

Государственное образовательное учреждение
«Приднестровский государственный университет им. Т. Г. Шевченко»

Физико-технический институт

Физико-математический факультет

Кафедра высшей и прикладной математики и информатики

УТВЕРЖДАЮ

директор физико-технического
института

 Калошин Д.Н.

«30» 09 2024 г.



РАБОЧАЯ ПРОГРАММА

по дисциплине

**Б1.В.02 «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ ДАННЫХ
И КРИПТОГРАФИИ»**

на 2024/2025 учебный год

Направление

01.04.01 «Математика»

Профиль

«Математика. Преподавание математики и информатики»

Квалификация

магистр

Форма обучения

очная

ГОД НАБОРА 2023

Тирасполь 2024

Рабочая программа дисциплины «Математические основы кодирования данных и криптографии» разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки 01.04.01 «Математика» и основной профессиональной образовательной программы по профилю подготовки «Математика. Преподавание математики и информатики».

Составитель рабочей программы:

профессор Щербаков В.А.

Рабочая программа утверждена на заседании кафедры ВиПМиИ
«30» августа 2024 г. протокол № 1

Зав. кафедрой, отвечающий за реализацию дисциплины

« 03 » сентября 2024 г. Коровай А.В.

Зав. выпускающей кафедрой высшей и прикладной математики и информатики

« 03 » сентября 2024 г. Коровай А.В.

1. Цели и задачи освоения дисциплины

Целью освоения дисциплины «Математические основы кодирования данных и криптографии» является освоение базовых знаний в области защиты информации, анализа стойкости алгоритмов шифрования, разработки надежных протоколов защищенной передачи данных, помехоустойчивой передачи сообщений, теории информации, теории кодирования, а также ознакомление студентов с новыми применениями алгебраических структур, полученными в последние 10-15 лет.

Задачами освоения дисциплины «Математические основы кодирования данных и криптографии» является применение знаний, умений и навыков, приобретенных магистрантами при изучении дисциплины при написании выпускной работы.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.02 «Математические основы кодирования данных и криптографии» относится к дисциплинам по выбору блока Б1 части, формируемой участниками образовательных отношений учебного плана направления 01.04.01 «Математика», профиль «Математика. Преподавание математики и информатики», квалификация – магистр.

Курс занимает особое место в учебном плане среди дисциплин факультета по его значению. Вместе с курсами по программированию, курс Б1.В.02 «Математические основы кодирования данных и криптографии» составляет основу образования студента в части современных информационных технологий. Курс рассчитан на студентов, имеющих подготовку по предшествующим курсам, касающихся основ программирования с использованием алгоритмических языков, алгебры и теории чисел, теории вероятности. В течение преподавания курса предполагается, что студенты знакомы с основными понятиями алгебры, комбинаторики, теории вероятности, информатики, которые читаются на факультете перед изучением данной дисциплины.

Знания, навыки и умения, приобретенные в результате прохождения курса, будут востребованы при выполнении курсовых и дипломных работ, связанных с разработкой прикладного программного обеспечения, а также информационных систем, ориентированных на многопользовательский режим работы, или же на работу в сети Интернет.

3. Требования к результатам обучения по дисциплине:

Изучение дисциплины «Математические основы кодирования данных и криптографии» направлено на формирование компетенций приведенных в таблице ниже:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения универсальной компетенции
<i>Обязательные профессиональные компетенции и индикаторы их достижения</i>		
	ПК-1 Способен на самостоятельное построение целостной картины дисциплины	ИД-1ПК-1 Знает: историю, теорию, закономерности и принципы построения и функционирования образовательных систем, роль и место образования в жизни личности и общества
		ИД-2ПК-1 Умеет: разрабатывать и реализовывать программы учебных дисциплин в рамках основной общеобразовательной программы

		ИД-3 _{ПК-1} Владеет: формами и методами обучения, в том числе выходящими за рамки учебных занятий: проектная деятельность, лабораторные эксперименты, полевая практика и т.п.
	ПК-2. Владеет методами математического моделирования при анализе глобальных проблем на основе глубоких знаний фундаментальных математических дисциплин и компьютерных наук	ИД-1_{ПК-2} Знает: преподаваемый предмет в пределах требований федеральных государственных образовательных стандартов и основной общеобразовательной программы, его истории и места в мировой культуре и науке ИД-2_{ПК-2} Умеет: обеспечивать коммуникативную и учебную «включенности» всех учащихся в образовательный процесс (в частности, понимание формулировки задания, основной терминологии, общего смысла идущего в классе обсуждения) ИД-3_{ПК-2} Владеет: предметно-педагогической ИКТ-компетентностью (отражающей профессиональную ИКТ-компетентность соответствующей области человеческой деятельности)
	ПК-7. Способен к организации учебной деятельности в конкретной предметной области (математика, физика, информатика)	ИД-1_{ПК-7} Знает: преподаваемый предмет в пределах требований федеральных государственных образовательных стандартов и основной общеобразовательной программы, его истории и места в мировой культуре и науке ИД-2_{ПК-7} Умеет: использовать информационные источники, следить за последними открытиями в области математики и знакомить с ними обучающихся, квалифицированно набирать математический текст, проводить различия между точным и (или) приближенным математическим доказательством, в частности, компьютерной оценкой, приближенным измерением, вычислением и др. ИД-3_{ПК-7} Владеет: основными математическими компьютерными инструментами визуализации данных, зависимостей, отношений, процессов, геометрических объектов; вычислений - численных и символьных; обработки данных (статистики); экспериментальных лабораторий (вероятность, информатика)

4. Структура и содержание дисциплины

4.1. Распределение трудоемкости в з.е./часах по видам аудиторной и самостоятельной работы студентов по семестрам:

Семестр	Количество часов						Форма контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самостоя- тельная ра- бота (СР)	
		Всего	Лекций (Л)	Практи- ческих занятий (ПЗ)	Лабора- торных занятий (ЛЗ)		
3	3/108	72	36	36	-	36	Зачет с оценкой
Итого	3/108	72	36	36	-	36	Зачет с оценкой

4.2. Распределение видов учебной работы и их трудоемкости по разделам дисциплины

№ раздела	Наименование разделов	Всего	Аудиторная работа			СР
			Л	ПЗ	ЛЗ	
1	Коды. Расстояние Хэмминга. Линейные коды. Границы. Коды Хэмминга. Синдром. Циклические коды. БЧХ коды.	48	18	18	-	12
2	N-арные квазигруппы. Коды с одним проверочным символом (ISBN-код). Тотально антикоммутативные квазигруппы. Ортогональность группоидов.	24	6	6	-	12
3	Криптография. Шифры с симметрическим ключом. Алгоритм Марковского. Алгоритм Эль-Гамала.	36	12	12	-	12
ИТОГО:		108	36	36	-	36

4.3. Тематические план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
Коды. Расстояние Хэмминга. Линейные коды. Границы. Коды Хэмминга. Синдром. Циклические коды. БЧХ коды.				
1	1	2	Поля. Линейные пространства.	Учебники, интернет
2		2	Расстояние Хэмминга	Учебники, интернет
3		2	Линейные коды.	Учебники, интернет
4		2	Код Хэмминга	Учебники, интернет
5		2	Код Хэмминга	Учебники, интернет

6		2	Синдром	Учебники, интернет
7		2	Циклические коды	Учебники, интернет
8		2	Циклические коды	Учебники, интернет
9		2	БЧХ коды	Учебники, интернет
Итого по разделу часов:		18		
N-арные квазигруппы. Коды с одним проверочным символом (ISBN-код). Тотально антикоммутативные квазигруппы. Ортогональность группоидов.				
10	2	2	Коды с одним проверочным символом. Ортогональность.	Учебники, интернет
11		2	Тотально антикоммутативные квазигруппы.	Учебники, интернет
12		2	Ортогональность группоидов.	Учебники, интернет
Итого по разделу часов:		6		
Криптография. Шифры с симметрическим ключом. Алгоритм Марковского. Алгоритм Эль-Гамала.				
13	3	2	Шифры с симметрическим ключом	Учебники, интернет
14		2	Алгоритмы Марковского	Учебники, интернет
15		2	Алгоритмы Эль-Гамала	Учебники, интернет
16		2	Алгоритм RSA.	Учебники, интернет
17		2	Электронная цифровая подпись Эль-Гамала.	Учебники, интернет
18		2	Электронная цифровая подпись RSA. Хэш-функция.	Учебники, интернет
Итого по разделу часов:		12		
ИТОГО:		36		

Практические (семинарские) занятия

№ п/п	Номер раздела дисциплины	Объем часов	Тема практических (семинарских) занятий	Учебно-наглядные пособия
Коды. Расстояние Хэмминга. Линейные коды. Границы. Коды Хэмминга. Синдром. Циклические коды. БЧХ коды.				
1	1	2	Линейные пространства и подпространства.	Учебники, интернет
2		2	Расстояние Хэмминга	Учебники, интернет
3		2	Линейные коды	Учебники, интернет
4		2	Границы	Учебники, интернет
5		2	Коды Хэмминга	Учебники, интернет
6		2	Синдром	Учебники, интернет

№ п/п	Номер раз- дела дисци- плины	Объем часов	Тема практических (семи- нарских) занятий	Учебно-наглядные пособия
7		2	Циклические коды	Учебники, интернет
8		4	БЧХ-коды	Учебники, интернет
Итого по разделу часов:		18		
N-арные квазигруппы. Коды с одним проверочным символом (ISBN-код). Тотально антикоммутативные квазигруппы. Ортогональность группоидов.				
10	2	2	Коды с одним проверочным символом (ISBN-код).	Учебники, интернет
11		2	Тотально антикоммутатив- ные квазигруппы	Учебники, интернет
12		2	Ортогональность	Учебники, интернет
Итого по разделу часов:		6		
Криптография. Шифры с симметрическим ключом. Алгоритм Марковского. Алгоритм Эль-Гамала.				
13	3	2	Шифры с симметрическим ключом	Учебники, интернет
14		2	Алгоритмы Марковского	Учебники, интернет
15		2	Алгоритмы Эль-Гамала	Учебники, интернет
16		2	Алгоритм RSA.	Учебники, интернет
17		2	Электронная цифровая под- пись Эль-Гамала.	
18		2	Электронная цифровая под- пись RSA. Хэш-функция.	
Итого по разделу часов:		12		
ИТОГО:		36		

Лабораторные занятия

Лабораторные занятия учебным планом не предусмотрены

Самостоятельная работа обучающегося

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
Раздел 1	1	Линейные коды. (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	2
	2	Код Хэмминга. (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	2
	3	Циклические коды (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	2

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
	4	БЧХ-коды (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	2
	5	Коды Рида-Соломона (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	4
Итого по разделу часов:			12
Раздел 2	6	Коды с одним проверочным символом. (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
	7	n-арные квазигруппы (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
	8	ISBN-код (Самостоятельная работа с литературой с последующей защитой изученного материала)	3
	9	Ортогональность (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
Итого по разделу часов:			12
Раздел 3	10	Шифры с симметрическим ключом (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
	11	Алгоритмы Марковского (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
	12	Алгоритм Эль-Гамала (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	3
	13	Система RSA (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	2
	14	Электронная цифровая подпись RSA. Хэш-функция. (Самостоятельная работа с литературой, выполнение упражнений с последующей защитой изученного материала)	1
Итого по разделу часов:			12
ИТОГО:			36

5. Примерная тематика курсовых проектов (работ)

Курсовые проекты и курсовые работы учебным планом не предусмотрены.

6.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

6.1. Обеспеченность обучающихся учебниками, учебными пособиями:

№ п/п	Наименование учебника, учебного пособия	Автор	Год издания	Количество экземпляров	Электронная версия	Место размещения электронной версии
Основная литература						
1	Основы теории квазигрупп и луп	Белоусов В.Д.	1967	-	есть	https://www.twirpx.com
2	Элементы теории квазигрупп и ее приложений	Щербаков В.А.	2017	-	есть	https://www.twirpx.com
3	Спецкурс по теории квазигрупп	Белоусов В.А.	1982	-	есть	https://www.twirpx.com
4	Введение в теорию кодирования	Соловьева Ф.И.	2006	-	есть	https://www.twirpx.com
5	Алгебраическая теория кодирования	Бэрлекэмп Е.Р.	1971	-	есть	https://www.twirpx.com
Дополнительная литература						
1	Quasigroups and Loops: Introduction	Pflugfelder Н.О.	1990	-	есть	https://ibn.idsi.md/
2	Введение в криптографию	Яценко В.В.	2012	-	есть	http://cryptography.ru/
Итого по дисциплине: 0 % печатных изданий; 100 % электронных						

6.2. Программное обеспечение и Интернет-ресурсы

<https://www.twirpx.com>,

<https://ibn.idsi.md/>

6.3. Методические указания и материалы по видам занятий

Учебные пособия по дисциплине «Математические основы кодирования данных и криптографии», тексты лекций.

<http://www.karlin.mff.cuni.cz/~drapal/speccurs.pdf>

tc.nsu.ru/uploads/codingtheory.pdf

<http://www.mastermathmentor.com/mmm/content/files/crypt/Ciphering%20manual.pdf>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Для обеспечения освоения дисциплины необходимо наличие стандартных учебных аудиторий.

8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ:

Курс предполагает овладение студентами основными понятиями, определениями и методами общей теории кодирования и криптографии, ознакомить их с методами исследовательской работы при изучении тем курса. Для лучшего усвоения дисциплины рекомендуется изучать темы по конспектам лекций и базовым учебникам с последующей сдачей

зачета; конспектировать вопросы, предназначенные для самостоятельного изучения, пользуясь базовыми учебниками и методическими рекомендациями по теме (самостоятельная работа) с последующей защитой на индивидуальных консультациях; решать контрольные задания, пользуясь методическим пособием во время плановых работ на индивидуальных консультациях.

9. ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ ДАННЫХ И КРИПТОГРАФИИ»

Курс II

группа ФТ23ДР68МА (602)

семестр 3

2024-2025 учебный год

Преподаватель – лектор Щербаков В.А.

Преподаватель, ведущий практические занятия Щербаков В.А.

Кафедра высшей и прикладной математики и информатики

Семестр	Количество часов						Форма контроля
	Трудоемкость, з.е./часы	В том числе					
		Аудиторных				Самостоя- тельная ра- бота (СР)	
		Всего	Лекций (Л)	Практи- ческих занятий (ПЗ)	Лабора- торных занятий (ЛЗ)		
3	3/108	72	36	36	-	36	Зачет с оценкой

Форма текущей аттеста- ции	Расшифровка	Минимальное количество бал- лов	Максимальное количество бал- лов
III семестр			
Посещение занятий	<i>Рассчитывается со- гласно приложению 1</i>	0	10
Работа на практических занятиях	<i>Рассчитывается со- гласно приложению 2</i>	0	10
Самостоятельное реше- ние упражнений по всем разделам	<i>1,5 балла за одно само- стоятельно решённое упражнение</i>	0	30
Самостоятельный разбор следующих тем «Шифры с симметриче- ским ключом», «Система RSA»	<i>По 10 баллов за тему</i>		20
Итого количество баллов по текущей аттестации		45	70
Промежуточная аттеста- ция	Зачет с оценкой	10	30
Итого по дисциплине:		55	100

Приложение 1

Процент посещенных занятий	Начисляемые баллы
0-49%	0 баллов
50-54%	1 балл
55-59%	2 балла
60-64%	3 балла
65-69%	4 балла
70-74%	5 баллов
75-79%	6 баллов
80-84%	7 баллов
85-89%	8 баллов
90-94%	9 баллов
95-100%	10 баллов

*В случае посещения студентом менее чем 85% лекций, предусмотренных учебной программой по дисциплине, для получения рейтингового балла, начисляемого по данному критерию, студент обязан предоставить преподавателю конспект пропущенных лекций. Пропущенные практические занятия отрабатываются в установленном порядке.

Приложение 2

Средняя оценка полученных оценок на занятиях	Начисляемые баллы
3	6 баллов
3,5	7 баллов
4	8 баллов
4,5	9 баллов
5	10 баллов