

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЛГПУ»)**

Структурное подразделение **Институт физико-математического
образования, информационных и обслуживающих технологий**
Кафедра информационных образовательных технологий и систем

УТВЕРЖДАЮ
Директор ИФМОИОТ
 **Е.Е. Горбенко**
«» _____ **2023 г.**

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Теория кодирования

**По направлению подготовки 44.03.05 Педагогическое образование (с двумя
профилями подготовки)**

Профиль подготовки Физика. Информатика

Квалификация выпускника бакалавр

Форма обучения очная, заочная

Курс ОФО – 3 курс

Луганск, 2023

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы для подготовки бакалавров по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) очной формы обучения.

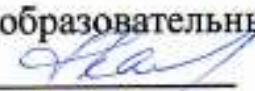
Рабочая программа учебной дисциплины разработана в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденным приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. №125 (с изменениями и дополнениями) и Профессиональным стандартом, утвержденным Приказом Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)"» от 18 октября 2013 г. № 544н.

СОСТАВИТЕЛЬ:

доцент кафедры информационных образовательных технологий и систем, кандидат физико-математических наук, доцент Швыров Вячеслав Владимирович

Утверждена на заседании кафедры фундаментальной математики
Протокол от «24» ноября 2023 г. №8

Заведующий кафедрой информационных образовательных технологий и систем


(подпись)

Одобрена на заседании учебно-методической комиссии Института физико-математического образования, информационных и обслуживающих технологий

Протокол от «06» декабря 2023 г. №5

Председатель учебно-методической комиссии Института физико-математического образования, информационных и обслуживающих технологий


(подпись)

О.В. Давыскиба

СОГЛАСОВАНО:

Заведующий учебно-методическим отделом


(подпись)

В.В. Савенков

1. Цели и задачи дисциплины

Цели изучения дисциплины: изучение методов кодирования информации, основных алгоритмов кодирования и методов коррекции ошибок.

Задачи:

- формирование профессиональных компетенций, позволяющих выполнять кодирование и декодирование информации;
- изучение основных подходов для обеспечения целостности, доступности и конфиденциальности информации в компьютерных системах;
- формирование навыков использования различных методов кодирования;
- формирование базы знаний для самостоятельного решения задач в теории кодирования и решения прикладных задач.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Теория кодирования» относится к вариативной части учебного плана (Б1.В.03.ДВ.02.02). Дисциплина реализуется кафедрой информационных образовательных технологий и систем (12) Институт физико-математического образования, информационных и обслуживающих технологий ФГБОУ ВО «ЛГПУ».

Необходимым условием для освоения учебной дисциплины являются знания принципы, методы и средства решения стандартных задач профессиональной деятельности.

Содержание дисциплины «Теория кодирования» является логическим продолжением содержания дисциплин «Объектно-ориентированное программирование» и основой для дальнейшего освоения дисциплин: написания разделов выпускной квалификационной работы.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код по ФГОС ВО	Индикатор достижения	Результаты обучения по дисциплине
Универсальные		
Общепрофессиональные		
Профессиональные		
ПК-1. Способен проектировать и реализовывать основные общеобразовательные программы различных	ПК.1.1. Формулирует личностные, предметные и метапредметные результаты обучения средствами информационно-	ПК.1.1. Формулирует личностные, предметные и метапредметные результаты обучения средствами информационно-

уровней и направленности с использованием современных предметно-методических подходов и образовательных технологий	коммуникационных технологий и математических дисциплин ПК.1.2. Осуществляет отбор предметного содержания, методов, приемов и технологий, в том числе информационных, обучения, организационных форм учебных занятий, средств диагностики в соответствии с планируемыми результатами обучения. ПК.1.3. Формирует познавательную мотивацию обучающихся к изучению математики и информатики в рамках урочной и внеурочной деятельности	коммуникационных технологий и математических дисциплин ПК.1.2. Осуществляет отбор предметного содержания, методов, приемов и технологий, в том числе информационных, обучения, организационных форм учебных занятий, средств диагностики в соответствии с планируемыми результатами обучения. ПК.1.3. Формирует познавательную мотивацию обучающихся к изучению математики и информатики в рамках урочной и внеурочной деятельности
--	---	---

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (2 зач. ед.)	
	Очная форма	Заочная форма
Общая учебная нагрузка (всего)	72	
Обязательная аудиторная учебная нагрузка (всего часов), в том числе:		
Лекции	14	
Семинарские занятия		
Практические занятия		
Лабораторные работы	18	
Курсовая работа / курсовой проект		
Другие формы организации учебного процесса (контрольные работы, индивидуальные занятия, консультации и др.)	27	
Самостоятельная работа студента (всего)	13	
Форма аттестация	Экзамен	

4.2. Содержание дисциплины

Тема 1. Введение. Кодирование информации

Основные понятия информационной безопасности. Конфиденциальность. Ценность информации. Целостность информации. Классификация информационных угроз. Методологии оценки угроз. Методики STRIDE и DREAD. Стандарты информационной безопасности.

Тема 2. Сжатие информации. Алгоритм Хаффмана

Методы сжатия данных. Сжатие с потерями. Сжатие без потерь. Алгоритм Хаффмана. Защита информации в архивах. Технологии и уровни RAID.

Зеркалирование. Технология чередования. Составные уровни RAID. Методы восстановления информации.

Тема 3. Коды Хемминга

Понятие аутентификации и авторизации. Базовая аутентификация. Основные требования к паролям. Биометрическая аутентификация. Протоколы аутентификации. Форматы токенов аутентификации. Аутентификация в корпоративных сетях. Методы разграничения доступа.

Тема 4. Линейные коды

Использование командной строки. Основные системные утилиты. Брандмауэр Windows. Входящие и исходящие правила. Локальные политики безопасности. Групповые политики безопасности. Анализ безопасности. Шаблоны безопасности. Контроль над использованием сменных носителей. Черные и белые списки устройств.

Тема 5. Групповые коды

Основные понятия и определения. Криптография и криптоанализ. Классические криптосистемы. Шифр Сцигала. Магические квадраты. Шифр Трисемуса. Шифр Плейфера. Обзор современных криптосистем. Блочные шифры. Сеть Фейстеля. Применение сети Фейстеля в DES. Криптосистема RSA. Криптосистема AES. Современные хеш-функции.

Тема 6. Коды БЧХ

Понятие вируса. Классификация вирусов. Макровирусы. Загрузочные вирусы. Файловые вирусы. Троянские программы. Основные источники заражения вирусами. Методы внедрения руткитов. Методы профилактики. Современные клавиатурные шпионы. Общая модель аппаратного ввода. Методы внедрения шпионов. Методы обнаружения клавиатурных шпионов.

Тема 7. Коды Рида-Соломона

Понятие спама. Методы защиты от спама. Капча виды капчи. Графическая капча. Особенности защиты веб-ресурсов. Анализ уязвимостей с помощью утилиты Burp Suite. Защита от SQL-инъекций.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
5 семестр /			
1	Тема 1. Введение. Кодирование информации	2	
2	Тема 2. Сжатие информации. Алгоритм Хаффмана	2	
3	Тема 3. Коды Хемминга	2	
4	Тема 4. Линейные коды	2	
5	Тема 5. Групповые коды	2	
6	Тема 6. Коды БЧХ	2	
7	Тема 7. Коды Рида-Соломона	2	
Итого:		14	

4.4. Практические занятия

Не предусмотрено учебным планом

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
3 семестр / 4-5 триместр			
1	Простые коды. Коды Грея	2	
2	Методы сжатия данных. Алгоритм Хаффмана	2	
3	Коды Хемминга	2	
4	Линейные коды	2	
5	Групповые коды	2	
6	Коды БЧХ	2	
7	Коды Рида-Соломона	2	
8	Систематические коды	2	
9	Коды корректирующие ошибки	2	
Итого:		18	

4.6. Самостоятельная работа студентов

№ п/п	Название раздела / темы	Вид самостоятельной работы	Объем часов	
			Очная форма	Заочная форма
3 семестр / 4-5 триместр				
1	Коды в криптографии	Конспект лекций	2	
2	Обзор методов кодирования	Конспект лекций	2	
3	Групповые коды. Декодирование данных	Конспект лекций	2	
4	Коды Рида-Соломона. Особенности использования	Конспект лекций	2	
5	Контроль целостности информации. Основные алгоритмы контроля целостности.	Конспект лекций	5	
Итого:			13	

4.7. Курсовые работы / проекты

Не предусмотрено учебным планом

5. Методическое обеспечение, образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий.

Наряду с методикой традиционной лекционно-практической работы предусмотрено использование активных форм и методов учебной деятельности, в том числе: учебные дискуссии, беседы, мозговой штурм.

Методика проблемно-диалогического обучения применяется в процессе лекционной работы над учебным материалом в каждой из тем учебной дисциплины.

Методика обучения в сотрудничестве с применением командных, групповых видов работы используется в процессе организации лабораторных работ.

Методика исследовательской деятельности используется как основа для организации самостоятельной работы студентов в объеме учебных тем.

Применяются средства мультимедиа: презентации, видео, базы ЭОР.

Информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный во внутренней сети или т.п.) при подготовке к лекциям, лабораторным работам и самостоятельной работе.

Работа в команде, проектная деятельность: совместная работа студентов в группе при выполнении лабораторных работ.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы в следующих формах: выполнение лабораторных работ; защита лабораторных работ.

Промежуточный контроль по результатам освоения дисциплины проходит в форме зачета (включает в себя ответ на теоретические вопросы и выполнение тестового задания).

Система оценивания учебных достижений студентов, оценочные средства представлены в фонде оценочных средств к рабочей программе учебной дисциплины (в приложении).

7. Учебно-методическое и программно-информационное обеспечение дисциплины

А) основная литература:

1. Барычев С.Г. Основы современной криптографии / С.Г. Барычев, Р.Е. Серов. – М. : Горячая линия – Телеком, 2002. – 152 с.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М. : МЦНМО, 2003. – 326 с.
3. Глухих В.И. Информационная безопасность и защита данных: учебное пособие / В.И. Глухих. – Иркутск : Изд-во Иркутского государственного технического университета, 2011. – 250 с.
4. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М. : ТВП, 2001. – 254 с.

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

Б) дополнительная литература:

1. Климов А.П. Реестр Windows 7 / А.П. Климов. – С-П. : Питер, 2010. – 325 с.
2. Романец Ю.В. Защита информации в компьютерных системах и сетях. / Ю.В. Романец, И.А. Тимофеев, В.Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с.
3. Складов Д.В. Искусство защиты и взлома информации / Д.В. Складов. – СПб.:БХВ-Петербург, 2004. – 288с.

В) Интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины

Лекционные занятия: комплект электронных презентаций/слайдов, аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и т.п.

Лабораторные работы: компьютерный класс, оснащенный мультимедийным проектором, интерактивной доской, сетевой инфраструктурой и организованным доступом в Интернет, пакеты ПО MS Word, MS Excel , среда Visual Studio 2022.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде и т.п.

9. Лист дополнений и изменений

[illegible]