БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

_____А.Д.Король

15 июля 2024 г.

Регистрационный №УД- 13400/уч.

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Учебная программа учреждения образования
по учебной дисциплине для специальности:

1-31 03 09 Компьютерная математика и системный анализ

2024 г.

Учебная программа составлена на основе ОСВО 1-31 03 09-2021, и учебного плана № G31-1-019/уч. от 25.05.2021, № G31-1-004/уч.ин. от 31.05.2021, № G31-1-222/уч. от 22.03.2022, № G31-1-226/уч.ин. от 27.05.2022.

СОСТАВИТЕЛИ:

А.В. Кушнеров, старший преподаватель кафедры дифференциальных уравнений и системного анализа механико-математического факультета Белорусского государственного университета.

РЕЦЕНЗЕНТЫ:

О.А. Кушнерова, инженер-программист, ООО "Мобильная аналитика".

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа БГУ
(протокол № 12 от 25.04.2024)

Научно-методическим советом БГУ
(протокол № 9 от 28.06.2024)

Зав. кафедрой дифференциальных уравнений
и системного анализа Л. Л. Голубева

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины «Теория помехоустойчивого кодирования» – формирование у студентов магистратуры знаний и навыков в теории помехоустойчивого кодирования и теории информации.

Образовательная цель: обучение магистрантов современным приёмам для моделирования работы информационно-коммуникационных систем (ИКС); приобретение навыков исправления ошибок в каналах с шумами математическими методами; изучение теории норм синдромов и полиномиальных алгебраических методов исправления ошибок.

Развивающая цель: развитие навыков разработки учебных моделей алгоритмов защиты информации на платформе *Python*, а также в среде разработки *Wolfram Mathematica*; развитие алгоритмических шаблонов для задач поиска, индексации, сжатия.

Задачи учебной дисциплины:

1. Формирование у студентов способностей разрабатывать алгоритмы решения задач и их анализировать;
2. Приобретение способностей самостоятельно расширять математические знания и компьютерные навыки с дальнейшим их использованием при анализе математических моделей широкого круга прикладных задач.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Теория помехоустойчивого кодирования» относится **к модулю** «Компьютерное моделирование» компонента учреждения высшего образования, является дисциплиной по выбору студента.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Изучение дисциплины основывается на знаниях, полученных студентами при изучении дисциплин: «Компьютерная математика» и «Математические основы защиты информации»

Требования к компетенциям

Освоение учебной дисциплины «Теория помехоустойчивого кодирования» должно обеспечить формирование следующей **специализированной компетенции:**

СК Осуществлять математическое и компьютерное моделирование для прикладных исследований.

В результате изучения учебной дисциплины студент должен:

знать:

- китайскую теорему об остатках и ее применение;
- свойства конечных полей;
- основы теории норм синдромов;
- основы классификации двоичных векторов и матриц.

уметь:

– корректно применять изученные в курсе алгоритмы;

– формировать поля Галуа заданного порядка и проводить вычисления в них;

владеть:

– методами вычислений в кольцах классов вычетов и в конечных полях;

– методами решения алгебраических уравнений над кольцами классов вычетов и над полями Галуа;

– алгоритмами групповой классификации векторов и матриц.

Структура учебной дисциплины

Дисциплина «Теория помехоустойчивого кодирования» изучается в седьмом семестре. Всего на изучение учебной дисциплины «Теория помехоустойчивого кодирования» отведено:

– для очной формы получения высшего образования – 120 часов, в том числе 72 аудиторных часов, из них: лекции – 36 часов (в том числе – 4 ч ДОТ), лабораторные занятия – 30 часов (в том числе – 4 ч ДОТ), управляемая самостоятельная работа – 6 часов.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Линейные коды.

Теорема Шеннона о возможности коррекции ошибок при передачи информации в каналах с шумами. Цифровые системы связи. Определение линейного кода и его технический смысл. Проверочная и порождающая матрицы кода. Метрика Хемминга. Минимальное расстояние кода. Коды Хемминга. Декодирование по методу максимального правдоподобия. Декодирование по таблицам смежных классов. Синдромы ошибок и их свойства. Синдромное декодирование.

Тема 2. БЧХ-коды.

Классические БЧХ-коды и реверсивные коды, исправляющие двойные и тройные ошибки. Структура их проверочных матриц. Декодирование двойных и тройных ошибок решением квадратных и, соответственно, кубических уравнений в полях Галуа. Общее определение БЧХ-кодов, их свойства и параметры. Связь декодирования с проблемой решения уравнений в полях Галуа.

Тема 3. Автоморфизмы кодов.

Неоднозначность проверочных матриц кодов и их взаимосвязь. Эквивалентные коды и их матрицы. Автоморфизмы кодов. Циклические коды.

Тема 4. Орбиты ошибок и их сидромные спектры.

Строение, свойства и мощности циклических и циклотомических орбит векторов. Синдромные спектры орбит векторов-ошибок в реверсивных и БЧХ-кодах.

Тема 5. Нормы синдромов и их свойства.

Нормы синдромов в реверсивных и БЧХ-кодах, исправляющих двойные ошибки. Инвариатность норм относительно группы циклических сдвигов. Идея норменного декодирования. Общее определение норм синдромов для произвольных БЧХ-кодов. Основные свойства норм синдромов.

Тема 6. Полиномиально-норменная процедура коррекции ошибок БЧХ-кодами.

Минимальные полиномы как инварианты G-орбит ошибок. Полиномиально-норменный метод коррекции ошибок БЧХ-кодами.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
	Всего	**36**			**30**		**6**	
1	Линейные коды.	8			8			Отчет по лабораторной работе с устной защитой
2	БЧХ-коды.	4 (ДОТ)			4 (ДОТ)			Отчет по лабораторной работе с устной защитой
3	Автоморфизмы кодов.	6			4		2	Отчет по лабораторной работе с устной защитой, контрольная работа.
4	Орбиты ошибок и их сидромные спектры.	6			6			Отчет по лабораторной работе с устной защитой
5	Нормы синдромов и их свойства.	6			4		2	Отчет по лабораторной работе с устной защитой, контрольная работа.
6	Полиномиально-норменная процедура коррекции ошибок БЧХ-кодами.	6			4		2	Отчет по лабораторной работе с устной защитой, контрольная работа.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Романьков, В. А. Алгебраическая криптология / В. А. Романьков ; М-во науки и высшего образования РФ, ФГБОУ ВО "Омский гос. ун-т им. Ф. М. Достоевского". - Омск : Изд-во ОмГТУ, 2020. - 261 с.
2. Виноградов, И. М. Основы теории чисел : учебное пособие [для вузов] / И. М. Виноградов. - Изд. 15-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. - 176 с. - URL: https://reader.lanbook.com/book/298499.
3. Бухштаб, А. А. Теория чисел : учебное пособие / А. А. Бухштаб. - Изд. 6-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2022. - 384 с. - URL: https://e.lanbook.com/book/189329.
4. Гулай, А. В. Построение интеллектуальных систем : учебное пособие для студентов учреждений высшего образования по направлениям образования "Интеллектуальные системы" / А. В. Гулай, В. М. Зайцев. - Минск : ИВЦ Минфина, 2022. - 367 с.
5. Березкин, Е. Ф. Основы теории информации и кодирования / Е. Ф. Березкин. - 4-е изд., стер. - Санкт-Петербург : Лань, 2023. - 320 с. - URL: https://e.lanbook.com/book/330500.

Перечень дополнительной литературы

1. Котов, В. М. Теория алгоритмов. Организация перебора и приближенные алгоритмы : учебно-методическое пособие для студ. учреждений высшего образования, обуч. по спец. "Информатика" / В. М. Котов, Е. П. Соболевская, Г. П. Волчкова ; БГУ. - Минск : БГУ, 2022. - 151 с. - URL: https://elib.bsu.by/handle/123456789/312810.
2. Математические и компьютерные основы криптологии: Учеб. пособие для студ. матем. и инженерно-техн. спец. вузов / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. - Минск: Новое знание, 2003. - 381с.
3. Тилборг, Х.К.А. ван. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.
4. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие для студ. матем. и инженерно-технических спец. вузов / Ю.С.Харин, С.В.Агиевич. – Мн. : БГУ, 2001. - 190с.
5. Мао, Венбо Современная криптография = Modern Cryptography : теория и практика / Венбо Мао ; [пер. с англ. и ред. Д. А. Клюшина]. – Москва; Санкт-Петербург; Киев: Вильямс, 2005. - 764с.
6. Алферов, А.П. Основы криптографии. Учебное пособие, 2-е изд., испр. и доп. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

7. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

8. Эндрюс, Г. Теория разбиений / Г. Эндрюс. – М.: Наука, 1982. – 256 с.

9. Холл, М. Комбинаторика / М. Холл. – М.: Мир, 1970. – 424 с.

10. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. – 324 с.

11. Крэндалл Р., Померанс Р. Простые числа. Криптографические и вычислительные аспекты. М.: УРСС, 2011. – 664 с.

12. Ленг С. Алгебра. М.: Мир, 1968. – 564 с.

13. Лиддл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. – 822 с.

14. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учебно-метод. пособие. – Мн.: БГУИР, 2005. – 88 с. 2-е издание – Мн.: БГУИР, 2006. – 88 с.

15. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мн.: Издательский центр БГУ, 2007. – 240 с.

16. Липницкий, В.А., Аль-Хайдар Е.К. Норменное декодирование ошибок посредством их модификации. – Доклады БГУИР, 2009, №5(43). – С. 12 – 16.

17. Липницкий, В.А. Теория норм синдромов. – Мн.: БГУИР, 2011. – 96 с.

18. Липницкий, В.А., Михайловская Л.В., Валаханович Е.В. Защита информации: практикум. – Мн.: ВА РБ, 2012. – 86 с.

19. Липницкий, В.А., Цветков В.Ю., Конопелько В.К. Предсказание, паспознавание и формирование образов многоракусных изображений с подвижных объектов. – Мн.: Издат. центр БГУ, 2014. – 224 с.

20. Логачев О. А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М.: Изд-во МЦНМО, 2004. – 470 с.

21. Лосев В.В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки. Мн.: Вышэйшая школа. 1990. – 132 с.

22. Манин Ю.И., Пончишкин А.А. Введение в современную теорию чисел. – М.: Изд-во МЦНМО, 2009. – 552 с.

23. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Учебное пособие для ВУЗов. М.: Техносфера, 2006. – 320 с.

24. Ноден, П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999. – 720 с.

25. Сидельников, В.М. Теория кодирования. М.: Физматлит, 2008. – 324 с.

26. Смарт, Н. Криптография/ Н. Смарт. М.: Техносфера, 2005. – 524 с.

27. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. М.: МЦНМО, 2002. – 104 с.

Рекомендуемое учебно-лабораторное оборудование

Для проведения лабораторных занятий и УСР рекомендуется следующее программное обеспечение: MS Office, пакет *Mathematica*, пакет MATLAB, Python.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Объектом диагностики компетенций студентов являются знания, умения, полученные ими в результате изучения учебной дисциплины.

Для диагностики компетенций используется отчет по лабораторной работе с устной защитой и контрльная работа.

Оценка текущего контроля по дисциплине «Теория помехоустойчивого кодирования» формируется в результате регулярной и систематической проверки знаний обущающегося во время занятий и по итогам их самостоятельной работы. Текущий контроль знаний проходит во время устной защиты отчёта по лабораторным работам, выполняемым в учебной лаборатории и самостоятельно.

При защите лабораторных работ оценивается полнота ответа, аргументация выбранных решений, последовательность и оригинальность изложения материала, оригинальность кода, корректность оформления, самостоятельность выполнения заданий. Также ценится знание теоретических сведений, полученных на лекциях, поэтому студенту при выполнении лабораторных заданий необходимо знание лекционных материалов.

Формой промежуточной аттестации по дисциплине «Теория помехоустойчивого кодирования» учебным планом предусмотрен **зачёт.**

Примерный перечень заданий для управляемой самостоятельной работы обучающихся

Тема 3. Автоморфизмы кодов. (2 ч)

Примерный перечень заданий:

Для поля $GF\left(2^7\right)$ выполнить следующие действия.

1.Выписать все элементы.

2.Составить таблицу мультипликативной группы по степеням образующего элемента .

3.Выписать порядок каждого элемента мультипликативной группы поля.

4.Выписать элементы всех подгрупп мультипликативной группы поля.

5.Для каждого элемента поля отыщите полином с коэффициентами из минимального подполя, корнем которого он является.

Указание: Примитивные полиномы ищите в книге "Конечные поля" Лидл, Ниддерайтер.

Форма контроля – контрольная работа.

Тема 5. Нормы синдромов и их свойства (2 ч.)

БЧХ -код (91,12 δ = 5) задан матрицей H2. При построении поля использован полином $1+\alpha+\alpha^2+\alpha^{10}+\alpha^{12}$.

Примерный перечень заданий:

1. Исправить ошибки принятые декодером с пр. матрицей H2 методом систем и уравнения (1 и 2 сообщения).
2. Вывести позиции ошибочных меток. Вывести все промежуточные вычисления.
3. Позиции ошибок в 3-ем сообщении отыскать любым способом.

Форма контроля – контрольная работа.

Тема 6. Полиномиально-норменная процедура коррекции ошибок БЧХ-кодами (2 ч.)

БЧХ -код (91,12 δ = 5) задан матрицей H2. При построении поля использован полином $1+\alpha+\alpha^2+\alpha^{10}+\alpha^{12}$.

Примерный перечень заданий:

4. Исправить ошибки принятые декодером с пр. матрицей H2 методом норм синдромов (1 и 2 сообщения).
5. Вывести позиции ошибочных меток. Вывести все промежуточные вычисления.
6. Позиции ошибок в 3-ем сообщении отыскать любым способом.

Форма контроля – контрольная работа.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает***:***

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине рекомендовано разместить на образовательном портале или сайте кафедры учебно-методические материалы: курсы лекций и лабораторные

практикумы, методические указания к лабораторным занятиям, вопросы для подготовки к экзамену, перечень рекомендуемой литературы, информационные ресурсы.

Самостоятельная работа студента включает в себя работу с учебной литературой по заданным темам дисциплины, поиск в Интернете новейшей учебной и научной информации в указанных областях знаний и знакомство с ней, а также выполнение задач, поставленных на занятиях.

Примерный перечень вопросов к зачёту

1. Конечное поле. Построение. Определение. Примеры. Свойства. Вычисления в конечных полях.
2. Суть помехоустойчивого кодирования. Сферы применения. Линейный код.
3. Проверочная матрица линейного кода. Свойства.
4. Связь проверочной и порождающей матрицы линейного кода. Характеристики линейного кода.
5. Метрика Хемминга на пространстве кодовых слов. Минимальное расстояние кода. Свойства. Влияние на корректирующие возможности кода.
6. Методы нахождения минимального расстояния кода. Сравнение. Особенности реализации.
7. Коды Хемминга. Построение. Свойства. Корректирующие возможности.
8. Минимальное расстояние кодов Хемминга.
9. Синдромы и их свойства. Синдромный метод декодирования кодов Хемминга.
10. БЧХ –коды. Построение. Свойства.
11. Корректирующие возможности БЧХ – кодов. Конструктивное расстояние кода. Методы декодирования для БЧХ – кодов.
12. Автоморфизмы кода. Циклическая подстановка. Г-обиты. Свойства спектра синдромов Г-орбиты. Нормы синдромов.
13. Алгоритм норменного метода декодирования.
14. Циклотомическая подстановка. G-орбиты. Свойства норменного спектра G-орбиты. Полиномиальные инварианты G-орбит.
15. Двухступенчатая процедура полиномиально-норменного декодирования для БЧХ-кодов с различным конструктивным расстоянием. Алгоритм. Особенности реализации.
16. Коды Рида-Соломона. Построение, общие свойства.
17. Синдромные и норменные методы декодирования для кодов Рида-Соломона.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения Об изменениях в содержании учебной программы УВО по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Анализ данных	Кафедра дифференциальных уравнений и системного анализа	Изменений не требуется	Протокол № 12 от 25.04.2024

Зав. кафедрой дифференциальных уравнений
и системного анализа  Л. Л. Голубева

25.04.2024

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры

_____(протокол № ____ от _____ 202_ г.)

(название кафедры)

Заведующий кафедрой

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)

УТВЕРЖДАЮ

Декан факультета

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)