МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Механико-математический факультет

УТВЕРЖДАЮ
Декан механико-математического факультета
_____ Захаров А.М.
"2" 09 2024 г.

Алгебраические приложения в криптографии

Направление подготовки магистратуры

02.04.01 – **Математика и компьютерные науки**

Профиль подготовки магистратуры
Математические основы компьютерных наук

Квалификация (степень) выпускника
магистр

Форма обучения

очная

Саратов,

2024

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Водолазов А.М.		2.09.2024
Председатель НМК	Тышкевич С.В.		2.09.2024
Заведующий кафедрой	Водолазов А.М.		2.09.2024
Специалист Учебного управления			

1. Цели освоения дисциплины

С помощью теории конечных полей и абстрактной алгебры, изложить теорию кодов, исправляющих ошибки, и кодов, обнаруживающих ошибки, вызванных «зашумлением» каналов связи. А именно, изложить основы теории линейных кодов и теории циклических кодов.

2. Место дисциплины в структуре ООП

Место дисциплины в структуре ООП Дисциплина «Алгебраические приложения в криптографии» относится к дисциплинам по выбору (Б1.В.ДВ.03.02) вариативной части блока 1 «Дисциплины» . Дисциплина читается в третьем семестре и, поэтому, является одним из курсов, заканчивающих обучение студентов в магистратуре. С другой стороны, этот курс один из наиболее трудных, ввиду его абстрактности и сложности доказательства основных результатов. Его усвоение свидетельствует об уровне квалификации студента. В качестве предварительной основы для этого курса необходимо знание разделов абстрактной алгебры, как теория конечных полей и теория многочленов над конечными полями. Проблемы передачи информации, а также вопросы кодирования и декодирования информации в целях ее надежной передачи в настоящее время являются весьма актуальными Этот курс тесно связан с отражение вопросов влияния этих разделов на развитие теории линейных и циклических кодов. Является одним из курсов, служащих основой для написания выпускных квалификационных работ

3. Результаты обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора (индикаторов) достижения компетенции**	**Результаты обучения**
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**1.1_М.УК-1.** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	**Знать:** - основные задачи и методы конечных полей и алгебраической теории кодирования; - **Уметь:** - анализировать математические проблемы используя конечных полей и алгебраической теории кодирования **Владеть:** - методами решения задач используя методы конечных полей и алгебраической теории кодирования навыками анализа математических проблем; - навыками самостоятельного изучения математической литературы по данной тематике.
	1.2_М.УК-1. Осуществляет поиск	**Знать:** - алгоритмы решения поставленной проблемной

	алгоритмов решения поставленной проблемной ситуации на основе доступных источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей детальной разработке. Предлагает способы их решения.	ситуации на основе доступных источников информации. **Уметь:** - выделять и систематизировать основные идеи в научных текстах, делать обоснованные выводы из учебной литературы; **Владеть:** – навыками критического анализа информации по теории конечных полей и алгебраической теории кодирования
	2.1_М.УК-1. Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности	**Знать:** – основы планирования целей деятельности. **Уметь:** – планировать цели деятельности с учетом условий, средств, личностных возможностей, временной перспективы развития деятельности. **Владеть:** – навыками постановки и решения задач в рамках поставленной цели; – навыками публичного представления результатов решения конкретной задачи
ПК-1 Способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий.	**1.1_М.ПК-1.** Понимает основные концепции, принципы, теории и факты, в области математических и (или) естественных наук, программирования и информационных технологий.	**Знать:** – основные концепции, принципы, теории и факты, связанные с алгебраической геометрией **Уметь:** – находить основные концепции, принципы, теории и факты, алгебраической геометрией. **Владеть:** – основные концепциями, принципами, теорией и фактами, связанными с алгебраической геометрией
	• **2.1_М.ПК-1.** Формулирует и решает стандартные задачи в собственной научно- исследовательской деятельности.	**Знать:** – основные методы решения стандартных задач, связанных с моделями и методами конечных полей и алгебраической теории коди-рования **Уметь:**

		– применять модели и методы конечных полей и алгебраической теории кодирования при формулировании и решении стандартных задач в собственной научно-исследовательской деятельности. **Владеть:** – навыками формулирования и решения стандартных задач, связанных с моделями и методами конечных полей и алгебраической теории кодирования в собственной научно-исследовательской деятельности
	3.1_М.ПК-1. Проводит научно-исследовательские работы в области математики и компьютерных наук.	**Знать:** – основные методы проведения научно-работы в области математики и компьютерных наук, основанные на методах конечных полей и алгебраической теории кодирования. **Уметь:** – проводить научно-исследовательские работы в области математики и компьютерных наук, основанные на на методах конечных полей и алгебраической теории кодирования. **Владеть:** – навыками проведения научно-исследовательских работ в области математики и компьютерных наук, основанные на методах конечных полей и алгебраической теории кодирования.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по семестрам)*
				Лек.	**Пр.**	**СРС**	**КСР**	
1	Строение конечных полей.	1	1-5	5	10	15		Консультация
2	Многочлены над конечными полями.	1	6-10	5	10	15		Консультация
3	Линейные коды.	1	11-14	4	8	20		Консультация
4	Циклические коды.	1	15-18	4	8	40		Консультация
								экзамен 36
	Итого за 3 семестр			**18**	**36**	**90**		**180 ч**

Содержание дисциплины

1. Строение конечных полей.

Характеристики конечных полей и их простые подполя. Порядки конечных полей. Критерий расширения для конечных полей. Нормальность и сепарабельность расширений конечных полей. Критерий подполя. Цикличность мультипликативной группы конечного поля. Примитивный элемент конечного поля. Количество примитивных элементов конечного поля. Существование неприводимых многочленов любой положительной степени над любым конечным полем. Автоморфизм Фробениуса. Группа Галуа расширения конечного поля. Корни неприводимых многочленов над конечным полем. Поля разложений неприводимых многочленов. Порядки сопряженных элементов в мультипликативной группе поля. Следы и нормы элементов расширений конечных полей и их свойства. Характеристические многочлены элементов расширений. Круговые поля и круговые многочлены. Конечные поля как круговые расширения. Три способа представлений элементов конечных полей

2. Многочлены над конечными полями.

Порядок многочленов со свободным членом. Теорема о порядке многочлена и ее следствие для неприводимых многочленов. Теорема о числе неприводимых многочленов данной степени и данного порядка. Формула для порядков многочленов, разложенных в произведение.

3. Линейные коды.

Понятие линейного кода. Проверочная матрица линейного кода. Стандартная порождающая матрица линейного (n,k) - кода. Понятие кода, исправляющего t ошибок. Понятие минимального расстояния линейного кода. Алгоритм декодирования линейного кода по лидеру смежного класса. Теорема о границе минимального расстояния линейного (n,k) - кода.

4. Циклические коды.

Понятие весовой функции кода. Понятие циклического линейного (n,k) - кода. Теорема о цикличности линейного (n,k) - кода. Понятие порождающего и проверочного многочлена циклического кода. Понятие максимального циклического кода. Понятие БЧХ-кода длины k и

с конструктивным расстоянием d. Теорема о минимальном расстоянии БХЧ кода с конструктивным расстоянием d. Алгоритм декодирования БХЧ-кода.

Примерный план практических занятий.

1. Строение конечных полей.
2. Автоморфизм Фробениуса. Группа Галуа расширения конечного поля.
3. Круговые поля и круговые многочлены.
4. Неприводимые многочлены в конечных полях.
5. Линейные коды.
6. Алгоритм декодирования линейного кода
7. Циклический линейный (n,k) - код
8. БЧХ-кода длины k и с конструктивным расстоянием d
9. Алгоритм декодирования БХЧ-кода.

5. Образовательные технологии, применяемые при освоении дисциплины

Практические занятия и консультации проходят в виде бесед, научного диалога и опроса, включающие самостоятельную подготовку магистров по смежным вопросам дисциплины, используя дополнительную литературу. Предусмотрены вызывные консультации, написание рефератов по пропущенным темам. Подготовлен электронный вариант лекционного курса, который предлагается студентам, в том числе и студентам с ограниченными возможностями здоровья.

Для студентов, с ограниченными возможностями зрения предлагается прослушать лекционный курс в отведенное для этого время и активно участвовать в научных диалогах по тематике данной дисциплины.

Для магистров с ограниченными возможностями здоровья предусмотрены следующие формы организации учебного процесса и контроля знаний: -для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения контрольных заданий при необходимости предоставляется увеличивающее устройство; задания для выполнения, а также инструкция о порядке выполнения контрольных заданий оформляются увеличенным шрифтом (размер 16-20);

- для глухих и слабослышащих: обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости магистру предоставляется звукоусиливающая аппаратура индивидуального пользования;

- для лиц с тяжелыми нарушениями речи, глухих, слабослышащих все контрольные задания по желанию магистра могут проводиться в письменной форме. Основной формой организации учебного процесса является интегрированное обучение инвалидов, т.е. все магистры обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Самостоятельная работа студентов предполагает индивидуальную работу с учебно-методической литературой: учебниками, методическими пособиями, а также со специальной литературой, монографиями, статьями. Консультации лектора помогают усвоению материала. Контроль за успеваемостью осуществляется в форме бесед учебного и творческого характера, опроса, индивидуальных заданий, контрольной работы.

План самостоятельной работы.

1. Определение линейного кода. Порождающая матрица линейного кода. Приведенно-ступенчатая форма порождающей матрицы.
2. Блочные коды, примеры.
3. Расстояние Хемминга. Декодер.
4. Минимальное расстояние кода.
5. Линейные коды, их структура. Порождающая и проверочная матрица.
6. Граница Синглтона, коды с максимальным минимальным расстоянием
7. Теорема кодирования Шеннона.
8. Код Маллера Декодер Рида.
9. Описание циклического кода, как идеала кольца многочленов.
10. Синдромное декодирование.
11. Свойства порождающего многочлена, сопряженные корни и вид неприводимого многочлена.
12. Нижняя граница Варшамова-Гилберта
13. Коды Боуза-Чоудхури-Хоквингема.
14. Декодер Питерсона-Горенстейна-Циклера.
15. Алгоритм декодирования. Код Рида-Соломона, кодирование и декодирование.
16. Код РС как частный случай кода БЧХ.
17. Двоичный и троичный коды Голея.

ПРИМЕРНЫЕ ВАРИАНТЫ КОНТРОЛЬНОЙ РАБОТЫ
Вариант 1.

1. Пусть задан многочлен $f(x) = x^2 + 1 \in F_3[x]$. Сопровождающая матрица для него имеет вид $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.
   Найти представления поля F_9.
2. Линейный блоковый (6,3)-код задан порождающей матрицей:

	0	1	1
	1	0	1
	1	0	0
G=	1	1	1
	1	1	0
	0	1	1

.

Требуется для данного кода осуществить несистематическое и систематическое кодирование векторов u^t =(0 1 1) и v^t =(1 0 1) построить проверочную матрицу кода H, а также определить минимальное кодовое расстояние d.

Вариант 2.

1. Пусть задан многочлен $f(x) = x^2 + 1 \in F_3[x]$. Сопровождающая матрица для него имеет вид

	0	2
A=	-1	0

.

Найти представления поля F_9.

2. Рассмотреть (15,5,7) БЧХ код, исправляющий две ошибки.

Вопросы для текущего контроля

1. Характеристика конечного поля.
2. Порядок конечных полей.
3. Нормальность и сепарабельность расширений конечных полей.
4. Цикличность мультипликативной группы конечного поля.
5. Автоморфизм Фробениуса.
6. Группа Галуа расширения конечного поля.
7. Поля разложений неприводимых многочленов.
8. Строение конечных полей.
9. Характеристика и порядок конечного поля.
10. Существование конечных полей данного порядка.
11. Многочлены над конечными полями.
12. Неприводимые многочлены.
13. Построение неприводимых многочленов.
14. Понятие линейного кода.
15. Проверочная матрица линейного кода.
16. Стандартная порождающая матрица линейного (n,k) - кода.
17. Понятие кода, исправляющего t ошибок.
18. Понятие минимального расстояния линейного кода.
19. Понятие максимального циклического кода.
20. Понятие БЧХ-кода длины k и с конструктивным расстоянием d.

.

Вопросы для промежуточной аттестации

1. Характеристика конечного поля.
2. Порядок конечных полей.
3. Нормальность и сепарабельность расширений конечных полей.
4. Цикличность мультипликативной группы конечного поля.
5. Примитивный элемент конечного поля.
6. Неприводимые многочлены над любым конечным полем.
7. Автоморфизм Фробениуса.

8. Группа Галуа расширения конечного поля.
9. Поля разложений неприводимых многочленов.
10. Строение конечных полей.
11. Характеристика и порядок конечного поля.
12. Существование конечных полей данного порядка.
13. Расширения конечных полей. Расширения Галуа.
14. Группа Галуа расширения конечных полей.
15. Многочлены над конечными полями.
16. Неприводимые многочлены.
17. Построение неприводимых многочленов.
18. Примитивные многочлены, их корни.
19. Линейные коды.
20. Понятие линейного кода.
21. Проверочная матрица линейного кода.
22. Стандартная порождающая матрица линейного (n,k) - кода.
23. Понятие кода, исправляющего t ошибок.
24. Понятие минимального расстояния линейного кода.
25. Алгоритм декодирования линейного кода по лидеру смежного класса.
26. Теорема о границе минимального расстояния линейного (n,k) - кода.
27. Понятие весовой функции кода.
28. Понятие циклического линейного (n,k) - кода.
29. Теорема о цикличности линейного (n,k) - кода.
30. Понятие порождающего и проверочного многочлена циклического кода.
31. Понятие максимального циклического кода.
32. Понятие БЧХ-кода длины k и с конструктивным расстоянием d.
33. Теорема о минимальном расстоянии БХЧ-кода с конструктивным расстоянием d.
34. Алгоритм декодирования БХЧ-кода.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1. Таблица максимальных баллов по видам учебной деятельности.

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
3	5	0	15	20	0	20	40	100

Программа оценивания учебной деятельности студента

3 семестр

Лекции

Посещаемость, оценка конспектов от 0 до 5 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Посещаемость, уровень подготовки к занятиям – от 0 до 5 баллов,
активность работы в аудитории – от 0 до 5 баллов,
выполнение домашних заданий– от 0 до 5 баллов.

Самостоятельная работа

Рефераты по отдельным темам – от 0 до 10 баллов,
Конспектирование отдельных тем – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

1. Контрольная работа №1 – от 0 до 20 баллов.

Промежуточная аттестация

при проведении промежуточной аттестации
ответ на «отлично» оценивается от 36 до 40 баллов;
ответ на «хорошо» оценивается от 31 до 35 баллов;
ответ на «удовлетворительно» оценивается от 25 до 30 баллов;
ответ на «неудовлетворительно» оценивается от 0 до 24 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 3 семестр по дисциплине «Алгебраические приложения в криптографии» составляет 100 баллов.

Таблица 2. Таблица пересчета полученной студентом суммы баллов по дисциплине «**Алгебраические приложения в криптографии»**

85 – 100 баллов	«отлично»
70 – 84 баллов	«хорошо»
60 – 69 баллов	«удовлетворительно»
0 – 59 баллов	«не удовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

Учебная аудитория с обязательным наличием специализированной доски, мела (маркера), проектора, с возможностью размещения всех обучающихся по данной дисциплине.

а) литература

1. *Курош А.Г. Курс высшей алгебры. – СПб.*2024. https://e.lanbook.com/book/118617 Книга находится в ЭБС "ЛАНЬ".

2. Виноградов, И.М. Основы теории чисел/ И.М. Виноградов. -Москва: Лань, 2023.-176с. https://e.lanbook.com/book/115195

б) программное обеспечение и Интернет-ресурсы:

Лицензионное программное обеспечение:

1. Операционная система Windows 7, или более поздняя версия
2. Microsoft Office PowerPoint

Интернет-ресурсы:

1. Саратовской государственный университет им. Н.Г. Чернышевского. – Режим доступа: www.sgu.ru/
2. Зональная научная библиотека им. В.А. Артисевич Саратовского государственного университета им. Н.Г. Чернышевского. – Режим доступа: http://library.sgu.ru/
3. Каталог образовательных Интернет-ресурсов. – Режим доступа: http://window.edu.ru/

9. Материально-техническое обеспечение дисциплины (модуля)

Учебная аудитория с обязательным наличием специализированной доски, мела (маркера), проектора, с возможностью размещения всех обучающихся по данной дисциплине.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *02.04.01* – «Математика и компьютерные науки» и профилю подготовки «Математические основы компьютерных наук».

Автор: к.ф.-м.н., доцент, доцент кафедры компьютерной алгебры и теории чисел Водолазов А.М.

Программа одобрена на заседании кафедры компьютерной алгебры и теории чисел от 2 сентября 2024 года, протокол № 2.

Приложение

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература:

1. Лидл Р., Нидеррайтер Г. Конечные поля. Т.1. - М.: Мир, 1988.
2. Лидл Р., Нидеррайтер Г. Конечные поля. Т.2. - М.: Мир, 1988.
3. Ленг С. Алгебра – М: Мир, 1968
4. Берлекэмп Э. Алгебраическая теория кодирования. / М.: Мир, 1971
5. Блейхут Р. Теория и практика кодов, контролирующих ошибки./ М. Мир, 1986