое расстояние Блочное кодирование и декодирование.	7	2	2		3
3.2	Коды Хэмминга Теорема Хэмминга Код Голея	7	2	2		3
3.3	Линейные коды. Определения и свойства Порождающая и проверочная матрицы	8	2	2		4
3.4	Кодирование линейными кодами Систематическое кодирование. Проверочная матрица Кодирования блочным линейным кодом Систематическое и несистематическое кодирование	8	2	2		4
3.5	Декодирование линейных кодов Тривиальный метод Декодирование по синдрому Декодирование кода Хэмминга Резюме	8	2	2		4
3.6	Циклические коды Определение и построение циклических кодов Полиномиальное представление слов Кодирование циклическими кодами Декодирование циклических кодов Резюме	8	2	2		4
3.7	Коды БЧХ Определение и основное свойство БХЧ-кодов Циклотомический класс элемента пол. Свойства классов. БХЧ коды: синдромы	6	2			4
3.8	Построение БЧХ-кодов Алгоритм построения Декодирование БХЧ	6		2		4
3.9	Коды Рида-Соломона	3				3
	Раздел 4. Теория перечисления Поля					
4.1	Действие группы на множестве Фиксатор перестановки и стабилизатор элемента множества	3				3

4.2	Лемма Бернсайда Цикловой индекс Задачи на применение циклового индекса Применение теоремы Пойя для решения комбинаторных задач	3				3
	Экзамен					
	Всего	144	36	36		72

6. Основные формы учебной работы и образовательные технологии, используемые при реализации образовательной программы

Лекционные занятия. Лекция является основной формой учебной работы в вузе, она является наиболее важным средством теоретической подготовки обучающихся. На лекциях рекомендуется деятельность обучающегося в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции. Основная дидактическая цель лекции - обеспечение ориентировочной основы для дальнейшего усвоения учебного материала. Лекторами активно используются: лекция-диалог, лекция - визуализация, лекция - презентация. Лекция - беседа, или «диалог с аудиторией», представляет собой непосредственный контакт преподавателя с аудиторией. Ее преимущество состоит в том, что она позволяет привлекать внимание слушателей к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей аудитории. Участие обучающихся в лекции – беседе обеспечивается вопросами к аудитории, которые могут быть как элементарными, так и проблемными.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Рекомендуется на первой лекции довести до внимания студентов структуру дисциплины и его разделы, а в дальнейшем указывать начало каждого раздела (модуля), суть и его задачи, а, закончив изложение, подводить итог по этому разделу, чтобы связать его со следующим. Содержание лекций определяется настоящей рабочей программой дисциплины. Для эффективного проведения лекционного занятия рекомендуется соблюдать последовательность ее основных этапов:

1. формулировку темы лекции;
2. указание основных изучаемых разделов или вопросов и предполагаемых затрат времени на их изложение;
3. изложение вводной части;
4. изложение основной части лекции;
5. краткие выводы по каждому из вопросов;
6. заключение;
7. рекомендации литературных источников по излагаемым вопросам.

Практические занятия. Дисциплины, по которым планируются практические занятия, определяются учебными планами. Практические занятия относятся к основным видам учебных занятий и составляют важную часть теоретической и профессиональной практической подготовки. Выполнение студентом практических занятий направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплин математического и общего естественно-научного, общепрофессионального и профессионального циклов;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива. Методические рекомендации разработаны с целью единого подхода к организации и проведению практических занятий.

Практическое занятие — это форма организации учебного процесса, направленная на выработку у студентов практических умений для изучения последующих дисциплин (модулей) и для решения профессиональных задач. Практическое занятие должно проводиться в учебных кабинетах или специально оборудованных помещениях. Необходимыми структурными элементами практического занятия, помимо самостоятельной деятельности студентов, являются анализ и оценка выполненных работ и степени овладения студентами запланированными умениями. Дидактические цели практических занятий: формирование умений (аналитических, проектировочных, конструктивных), необходимых для изучения последующих дисциплин (модулей) и для будущей профессиональной деятельности.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Образовательные технологии. При проведении учебных занятий по дисциплине используются традиционные и инновационные, в том числе информационные образовательные технологии, включая при необходимости применение активных и интерактивных методов обучения.

Традиционные образовательные технологии реализуются, преимущественно, в процессе лекционных и практических занятий. Инновационные образовательные технологии используются в процессе аудиторных занятий и самостоятельной работы студентов в виде применения активных и интерактивных методов обучения. Информационные образовательные технологии реализуются в процессе использования электронно-библиотечных систем, электронных образовательных ресурсов и элементов электронного обучения в электронной информационно-образовательной среде для активизации учебного процесса и самостоятельной работы студентов.

Практические занятия могут проводиться в форме групповой дискуссии, «мозговой атаки», разборка кейсов, решения практических задач, публичная презентация проекта и др. Прежде, чем дать группе информацию, важно подготовить участников, активизировать их ментальные процессы, включить их внимание, развивать кооперацию и сотрудничество при принятии решений.

7. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модюлю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Компетенции	Высокий уровень (отлично) (86-100% баллов)	Средний уровень (хорошо) (71-85% баллов)	Низкий уровень (удовлетворительно) (56-70% баллов)	Ниже порогового уровня (не удовлетворительно) (до 55 % баллов)
--------------------	---	---	---	---

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. В полном объеме знает принципы сбора, отбора и обобщения информации	УК-1.1. Знает принципы сбора, отбора и обобщения информации	УК-1.1. В целом знает принципы сбора, отбора и обобщения информации	УК-1.1. Не знает принципы сбора, отбора и обобщения информации
	УК-1.2. В полном объеме умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	УК-1.2. В полном объеме умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	УК-1.2. Не умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности
	УК-1.3. В полном объеме владеет навыками работы с информационными объектами и сетью Интернет, опытом научного поиска, опытом библиографического поиска	УК-1.3. Владеет навыками работы с информационными объектами и сетью Интернет, опытом научного поиска, опытом библиографического поиска	УК-1.3. В полном объеме владеет навыками работы с информационными объектами и сетью Интернет, опытом научного поиска, опытом библиографического поиска	УК-1.3. Не владеет навыками работы с информационными объектами и сетью Интернет, опытом научного поиска, опытом библиографического поиска
ПК-2. Способен понимать, совершенствовать и применять современный математический аппарат	ПК-2.1. В полном объеме знает принципы построения и методы исследования математических моделей объектов различной природы	ПК-2.1. Знает принципы построения и методы исследования математических моделей объектов различной природы	ПК-2.1. В целом знает принципы построения и методы исследования математических моделей объектов различной природы	ПК-2.1. Не знает принципы построения и методы исследования математических моделей объектов различной природы
	ПК-2.2. В полном объеме умеет использовать и модифицировать существующие математические методы для решения прикладных задач	ПК-2.2. Умеет использовать и модифицировать существующие математические методы для решения прикладных задач	ПК-2.2. В целом умеет использовать и модифицировать существующие математические методы для решения прикладных задач	ПК-2.2. Не умеет использовать и модифицировать существующие математические методы для решения прикладных задач
	ПК-2.3. В полном объеме владеет навыками использования математического аппарата	ПК-2.3. Владеет навыками использования математического аппарата	ПК-2.3. В целом владеет навыками использования математического аппарата	ПК-2.3. Не владеет навыками использования математического аппарата при решении

математического аппарата при решении прикладных задач	та при решении прикладных задач	парата при решении прикладных задач	прикладных задач
---	---------------------------------	-------------------------------------	------------------

7.2. Перевод балльно-рейтинговых показателей оценки качества подготовки обучающихся в отметки традиционной системы оценивания

Порядок функционирования внутренней системы оценки качества подготовки обучающихся и перевод балльно-рейтинговых показателей обучающихся в отметки традиционной системы оценивания проводится в соответствии с положением КЧГУ «Положение о балльно-рейтинговой системе оценки знаний обучающихся», размещенным на сайте Университета по адресу: <https://kchgu.ru/inye-lokalnye-akty/>

7.3. Типовые контрольные вопросы и задания, необходимые для оценивания сформированности компетенций в процессе освоения учебной дисциплины

7.3.1. Примерные вопросы к итоговой аттестации (экзамен)

1. Определения и свойства групп.
2. Таблица Кэли.
3. Симметрическая группа.
4. Группы самосовмещений.
5. Подгруппы и смежные классы.
6. Изоморфизм групп. Теорема Кэли.
7. Циклические группы и их свойства.
8. Функция Эйлера.
9. Теорема Лагранжа и ее свойства.
10. Определение и основные свойства кольца.
11. Гомоморфизм колец.
12. Идеалы колец и их свойства.
13. Факторкольца.
14. Евклидовы кольца.
15. Поля.
16. Характеристика поля.
17. Мультипликативная группа и примитивный элемент конечного поля.
18. Деление в кольце многочленов.
19. Неприводимые многочлены. Понятие и свойства.
20. Теорема о существовании неприводимых многочленов.
21. Расширения простых полей.
22. Алгоритм Евклида.
23. Расширенный алгоритм Евклида
24. Векторное пространство
25. Представление элементов конечных полей
26. Минимальный многочлен.
27. Примитивные многочлены.
28. Свойства минимальных многочленов.
29. Свойства многочленов над конечным полем.
30. Нахождение корней неприводимого многочлена.
31. Вычисления в мультипликативной группе расширения поля
32. Нахождение минимальных многочленов
33. Существование и единственность поля $GF(p^n)$ для всех n
34. Среднее число неприводимых нормированных многочленов

35. Функция Мебиуса
36. Нормированный делитель порождающего элемента идеала
37. Циклическое пространство
38. Примитивные корни, т. е. корни из 1.
39. Задача помехоустойчивого кодирования
40. Понятия, связанные с булевым кубом
41. Кодовое расстояние
42. Блочное кодирование и декодирование
43. Блочное кодирование
44. Теорема Хэмминга
45. Код Голея
46. Определения и свойства
47. Порождающая и проверочная матрицы
48. Систематическое кодирование.
49. Проверочная матрица
50. Кодирования блочным линейным кодом
51. Систематическое и несистематическое кодирование
52. Тривиальный метод
53. Декодирование по синдрому
54. Декодирование кода Хэмминга
55. Определение и построение циклических кодов
56. Полиномиальное представление слов
57. Кодирование циклическими кодами
58. Декодирование циклических кодов
59. Определение и основное свойство БХЧ-кодов
60. Циклотомический класс элемента пол. Свойства классов.
61. БХЧ коды: синдромы
62. Алгоритм построения БЧХ-кода
63. Коды Римана – Соломона
64. Действие группы на множестве. Фиксатор перестановки и стабилизатор элемента множества
65. Лемма Бернсайда
66. Применение теоремы Пойа для решения комбинаторных задач.

Критерии оценки устного ответа на вопросы по дисциплине

✓ 5 баллов - если ответ показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.

✓ 4 - балла - знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

✓ 3 балла – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

✓ 2 балла – незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

7.3.2. Тестовые задания для проверки знаний студентов

7.3.3. Типовые задания к контрольным работам

Примеры заданий для контрольной работы по теме: Основные алгебраические структуры: группы, кольца, поля

1. Постройте инъективный гомоморфизм групп $(\mathbb{Z}_5, +) \rightarrow (\mathbb{C}^*, \cdot)$.
2. Опишите все подгруппы а) в циклических группах порядков 7, 4 и 12; б) в прямом произведении $S_2 \times S_3$.
3. Докажите, что в абелевой группе множество ее элементов конечного порядка образует группу.
4. Докажите, что в абелевой группе множество ее элементов конечного порядка образует группу.
5. Существует ли бесконечная группа, в которой каждый элемент имеет конечный порядок?
6. Постройте тело из 4 элементов. Докажите, что все такие тела изоморфны между собой и являются полями.
7. Найдите наибольший общий делитель многочленов x^3+1 и x^5+1 над полем $\mathbb{Z}/3\mathbb{Z}$.
8. Вычислите значение функции Эйлера $\phi(2008)$.

Примеры заданий для итоговой контрольной работы

- ✓ Какое количество ошибок может гарантированно обнаружить двоичный групповой код с минимальным расстоянием 7?
- ✓ Найдите два такие многочлена $p(x)$ и $q(x)$ над полем F_2 , что
$$p(x)(x^2+x+1)+q(x)(x^3+x+1)=1.$$
- ✓ Постройте код Хэмминга с параметрами (10, 14), перечислив все кодовые слова.
- ✓ Докажите, что если x и y — два элемента некоторой группы, то элементы xy и yx этой группы имеют один и тот же порядок.
- ✓ Перечислите все абелевы подгруппы группы S_4 .
- ✓ Найдите какой-нибудь примитивный элемент в поле $\mathbb{Z}_3[x]/(x^2-1)$. Каковы могут быть максимальные длины кодовых слов и кодовое расстояние в соответствующем БЧХ коде, построенном на основе данного примитивного элемента?
- ✓ В системе RSA при $e=7$ с открытым ключом (143, 7)
 - а) зашифруйте сообщение 99;
 - б) расшифруйте сообщение 11.
- ✓ Докажите следующее тождество, связывающее значения функции Эйлера для наименьшего общего кратного и наибольшего общего делителя:
$$\phi((m,n)) \phi([m,n]) = \phi(m)\phi(n).$$
- ✓ Постройте поле из 8 элементов как факторкольцо кольца многочленов от переменной x над полем из двух элементов и найдите в нем элемент, обратный к (x^2+x+1) .
- ✓ Сколько примитивных элементов насчитывает поле Галуа $GF(q)$?

Критерии оценки контрольных работ:

- студенту, если он безошибочно выполнил все задания;
- оценка «хорошо» выставляется студенту, если он выполнил все задания, но допустил

ошибки, не влияющую на ход и смысл их решения;

- оценка «удовлетворительно» выставляется студенту, если он выполнил правильно хотя бы одно задание работы;
- оценка «неудовлетворительно» выставляется студенту, если он не выполнил правильно ни одного задания.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.1. Основная литература

1. Вeneвeтитинa С. С. Прикладная математика. Задача коммивояжера. Системы массового обслуживания: Учебное пособие / Вeneвeтитинa С.С., Зенина В.В., Сапронов И.В. - Воронеж: ВГЛУ им. Г.Ф. Морозова, 2014. - 47 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/858465> – Режим доступа: по подписке.
2. Карнаухова О. А. Прикладные задачи в математике: учебное пособие / О. А. Карнаухова, В. А. Шершнева, Т. О. Кочеткова. — 2-е изд., испр. и доп. — Красноярск: СФУ, 2020. — 216 с. — ISBN 978-5-7638-4204-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/181564> — Режим доступа: для авториз. пользователей.
3. Карнаухова О. А. Прикладные задачи в математике: учебное пособие / О. А. Карнаухова, В. А. Шершнева, Т. О. Кочеткова. - 2-е изд., испр. и доп. - Красноярск: Сиб. федер. ун-т, 2020. - 216 с. - ISBN 978-5-7638-4204-3. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1819337> – Режим доступа: по подписке.
4. Крюкова О. Г. Численные методы линейной алгебры: учебное пособие. — 3-е изд., перераб. и доп. — Москва: Магистр, 2021. — 528 с. - ISBN 978-5-16-109374-0. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1238539> – Режим доступа: по подписке.
5. Тропин М. П. Основы прикладной алгебры: учебное пособие / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2020. — 288 с. — ISBN 978-5-8114-5327-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/139282> — Режим доступа: для авториз. пользователей.

8.2. Дополнительная литература

1. Винберг Э.Б. Курс алгебры.- М.: МЦНМО, 2011 [//biblioclub.ru](http://biblioclub.ru)
2. Ильин В.А. Прикладная алгебра: учебник М.: Физматлит, 2011, [// biblioclub.ru](http://biblioclub.ru)
3. Кочетова Ю.В. Алгебра. Конечномерные пространства. Линейные операторы: курс лекций. - М.: Прометей, 2013-80 с. [// biblioclub.ru](http://biblioclub.ru)
4. Панкратьев Е.В. Элементы компьютерной алгебры: Учеб. пособие.-М.: ИНТУИТ, 2007 - 248 с. [// biblioclub.ru](http://biblioclub.ru)
5. Морелос-Сарагоса Г. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2006.
6. Авдошин С. М., Набебин А. А. Дискретная математика. Модулярная алгебра, криптография, кодирование. М.: ДМК Пресс, 2017.
7. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: Ком Книга, 2006.
8. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: Ком Книга, 2006.
9. Бугров Я.С. Сборник задач по высшей математике: учебное пособие - М.: Физматлит, 2011.- URL: <http://www.knigafund.ru>

10. Введение в криптографию Под общ. ред. В. В. Яценко. 4-е изд., доп. М.: МЦНМО, 2012.
11. Вернер М. Основы кодирования. Учебник для ВУЗов. М: Техносфера, 2004.
12. Винберг Э.Б. Курс алгебры - М: МЦНМО, 2011 - URL: <http://www.knigafund.ru>
13. Дураков Б.К. Краткий курс высшей алгебры: учеб. пособие - М.: Физмалит, 2014- URL: <http://www.knigafund.ru>
14. Журавлёв К. И., Флёров Ю. А., Вялый М. Н. Дискретный анализ. Основы высшей алгебры. М.: МЗ Пресс, 2007.
15. Ильин В.А. Линейная алгебра: учебник. М: ФИЗМАТЛИТ, 2010.- URL:<http://www.knigafund.ru>
16. Касами Т., Токура Н., Ивадари Е.. Инагаки Я. Теория кодирования. М.: Мир, 1978.
17. Киселев А.П. Алгебра: в 2 ч: учебник. М.: Физматлит, 2011 – URL:<http://www.knigafund.ru>
18. Киселев А.П. Алгебра: в 2 ч: учебник. М.: Физматлит, 2011 – URL:<http://www.knigafund.ru>
19. Кочетова Ю.В. Алгебра. Конечномерные пространства. Линейные операторы: курс лекций. М.: Прометей, 2013.- 80с.
20. Курош А. Г. Курс высшей алгебры: учебник. СПб.: Изд-во «Лань» 2013.
21. Лидл Г., Нидеррайтер Г. Конечные поля: В 2-х т. М.: Мир. 1988.
22. Патерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.
23. Применко Э. А. Алгебраические основы криптографии: Учебное пособие. М.: Книжный дом «Либроком», 2014.
24. Токарева П. Симметричная криптография. Краткий курс: учебное пособие / Новосибир. гос. ун- т. Новосибирск, 2012.

9. Требования к условиям реализации рабочей программы дисциплины (модуля)

9.1. Общесистемные требования

Электронная информационно-образовательная среда ФГБОУ ВО «КЧГУ»

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее.

Функционирование ЭИОС обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование ЭИОС соответствует законодательству Российской Федерации.

Адрес официального сайта университета: <http://kchgu.ru>.

Адрес размещения ЭИОС ФГБОУ ВО «КЧГУ»: <https://do.kchgu.ru>.

Электронно-библиотечные системы (электронные библиотеки)

Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2025-2026 учебный год	Электронно-библиотечная система ООО «Знаниум». Договор № 249 эбс от 14.05.2025 г. Электронный адрес: https://znanium.com	от 14.05.2025г. до 14.05.2026г.
2025-2026 учебный год	Электронно-библиотечная система «Лань». Договор № 10 от 11.02.2025 г. Электронный адрес: https://e.lanbook.com	от 11.02.2025г. до 11.02.2026г.

2025-2026 учебный год	Электронно-библиотечная система КЧГУ. Положение об ЭБ утверждено Ученым советом от 30.09.2015г. Протокол № 1. Электронный адрес: http://lib.kchgu.ru	Бессрочный
2025-2026 учебный год	Национальная электронная библиотека (НЭБ). Договор №101/НЭБ/1391-п от 22.02.2023 г. Электронный адрес: http://rusneb.ru	Бессрочный
2025-2026 учебный год	Научная электронная библиотека «ELIBRARY.RU». Лицензионное соглашение №15646 от 21.10.2016 г. Электронный адрес: http://elibrary.ru	Бессрочный
2025-2026 учебный год	Электронный ресурс Polpred.com Обзор СМИ. Соглашение. Бесплатно. Электронный адрес: http://polpred.com	Бессрочный

9.2. Материально-техническое и учебно-методическое обеспечение дисциплины

Занятия проводятся в учебных аудиториях, предназначенных для проведения занятий лекционного и практического типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации в соответствии с расписанием занятий по образовательной программе. С описанием оснащённости аудиторий можно ознакомиться на сайте университета, в разделе материально-технического обеспечения и оснащённости образовательного процесса по адресу: <https://kchgu.ru/sveden/objects/>

9.3. Необходимый комплект лицензионного программного обеспечения

- Microsoft Windows (Лицензия № 60290784), бессрочная
- Microsoft Office (Лицензия № 60127446), бессрочная
- ABBY FineReader (лицензия № FCRP-1100-1002-3937), бессрочная
- Calculate Linux (внесён в ЕРПП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная
- Google G Suite for Education (IC: 01i1p5u8), бессрочная
- Kaspersky Endpoint Security (Лицензия № 280E-210210-093403-420-2061), с 25.01.2023 г. по 03.03.2025 г.
- Kaspersky Endpoint Security. Договор №0379400000325000001/1 от 28.02.2025г. Срок действия лицензии с 27.02.2025г. по 07.03.2027г.

9.4. Современные профессиональные базы данных и информационные справочные системы

1. Федеральный портал «Российское образование» - <https://edu.ru/documents/>
2. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – <http://school-collection.edu.ru/>
3. Базы данных Scopus издательства Elsevier <http://www.scopus.com/search/form.uri?display=basic>.
4. Портал Федеральных государственных образовательных стандартов высшего образования - <http://fgosvo.ru>.
5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) – <http://edu.ru>.
6. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) – <http://school-collection.edu.ru>.

7. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») – <http://window/edu.ru>.

10. Особенности организации образовательного процесса для лиц с ограниченными возможностями здоровья

В ФГБОУ ВО «Карачаево-Черкесский государственный университет имени У.Д. Алиева» созданы условия для получения высшего образования по образовательным программам обучающихся с ограниченными возможностями здоровья (ОВЗ).

Специальные условия для получения образования по ОПВО обучающимися с ограниченными возможностями здоровья определены «[Положением об обучении лиц с ОВЗ в КЧГУ](#)», размещенным на сайте Университета по адресу: <http://kchgu.ru>.

11. Лист регистрации изменений

Изменение	Дата и номер протокола ученого совета факультета/института, на котором были рассмотрены вопросы о необходимости внесения изменений в ОП	Дата и номер протокола ученого совета Университета, на котором были утверждены изменения в ОП
Переутверждена ОП ВО. Обновлено: учебный план, календарный учебный план, РПД, РПП, программы ГИА, воспитания календарный план воспитательной работы. Обновлены договоры: 1. На антивирус Касперского. (Договор №56/2023 от 25 января 2023г.). Действует до 03.03.2025г. 2. Договор №915 ЭБС ООО «Знаниум» от 12.05.2023г. Действует до 15.05.2024г. 3. Договор №36 от 14.03.2024г эбс «Лань». Действует по 19.01.2025г. 4. Договор №238 ЭБС ООО «Знаниум» от 23.04.2024г. Действует до 11 мая 2025г.	23.05.2024г. протокол №10	29.05.2024г. протокол №8
Переутверждена ОПВО. Обновлено: учебный план, календарный учебный график, РПД, РПП, программы ГИА, воспитания, календарный план воспитательной работы. Обновлены договоры: 1. На антивирус Касперского. (Договор №56/2023 от 25 января 2023г.). Действует до 03.03.2025г. 2. На антивирус Касперского. (Договор № 0379400000325000001/1 от 28.02.2025г. Действует по 07.03.2027г. 3. Договор № 10 от 11.02.2025г. эбс «Лань». Действует по 11.02.2026г. 4. Договор № 238 эбс ООО «Знаниум» от 23.04.2024г. Действует до 11 мая 2025г. Договор № 249-эбс ООО «Знаниум» от 14.05.2025г. Действует до 14.05.2026г.	29.04.2025г., протокол № 8	30.04.2025г., протокол № 8