МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ:

В.о. декана факультету
комп'ютерних інформаційних
технологій

Ігор ЯКИМЕНКО

«__» _____ 20___р.

ЗАТВЕРДЖУЮ:

В. о. проректора з науково-
педагогічної роботи

Віктор ОСТРОВЕРХОВ

«__» _____ 20___р

РОБОЧА ПРОГРАМА

з дисципліни

«ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ»

Ступінь вищої освіти – **бакалавр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека та захист інформації**
Освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	СРС (год.)	Разом (год.)	Екзамен (сем)
Денна	1	2	30	30	4	8	78	150	2

31.08.2023

Тернопіль – 2023

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності – 125 Кібербезпека та захист інформації, затвердженої на засіданні Вченою радою ЗУНУ, протокол № 9 від 15.06.2022 р.

Робочу програму склав доцент кафедри спеціалізованих комп'ютерних систем, к.т.н. Сегін Андрій Ігорович

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри кібербезпеки — Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол № 1 від 30.08.2023 р.

Керівник групи забезпечення спеціальності — Василь ЯЦКІВ

Гарант ОП — Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни „Теорія інформації та кодування ”

Дисципліна – Теорія інформації та кодування	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів – 5	Галузь знань 12 - Інформаційні технології	Статус дисципліни – обов’язкова Мова навчання - українська
Кількість залікових модулів – 3	Спеціальність - 125 Кібербезпека та захист інформації	Рік підготовки – 1 Семестр – 2
Кількість змістових модулів –2	Ступінь вищої освіти – бакалавр	Лекції – 30 год. Лабораторні заняття – 30 год.
Загальна кількість годин – 150		СРС – 78 год, тренінг, КПІЗ – 8 год. Індивідуальна робота – 4 год.
Тижневих годин: 10 год., з них аудиторних – 4 год.		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни «Теорія інформації та кодування»

2.1. Мета завдання дисципліни

Мета дисципліни «Теорія інформації і кодування» полягає в ознайомленні студентів з теоретичними основами оцінки інформаційних процесів, організації ефективного завадостійкого кодування з виявленням і виправленням помилок, алгоритмів кодування та декодування даних, сучасних методів кодування даних в каналах зв’язку, а також отриманні студентами практичних навичок в створенні як апаратних так і програмних кодерів і декодерів з використанням сучасних програмних і апаратних засобів.

2.2 Завдання вивчення дисципліни полягає у

– здобутті студентами теоретичних знань про принципи та методи оцінки інформативності повідомлень,

– формування кодів та оцінки їх ефективності,

– здобуття практичного досвіду вирішення завдань завадостійкого кодування,

– розробки апаратних та програмних кодерів-декодерів,

– освоєння сучасних методів кодування даних.

Проведення лекційних занять забезпечує знання основ теорії інформації та теорії кодування, принципів та методів побудови завадостійких кодів з виявленням та виправленням помилок, методів та засобів створення апаратних та програмних кодерів та декодерів та уміння оцінювати кількість інформації, надлишковість повідомлень, пропускну здатність каналів зв’язку, розробляти системотехнічні та програмні засоби для кодування та декодування повідомлень з використанням різних типів сучасних кодів, застосовувати сучасні методи кодування для реальних об’єктів з метою виявлення та усунення помилок у відповідності з програмою та робочим планом та формуванні у студентів цілісної системи теоретичних знань з курсу «Теорія інформації та кодування».

Проведення практичних занять забезпечує здатність розраховувати інформаційні характеристики об'єктів, обирати і реалізовувати адекватні способи та засоби кодування даних.

2.3.Найменування та опис компетентностей, формування котрих забезпечує вивченя дисципліни

Знання та розуміння предметної області та розуміння професії

Здатність до використання програмних та програмноапаратних комплексів засобів захисту інформації в інформаційнотелекомунікаційних (автоматизованих) системах

Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

2.4 Передумови для вивчення дисципліни.

Теоретичною базою вивчення дисципліни “Теорія інформації і кодування” є попередні навчальні дисципліни: «Вища математика», «Спеціальні розділи математики», «Теорія ймовірності і математична статистика», «Основи системної інженерії», «Програмування» та ін.

2.5. Результати навчання

Виконувати аналіз та декомпозицію інформаційно телекомунікаційних систем

Аналізувати проекти інформаційно телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних

Забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.

3. Програма навчальної дисципліни «Теорія інформації та кодування»

Змістовний модуль 1. Основи теорії інформації".

Тема 1. Основні поняття теорії інформації.

Поняття інформації, кількість інформації, ентропії, середня кількість інформації, пропускна здатність каналу для дискретних повідомлень.

Література 1-9.

Тема 2. Міри оцінки кількості інформації та ентропії

Визначення кількості інформації та ентропії за Хартлі, Шеноном та іншими оцінками.

Література 1-9.

Тема 3. Визначення кількості інформації та ентропії для багатоканальних об'єктів.

Кількість інформації, її визначення. Поняття ентропії.

Література 1-9.

Тема 4. Визначення умовної кількості інформації та ентропії для статистично залежних джерел. Умовна імовірність подій. Визначення кількості інформації для статистично залежних подій. Визначення середньої кількості інформації та середньої ентропії для статистично залежних джерел інформації.

Змістовний модуль 2. Ефективне та завадозахищене кодування

Тема 5. Загальна характеристика ефективного кодування.

Теорема Шенона про кодування при відсутності завад. Методика Шенона-Фано. Кодування блоками.

Література 1-9.

Тема 6. Алгоритм кодування методом Шенона-Фано та Хаффмена.

Побудови оптимальних кодів методами Шенона-Фано та Хаффмена. Префіксні коди.

Література 1-9.

Тема 7. Завадостійке кодування.

Загальна характеристика завадозахищених кодів. Кодова відстань і коректуюча здатність кодів. Коди з повторенням, коди з повторенням та інверсією.

Коди із захистом за паритетом по горизонталі та по вертикалі. Методика формування кореляційного та манчестерського коду, алгоритми виявлення та виправлення помилок.\

Література 1-9.

Тема 8. Коди Грея.

Методика побудови кодів Грея та їх властивості.

Література 1-9.

Тема 9. Лінійні групові коди.

Коди Хемінга. Групові коди та принципи формування утворюючої матриці.

Література 1-9.

Тема 10. Циклічні коди.

Методика формування циклічних кодів, алгоритми виявлення та виправлення помилок.

Література 1-9.

Тема 11. Коди Ріда-Соломона.

Методика побудови кодів та виправлення помилок.

Література 1-9.

Тема 12. Коди БЧХ

Методика кодування та декодування даних з використанням методики БЧХ.

Література 1-9.

Тема 13. Коди в системі залишкових класів.

Основи переведення даних в СЗК та навпаки. Типи кодувань в СЗК.
Література 1-9.

Тема 14. Коди Галуа.

Теорія полів Галуа. Методика формування кодів Галуа та їх властивості.
Література 1-9.

4. Структура залікового кредиту дисципліни «Теорія інформації та кодування»

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Тренінг, КПІЗ	Контрольні заходи
Змістовний модуль 1. Основи теорії інформації.						
Тема 1. Основні поняття теорії інформації.	2	2	5	1	2	Поточне опитування
Тема 2. Міри оцінки кількості інформації та ентропії.	2	2	5			Поточне опитування
Тема 3. Визначення кількості інформації та ентропії для багатоканальних об'єктів.	2	2	5			Поточне опитування
Тема 4. Визначення умовної кількості інформації та ентропії для статистично залежних джерел.	2	2	5			Поточне опитування
Змістовний модуль 2. Ефективне та завадозахищене кодування						
Тема 5. Загальна характеристика ефективного кодування.	2	2	5	1	2	Поточне опитування
Тема 6. Алгоритм кодування методом Шенона-Фано та Хаффмена.	2	2	5			Поточне опитування
Тема 7. Завадостійке кодування.	2	2	6			Поточне опитування
Тема 8. Коди Грея.	2	2	6			Поточне опитування
Тема 9. Лінійні групові коди.	2	2	6	2	4	Поточне опитування
Тема 10. Циклічні коди.	2	2	6			Поточне опитування
Тема 11. Коди Ріда-Соломона.	2	2	6			Поточне опитування
Тема 12. Коди БЧХ	2	2	6			Поточне опитування
Тема 13. Коди в системі залишкових класів.	4	4	6			Поточне опитування
Тема 14. Коди Галуа.	2	2	6			Поточне опитування
Разом	**30**	**30**	**78**	**4**	**8**	

5. Теми лабораторних робіт.

Лабораторна робота № 1

Тема: Основні поняття теорії інформації

Мета: Ознайомлення з основними поняттями і визначеннями теорії інформації та підходами до кількісної оцінки інформаційних характеристик.

Питання для обговорення:

1. Підходи до визначення поняття «інформація».
2. Визначення ентропії з позиції теорії інформації.
3. Відмінність між ентропією та кількістю інформації.
4. Зв'язок між кількістю інформації та імовірнісними характеристиками повідомлення.
5. Елементи теорії імовірності: визначення імовірнісних характеристик повідомлень та подій.

Література: 2, 3, 4, 6.

Лабораторна робота № 2

Тема: Міри оцінки кількості інформації та ентропії

Мета: Вивчення кількісних оцінок інформації та ентропії.

Питання для обговорення:

1. Визначення кількості інформації за Хартлі.
2. Визначення кількості інформації за Шеноном.
3. Середня кількість інформації джерела повідомлень.
4. Визначення кількості інформації для багатоканальних джерел інформації

Література: 2, 3, 4, 6.

Лабораторна робота № 3

Тема: Визначення кількості інформації та ентропії для статистично залежних джерел інформації.

Мета: Вивчення кількісних оцінок інформації та ентропії для стстистично залежних повідомлень.

1. Визначення імовірності статистично залежних повідомлень.
2. Визначення кількості інформації статистично залежних повідомлень.
3. Методи визначення ентропії статистично залежних повідомлень.

Література: 2, 3, 4, 6.

Лабораторна робота № 4

Тема: Загальна характеристика ефективного кодування

Мета: Вивчення критеріїв оцінки кодування повідомлень та класифікація методів кодування.

Питання для обговорення:

1. Теорема Шенона для кодування повідомлень в каналах без завад.
2. Незавадостійке і завадостійке кодування.
3. Надлишковість повідомлень.
4. Теорема Шенона для повідомлень в каналах із завадами.

Література: 1, 5, 8

Лабораторна робота № 5

Тема: Алгоритм кодування методом Шенона-Фано.

Мета: Вивчення побудови кодів методом Шенона-Фано

Питання для обговорення:

1. Методика побудови кодів Шенона-Фано.
2. Кодування блоками.
3. Загальна характеристика кодів Шенона-Фано.

Література: 1, 5, 8

Лабораторна робота № 6

Тема: Алгоритм кодування методом Хаффмена

Мета: : Вивчення побудови кодів методом Хаффмена

Питання для обговорення:

1. Методика побудови кодів Хаффмена.
2. Загальна характеристика кодів Хаффмена.
3. Префіксні коди.

Література: 1, 5, 8

Лабораторна робота № 7

Тема: Лінійні групові коди

Мета: Вивчення методики побудови групових кодів, їх властивостей та виправлення помилок на їх основі.

Питання для обговорення:

1. Завадостійке кодування, поняття Хемінгової відстані та визначення надлишковості коду на основі мінімальної Хемінгової відстані та коректуючих властивостей коду.
2. Загальна характеристика лінійних групових кодів.
3. Коди Хемінга, методика їх побудови та виправлення помилок.
4. Лінійні групові коди, методика їх побудови та виправлення помилок

Література: 1, 7, 9.

Лабораторна робота № 8

Тема: Циклічні коди

Мета: Вивчення принципів побудови циклічних кодів

Питання для обговорення:

1. Ідея побудови циклічних кодів та їх властивості.
2. Неприводимі многочлени та побудова на їх основі циклічних кодів.
3. Побудова циклічних кодів на основі утворюючої матриці.
4. Принципи формування синдрому помилок в циклічних кодах.
5. Побудова циклічних кодів шляхом множення на утворюючий многочлен.
6. Виявлення та виправлення помилок в циклічних кодах.

Література: 1, 7, 9.

Лабораторна робота № 9

Тема: Коди Ріда-Соломона

Мета: Вивчення методики побудови кодів Ріда-Соломона та їх характеристик.

Питання для обговорення:

1. Поля галуа.
2. Методика побудови кодів Ріда-Соломона на основі поля Галуа.
3. Алгоритм Берлекампа-Мессі для визначення позиції помилки.
4. Виправлення помилок методом Форні.

Література: 1, 7, 9.

Лабораторна робота № 10

Тема: Коди БЧХ

Мета: Загальна характеристика кодів БЧХ.

Питання для обговорення:

1. Загальна характеристика кодів БЧХ.
2. Методика побудови кодів БЧХ.
3. Виявлення та виправлення помилок в кодах БЧХ.

Література: 1, 7, 9.

Лабораторна робота № 11

Тема: Коди Грея

Мета: Вивчення методики побудови кодів Грея та їх характеристик.

Питання для обговорення:

1. Характеристика кодів Грея.
2. Методика побудови кодів Грея.
3. Методика апаратного формування кодів Грея.

Література: 1, 7, 9.

Лабораторна робота № 12

Тема: Манчестерський код

Мета: Вивчення методик побудови Манчестерського коду та виправлення помилок на його основі.

Питання для обговорення:

1. Методика побудови Манчестерського коду.
2. Виправлення помилок в Манчестерському коді.
3. Властивості манчестерського коду та його застосування.

Література: 1, 7, 9.

Лабораторна робота № 13

Тема: Основи переведення даних в СЗК та навпаки. Типи кодувань в СЗК

Мета: Вивчення непозиційної системи числення системи залишкових класів та побудова на її основі способів кодування.

Питання для обговорення:

1. Китайська теорема про залишки.
2. Загальна характеристика системи залишкових класів та арифметичні операції в ній.
3. Представлення кодів в системі залишкових класів, їх властивості.

Література: 1, 7, 9.

Лабораторна робота № 14

Тема: Коди Галуа

Мета: Вивчення методик побудови кодів Галуа та їх властивостей.

Питання для обговорення:

1. Загальні положення теорії полів, поля кільця, групи.
2. Методика побудови кодів Галуа різної розрядностіна основі ключів.
3. Властивості кодів Галуа та їх застосування.
4. Коректуючі властивості коду Галуа та виправлення помилок.
5. Перспективи використання кодів Галуа та системи залишкових класів.

Література: 1, 4, 8.

6. Комплексне практичне індивідуальне завдання (КПІЗ) з дисципліни

Індивідуальне завдання з курсу «Теорія інформації та кодування» виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту.

Метою виконання КПІЗ є оволодіння навиками оцінювання ступеня ризику при вирішенні конкретних задач кібербезпеки

Побудувати завадодостійкий циклічний код. В якості породжуючого многочлена коду взяти неприводимий примітивний поліном r(x) з таблиці варіантів.

1. По заданому поліному побудувати породжуючу і перевірочну матриці в систематичному вигляді.

2. Оцінити кориктуючу здатність побудованого коду і розрахувати характеристики його завадостійкості при заданій ймовірності спотворення одного символу коду.

3. Розробити алгоритм і програму захисту від спотворень під впливом завад даних з текстового файлу довільної довжини за допомогою розробленого завадостійкого коду.

4. Змоделювати процес проходження отриманого коду через двійковий симетричний канал зв'язку з імовірністю спотворення кожного символу коду p з таблиці варіантів. Додати кілька пакетів помилок в середині слова і кінці.

5. Розробити алгоритм і програму декодування спотвореного в каналі зв'язку коду шляхом перевірки наявності помилки в кожному блоці і виправлення помилки за критерієм найменшої відстані.

6. Порівняти файли даних: вихідний і отриманий в результаті декодування, порахувати кількість спотворених символів і порівняти його з характеристиками завадостійкості коду, обчисленими в п.2.

7. Залежно від результатів попереднього кроку змінити характеристику каналу зв'язку - імовірність спотворення p (збільшити, якщо якість передачі даних добра і зменшити, якщо погана) і повторити пункти 4-6. Зробити висновки про відповідність побудованого коду характеристикам каналу зв'язку.

7. Самостійна робота

№ п/п	Тематика
1	Кількість інформації та ентропія.
2	Оцінки кількості інформації.
3	Імовірнісні характеристики кодів.
4	Теорема Шенона про ефективне кодування.
5	Методика кодування Шенона-Фано.
6	Методика кодування Хаффмена.
7	Характеристики завадостійкого кодування.
8	Лінійні групові коди
9	Коди Хемінга.
10	Модифіковані коди Хемінга
11	Коди з перевіркою на парність.
12	Коди з перевіркою на парність по горизонталі і вертикалі.

13	Манчестерські коди.
14	Циклічні коди.
15	Коди БЧХ.
16	Коди в системі залишкових класів.
17	Коди Галуа.
18	Інші сучасні методи кодування.

8. Тренінг з дисципліни.

Написати програму, що читає побайтно заданий файл і підраховує кількість поява кожного з 256 можливих знаків.

Можна використовувати програму (макрос inByte) на мові VBA для Excel (міститься у файлі hw_tits2005.xls).

Дослідити за допомогою розробленої програми файли різних типів (.jpeg, .gif, .bmp, .txt, .doc, .xls, .exe).

Для кожного досліджуваного в роботі файлу зробити наступне:

• побудувати діаграму, що показує число кожного з 256 байт в досліджуваному файлі.

• розглядаючи знаки (байти) файлу як повідомлення, а частоти їх появи як імовірності, представити файл як імовірнісний джерело повідомлень. Обчислити ентропію цього джерела.

Пояснити спостережувані на діаграмах особливості.

Грунтуючись на побудованих діаграмах і обчислених значеннях ентропії, вказати, які з розглянутих файлів можуть бути стиснуті більше і чому.

Відповіді на дані питання сформулювати у вигляді висновків.

Результати роботи представити у вигляді роздрукованого звіту.

9. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

10. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Теорія інформації та кодування» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- стандартизовані тести;
- поточне опитування;
- залікове модульне тестування та опитування;
- презентації результатів виконаних завдань;
- оцінювання результатів КПІЗ;
- завдання на лабораторному обладнанні, тощо;
- ректорська контрольна робота;
- екзамен;

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Теорія інформації та кодування» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Семестр 2 – іспит

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ)	Заліковий модуль 4 (письмовий екзамен)
20 %	20 %	20 %	40 %
1. Усне опитування на заняттях (7 тем по 2 бали) - max 14 балів. 2. Письмова робота - max 51 бал. 3. Практичне завдання (7 лабораторних робіт по 5 балів)- max 35 балів.	1. Усне опитування на заняттях (7 тем по 2 балів) - max 14 балів. 2. Письмова робота - max 51 бал. 3. Практичне завдання (7 лабораторних робіт по 5 балів) - max 35 балів.	1. Підготовка КПІЗ - max 40 балів. 2. Захист КПІЗ - max 40 балів. 3. Участь у тренінгах - max 20 балів	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -14
2	Персональні комп'ютери	1 -14
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -14
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -14
5	Наявність доступу до мережі Інтернет	1 -14
6	Microsoft Windows, WinZip, DjVu Viewer, Total Commander, DevC++, .NET Framework, Visual studio community.	1-14

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Etzion T. Perfect Codes and Related Structures. World Scientific Publishing, 2022. — 436 p.
2. Radhakrishnan Sudhakar, Naduvath Sudev (eds.) Coding Theory. ITexLi, 2022. — 124 p.
3. Calkavur S., Bonnecaze A., Cruz R.D., Sole P. Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory. Springer, 2019. — 274 p.
4. Moon T.K. Error Correcting Codes: Mathematical Methods and Algorithms. 1st edition — Wiley, 2021. — 995p.
5. Spezia Stefano. Mathematical Theory and Applications of Error Correcting Codes. Arcler Press, 2021. — 560 p.
6. Alvim M.S., Chatzikokolakis K., McIver A., Morgan C., Palamidessi C., Smith G.S. The Science Of Quantitative Information Flow. New York: Springer, 2020. — 484 p.
7. Ball S. A Course in Algebraic Error-Correcting Codes. Birkhäuser, 2020. — xiii, 177 p.
8. Gazi O. Forward Error Correction via Channel Coding. Springer, 2020. — 326 p
9. Slinko A. Algebra for Applications: Cryptography, Secret Sharing, Error-Correcting, Fingerprinting, Compression. 2nd Ed. — Springer, 2020. — 376 p.
10. Stratonovich R.L. Theory Of Information And Its Value. Springer, 2020. — 431 p.