

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

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних
інформаційних технологій



Ігор ЯКИМЕНКО
«30» 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи



Віктор ОСТРОВЕРХОВ
«03» 2025 р.

ЗАТВЕРДЖУЮ

Директор Навчально-наукового інституту
новітніх освітніх технологій



Святослав ПИТЕЛЬ
«30» 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни

«СТЕГАНОГРАФІЧНІ МЕТОДИ»

ступінь вищої освіти – магістр

галузь знань – **F Інформаційні технології**

спеціальність – F5 Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семест р	Лекції (год.)	Лабора. заняття (год.)	Інд. роб. (год.)	Тренінг (год.)	Самост. робота (год.)	Разом (год.)	Залік/екзамен. (семестр)
Денна	1	2	32	14	5	6	93	150	Екзамен (2)
Заочна	1	2	8	4	-	-	138	150	Екзамен (2)

Тернопіль - 2025

Робочу програму склали доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК та кандидат технічних наук, доцент, доцент кафедри кібербезпеки Степан ІВАСЬСВ.

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 3 від 25.09.25 р.

Завідувач кафедри кібербезпеки



Василь ЯЦКІВ

Гарант освітньо-професійної
програми



Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Стеганографічні методи”

Дисципліна “Стеганографічні методи”	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	Статус дисципліни вибіркова Мова навчання українська
Кількість залікових модулів – 4	спеціальність – 125 Кібербезпека та захист інформації	Рік підготовки: Денна – 1 Заочна – 1 Семестр: Денна – 2 Заочна – 2
Кількість змістових модулів – 3	ступінь вищої освіти – магістр	Лекції (год): денна – 32; заочна – 8. Лабораторні заняття (год): денна – 14; заочна – 4.
Загальна кількість годин – 150		Самостійна робота (год): денна – 93; заочна – 138. Тренінг (год): денна – 6. Індивідуальна робота (год): денна – 5
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – екзамен.

2. Мета й завдання вивчення дисципліни “Стеганографічні методи”

2.1. Мета завдання дисципліни

Метою вивчення дисципліни є формування комплексу знань щодо отримання здобувачами необхідних базових знань з цифрової стеганографії, яка використовується для приховування факту передавання інформації та створення водяних знаків. Особлива увага в курсі приділяється вивченню проблематики використання цифрової стеганографії у сучасному інформаційному просторі, аналізу атак на стеганограми та оцінки стійкості.

Вивчення курсу “Стеганографічні методи» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Цифрова криміналістика», «Аналіз шкідливого програмного забезпечення», «Моніторинг та управління інформаційною безпекою»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи здобувачів.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є систематизація інформації щодо розроблення, впровадження та експлуатації систем захисту інформації на об'єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- основні положення та терміни стеганографії;
- нормативно-методичну базу в галузі стеганографії;
- етапи організації та застосування стеганографії;
- підходи у визначенні об'єктів захисту;
- типові джерела загроз стеганосистеми;

вміти:

- створювати стеганографічну модель системи захисту;
- складати окремі моделі стеганоконтейнерів.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити здобувачів із головними питаннями курсу «Стеганографічні методи». Завдання проведення лекцій полягає у: викладенні здобувачами у відповідності з програмою та робочим планом основних питань курсу «Стеганографічні методи» та формуванні у студентів цілісної системи теоретичних знань з курсу «Стеганографічні методи».

Завдання проведення лабораторних занять

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

3. Програма навчальної дисципліни “Стеганографічні методи”

Змістовий модуль 1. Вступ до стеганографії.

Тема 1. Основні поняття та положення стеганографії.

Структура та зміст дисципліни, її зв'язок з іншими дисциплінами учбового плану. Цифрова стеганографія. Предмет, термінологія, галузь використання Структура та зміст дисципліни, зв'язок з іншими дисциплінами учбового плану, призначення стеганографічної системи, основна термінологія та визначення, потенціальні області використання стеганографії.

Тема 2. Математична модель стеганосистеми. Практичні аспекти вбудовування даних.

Загальна структурна схема стеганосистеми як системи зв'язку. Математична модель стеганосистеми. Стеганографічні системи з відкритим та закритими ключами. Стеганографічні протоколи. Призначення стеганодетектора. Практичні аспекти вбудовування даних.

Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації.

Класифікація стеганографічних систем та стегоконтейнерів. Основні напрями стегонографії. Вбудовування інформації з метою її прихованої передачі; вбудовування цифрових водяних знаків, вбудовування ідентифікаційних номерів, вбудовування заголовків. Загальна класифікацію контейнерів.

Тема 4. Особливості зорової системи людини.

Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях. Аналіз механізмів зорового сприйняття людини. Низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні. Високорівневі властивості зорової системи людини.

Змістовий модуль 2. Приховування даних в зображеннях та відео

Тема 5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).

Особливості комп'ютерної обробки зображень. Структура форматів BMP, GIF, TIFF, JPEG. Структура файлів растрового зображення. Дескриптор екрану у форматі GIF, термінатор GIF, розширений блок GIF.

Тема 6. Приховування даних у просторовій області зображень та відео.

Метод приховування в найменш значущому біті даних. Приховування даних у просторовій області зображень. Приховування даних у просторовій області відео.

Тема 7. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.

Метод псевдовипадкової перестановки для приховування даних у просторовій області зображень та відео. Приховування даних у просторовій області зображень методом псевдовипадкової перестановки. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.

Тема 8. Приховування даних у просторовій області зображень та відео методом блокового приховування, заміни палітри та квантування зображення.

Метод блокового приховування. Метод заміни палітри. Метод квантування зображення.

Тема 9. Приховування даних у частотній області зображень та відео.

Метод Коха та Жао. Приховування даних у частотній області зображень та відео. Приховування даних у частотній області методом Коха та Жао.

Змістовий модуль 3. Приховування даних в аудіосигналах та текстових файлах. Атаки на стегосистеми та протидія їм

Тема 10. Особливості слухової системи людини (ССЛ).

Основні властивості ССЛ, що використовуються при приховуванні даних в аудіо сигналах. Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis). Особливості комп'ютерної обробки аудіо сигналів. Класи аудіосигналів. Опис форматів WAV, WMA, MP3, AAC, OGG Vorbis.

Тема 11. Приховування даних у просторовій множині аудіосигналу.

Приховування даних у частотній множині аудіо сигналу. Приховування в найменш значущому біті даних та за допомогою ехосигналів. Фазове кодування.

Тема 12. Приховування даних в аудіосигналах за допомогою методів розширення спектра.

Призначення стегакодера й стеганодекодера. Вплив на ЦВДЗ застосування до аудіосигналу ковзного фільтра середніх частот.

Тема 13. Методи текстової стеганографії.

Аналіз реалізації методів. Методи текстової стеганографії. Порівняння методів текстової стеганографії.

Тема 14. Атаки на системи прихованої передачі повідомлень та методи протидії їм.

Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків. Атаки на стеганосистеми цифрових відео знаків. Методи протидії атакам на системи цифрових водяних знаків. Статистичний стегоаналіз та протидії. Методи протидії атакам на системи цифрових водяних знаків.

Тема 15. Практична оцінка стійкості стеганосистем.

Теоретико-складніший підхід до оцінки стійкості стеганосистем. Імітостійкість систем передачі прихованих повідомлень. Класифікація атак зломисника. Досконала стеганосистема.

4. Структура залікового кредиту дисципліни “Стеганографічні методи”

4.1 Структура залікового кредиту дисципліни “Стеганографічні методи” для ДФН

	Кількість годин					
	Лек-ції	Лабора-торні заняття	Самостій-на робота	Індиві-ду альна робота	Тренінг	Контро-ль ні заходи
Змістовий модуль 1. Вступ до стеганографії.						
Тема 1. Основні поняття та положення стеганографії.	2	-	6	1	2	Поточне опитува-ння
Тема 2. Математична модель стеганосистеми. Практичні аспекти вбудування даних.	2	2	6			
Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації.	2	2	6			
Тема 4. Особливості зорової системи людини.	2	-	6			
Змістовий модуль 2. Приховування даних в зображеннях та відео						
Тема 5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).	2	-	6	2	2	Поточне опитува-ння
Тема 6. Приховування даних у просторовій області зображень та відео.	2	2	6			
Тема 7. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки	2	2	6			

Тема 8. Приховування даних у просторовій області зображень та відео методом блокового приховування, заміни палітри та квантування зображення	2	2	6			
Тема 9. Приховування даних у частотній області зображень та відео.	2	2	6			
Змістовий модуль 3. Приховування даних в аудіосигналах та текстових файлах. Атаки на стегосистеми та протидія їм.						
Тема 10. Особливості слухової системи людини (ССЛ).	2	-	6	2	2	Поточне опитування
Тема 11. Приховування даних у просторовій множині аудіосигналу.	2	-	6			
Тема 12. Приховування даних в аудіосигналах за допомогою методів розширення спектра.	3	-	7			
Тема 13. Методи текстової стеганографії.	2	2	6			
Тема 14. Атаки на системи прихованої передачі повідомлень та методи протидії їм.	3	-	7			
Тема 15. Практична оцінка стійкості стеганосистем.	2	-	7			
Разом	32	14	93	5	6	

4.2 Структура залікового кредиту дисципліни “Стеганографічні методи” для ЗФН

	Кількість годин			
	Лекції	Лабораторні заняття	Самостійна робота	Контрольні заходи
Тема 1. Основні поняття та положення стеганографії. Математична модель стеганосистеми. Практичні аспекти вбудування даних. Основні напрямки практичного використання стеганографічних методів захисту інформації. Особливості зорової системи людини.	2	1	34	Поточне опитування
Тема 2. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Приховування даних у просторовій області зображень та відео. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки. Приховування даних у просторовій області зображень та відео методом блокового приховування, заміни палітри та квантування зображення.	2	1	35	
Тема 3. Приховування даних у частотній області зображень та відео. Особливості ССЛ. Приховування даних у просторовій множині аудіосигналу. Приховування даних в аудіосигналах за допомогою методів розширення спектра.	2	1	34	
Тема 4. Методи текстової стеганографії. Атаки на системи прихованої передачі повідомлень та методи протидії їм. Практична оцінка стійкості стеганосистем.	2	1	35	
Разом	8	4	138	

5. Тематика лабораторних робіт.

5.1 Тематика лабораторних робіт для ДФН.

Лабораторна робота №1

Тема: Ознайомлення з методами стеганографічного захисту

Мета роботи: ознайомитися з методами стеганографічного захисту інформації.

Лабораторна робота № 2

Тема: Дослідження стеганографічних методів криптозахисту інформації

Мета роботи: Ознайомитися з принципами роботи стеганографічних методів захисту інформації, навчитися приховувати та витягувати інформацію за допомогою базових стеганографічних алгоритмів, оцінити ефективність та стійкість таких методів до виявлення.

Лабораторна робота №3

Тема: Стеганографічні методи приховування інформації форматуванням тексту

Мета роботи: Ознайомитися з принципами текстової стеганографії, зокрема методами приховування інформації через форматування тексту (невидимі символи, пробіли, табуляції, зміни стилів), а також реалізувати або протестувати такі методи на практиці.

Лабораторна робота №4

Тема: Метод найменшого значущого біта при стеганографічних перетвореннях графічної інформації

Мета роботи: Ознайомитися з принципами стеганографії на основі методу найменшого значущого біта (LSB) для приховування інформації у графічних файлах, реалізувати приховування та витягнення повідомлення, оцінити стійкість методу до змін та атак.

Лабораторна робота №5

Тема: Реалізація у середовищі Mathcad алгоритмів вбудовування даних в просторову область зображень методами блокового приховування

Мета роботи: Ознайомитися з методами стеганографії в просторовій області зображень, вивчити блокові методи вбудовування даних, а також реалізувати основні алгоритми стеганографії у середовищі Mathcad, використовуючи роботу з масивами та матрицями зображення.

Лабораторна робота № 6

Тема: Реалізація у середовищі Mathcad алгоритмів вбудовування даних у частотну область зображень методом Коха–Жао та його модифікацією

Мета роботи: Ознайомитися з принципами стеганографії у частотній області зображень, вивчити алгоритм Коха–Жао (Cox–Zhao), реалізувати його базову та модифіковану версії в середовищі Mathcad, дослідити вплив параметрів алгоритму на стійкість і якість зображення.

Лабораторна робота № 7

Тема: Реалізація аудіостеганографії на базі цифрових методів обробки сигналів дискретними перетвореннями

Мета роботи: Ознайомитися з теоретичними основами аудіостеганографії та цифрової обробки сигналів, дослідити методи вбудовування прихованої інформації в аудіосигнал на основі дискретного косинусного перетворення (DCT) та дискретного перетворення Фур'є (DFT), реалізувати ці методи на практиці у відповідному середовищі програмування або математичного моделювання.

5.2 Тематика лабораторних робіт для ЗФН.

Лабораторна робота №1

Тема: Ознайомлення з методами стеганографічного захисту. Дослідження стеганографічних методів криптозахисту інформації.

Мета роботи: ознайомитися з методами стеганографічного захисту інформації. Ознайомитися з принципами роботи стеганографічних методів захисту інформації, навчитися приховувати та витягувати інформацію за допомогою базових стеганографічних алгоритмів, оцінити ефективність та стійкість таких методів до виявлення.

Лабораторна робота № 2

Тема: Стеганографічні методи приховування інформації форматуванням тексту. Метод найменшого значущого біта при стеганографічних перетвореннях графічної інформації

Мета роботи: Ознайомитися з принципами текстової стеганографії, зокрема методами приховування інформації через форматування тексту (невидимі символи, пробіли, табуляції, зміни стилів), а також реалізувати або протестувати такі методи на практиці. Ознайомитися з принципами стеганографії на основі методу найменшого значущого біта (LSB) для приховування інформації у графічних файлах, реалізувати приховування та витягнення повідомлення, оцінити стійкість методу до змін та атак.

Лабораторна робота № 3

Тема: Реалізація у середовищі Mathcad алгоритмів вбудовування даних в просторову область зображень методами блокового приховування. Реалізація у середовищі Mathcad алгоритмів вбудовування даних у частотну область зображень методом Коха–Жао та його модифікацією.

Мета роботи: Ознайомитися з методами стеганографії в просторовій області зображень, вивчити блокові методи вбудовування даних, а також реалізувати основні алгоритми стеганографії у середовищі Mathcad, використовуючи роботу з масивами та матрицями зображення. Ознайомитися з принципами стеганографії у частотній області зображень, вивчити алгоритм Коха–Жао (Cox–Zhao), реалізувати його базову та модифіковану версії в середовищі Mathcad, дослідити вплив параметрів алгоритму на стійкість і якість зображення.

Лабораторна робота №4

Тема: Реалізація аудіостеганографії на базі цифрових методів обробки сигналів дискретними перетвореннями

Мета роботи: Ознайомитися з теоретичними основами аудіостеганографії та цифрової обробки сигналів, дослідити методи вбудовування прихованої інформації в аудіосигнал на основі дискретного косинусного перетворення (DCT) та дискретного перетворення Фур'є (DFT), реалізувати ці методи на практиці у відповідному середовищі програмування або математичного моделювання.

6. Тематика самостійної роботи студентів

На самостійну роботу кожному студенту пропонується написання і представлення реферату на запропоновану або самостійно вибрану тему. Орієнтовна тематика рефератів:

1. Загальна схема стеганографічної системи, призначеної для передачі даних. Схема стеганографічної системи при наявності пасивного противника.
2. Основні відмінності схем при наявності пасивного і активного противника.
3. Поняття контейнера-носія.
4. Інформаційний підхід до визначення інформації і до оцінки стійкості систем.
5. Поняття ентропії, відносної й умовної ентропії. Теорема Неймана- Пірсона.
6. Правило прийняття рішення як двійкове відображення.
7. Необхідна умова стійкості. Поняття абсолютно стійкої системи.
8. Елементи теорії ігор, що застосовуються в стеганографії.
9. Гра двох учасників з нульовою сумою.
10. Ігри з кінцевою множиною стратегій.
11. Ігри з оптимальними стратегіями.
12. Матричні гри.
13. Поняття функції виграшу і чистої ціни гри.
14. Поняття протоколу, оракула, детермінованого оракула, запит і відповідь оракула.
15. Абстрактна обчислювальна машина з оракулом Алана Тьюринга, її схема.
16. Нескінченно мала функція і конкатенація двох строкових функцій.

17. Поріг приховування і поріг виявлення. Принцип виявлення прихованої інформації.
18. Універсальний стеганоаналітичний алгоритм.
19. Пропускна здатність каналів передачі інформації.
20. Застосування перетворення обертання в стеганосистемах для контролю спотворень.
21. Методи контролю спотворень, що застосовуються в сучасних комп'ютерних системах.
22. Алгоритми вбудовування та вилучення цифрових водяних знаків.
23. Призначення цифрових водяних знаків.
24. Захист за допомогою цифрових водяних знаків авторських прав на електронні твори.
25. Підвищення рівня захищеності за допомогою цифрового підпису.
26. Позитивна судова практика з використанням методів стеганографії.
27. Захист особистої, комерційної та державної інформації методами стеганографії.
28. Стегоалгоритми, які використовують фрактальне перетворення.

7. Організація та проведення тренінгу з дисципліни «Стеганографічні методи»

Тематика тренінгу: застосування і практична реалізація стеганографічних методів для захисту інформаційних потоків.

Цей тренінг охоплює ключові аспекти стеганографічного захисту інформації, поєднуючи теоретичні знання з практичними навичками. Студенти отримають практичні навички роботи з різноманітними програмними середовищами та апаратним забезпеченням.

Мета тренінгу: забезпечити студентів комплексними теоретичними знаннями та практичними навичками в галузі реалізації стеганографічного захисту інформації, підготувавши їх до ефективної фахової діяльності у сучасному цифровому середовищі.

Орієнтовний перелік завдань для тренінгу:

1. Застосування контейнерів «не комп'ютерної» природи в методах стеганографії.
2. Молекула ДНК як стеганографічна модель приховування даних.
3. Алгоритм генерації фрагмента молекули ДНК.
4. Приклади успішного механізму поширення ДНК коду в стеганографії.
5. Метод приховування у вихідних даних зображення.
6. Метод приховування з використанням таблиць квантування.
7. Метод використання неправдивих таблиць квантування.
8. Метод приховування в спектрі зображення після квантування.
9. Дописування даних в кінець JPEG файлу.
10. Метод приховування інформації в графічних зображеннях з палітрою кольорів.
11. Метод приховування з використанням молодших біт даних зображення.
12. Метод приховування, заснований на наявності однакових елементів палітри.
13. Абсолютний поріг чутності.
14. Метод частотного маскування: маскування вперед і маскування назад.
15. Обчислення спектру потужності аудіосигналу.
16. Принцип видалення маскованих компонент.
17. Методи приховування інформації в найменших значущих бітах.
18. Впровадження переданого повідомлення в фазову частину аудіосигналу.
19. Метод формування сегмента з початковою фазою.
20. Метод приховування на основі шумоподібних сигналів.
21. Механізм зворотного перетворення.
22. Застосування методу зворотного перетворення на основі шумоподібних сигналів.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів із запропонованими завданнями тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання одного вибраного завдання тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Стеганографічні методи” використовуються наступні методи оцінювання навчальної роботи студента:

- поточне опитування;
- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;
- підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни “Стеганографічні методи” визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту.

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне з оцінок, отриманих за виконання та захист лабораторних робіт.	Підсумкова письмова робота за темами №1-15.	Оцінка за виконання та представлення одного вибраного завдання тренінгу	Оцінка за виконаний і представлений реферат на вибрану тему.	1. Теоретичні питання: 2 питання по 30 балів - тах 60 балів. 2. Практичне завдання - тах 40 балів

Поточне оцінювання під час заняття:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань. Підсумкова оцінка за поточне опитування кожного модуля визначається як середнє арифметичне оцінок, отриманих під час занять в межах кожного модуля.

Тренінг:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його використовує під час розв’язування задач тренінгу;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при розв’язуванні окремих задач тренінгу не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при розв’язування задач тренінгу, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його використовує, частково розв’язуючи задачі тренінгу, допускаючи при цьому суттєві неточності;

1–59 – не володіє навчальним матеріалом, не розв’язує задачі тренінгу, не бере участі у колективних завданнях під час проведення тренінгу.

Самостійна робота:

90–100 балів – зміст та захист реферату свідчить про високий рівень опанування навчального матеріалу, реферат містить елементи самостійного дослідження, студент на високому рівні виявляє творчий підхід до виконання завдань;

75–89 балів – зміст та захист реферату загалом свідчить про належний рівень опанування навчального матеріалу, можуть бути несуттєві недопрацювання, студент належно виявляє творчий підхід до виконання завдань;

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабо обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань;

1–59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Модульна робота, екзамен – види контролю, при яких засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання. Екзаменаційний білет складається з двох теоретичних питань, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів, та однієї практичної задачі, за яку можна отримати від 0 до 40 балів. За теоретичне питання студент отримує 15–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання, і 1–14 балів – якщо в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання, допускаючи при цьому суттєві неточності, відповіді на запитання нечіткі. За практичну задачу студент отримує 25–40 балів, якщо у повному обсязі володіє навчальним матеріалом, правильно розв’язує практичну задачу і інтерпретує отримані результати, демонструє самостійність виконання; 10–24 балів – у достатньому обсязі володіє навчальним матеріалом, правильно розв’язує практичну задачу, але на додаткові контрольні запитання відсутня повна відповідь, допускає несуттєві неточності та фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання; 1–9 балів – не в повному обсязі володіє матеріалом, фрагментарно розв’язує практичне завдання, допускає суттєві неточності, поверхнево його викладає, недостатньо розкриває зміст поставлених питань.

Шкала оцінювання:

За шкалою ТНЕУ	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)

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

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -15
2	Персональні комп'ютери	1 -15
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -15
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -15
5	Наявність доступу до мережі Інтернет	1 -15
6	Openstego, WavSteg, StegCracker, Scilab.	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Stallings, W., & Brown, L. Computer Security: Principles and Practice (4th ed.). Pearson. 2022. 384 p.
2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
3. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
4. Ya.M.Nykolaychuk, M.M.Kasianchuk, I.Z.Yakymenko. Symmetric Crypt algorithms in the Residue Number System/ // Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
5. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
6. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
10. Ахматєєва Г.В., Кирилюк В.О. Розробка стеганографічного методу вбудови бінарного цифрового водяного знаку в зображення на основі дискретного косинусного

перетворення. Інформатика та математичні методи в моделюванні. 2021. Том 11, № 1-2. С.5-14.

11. Jayashree N., Bhuvaneswaran R.S. A Robust Image Watermarking Scheme Using Z-Transform, Discrete Wavelet Transform and Bidiagonal Singular Value Decomposition. CMC-Tech Science Press. 2019. Volume 58, No. 1. P. 263-285.

12. Priyank Khare, Vinay Kumar Srivastava. A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT. Journal of Intelligent Systems. 2021. Vol. 30, No. 1. P. 297-311.

13. Mahbuba Begum, Mohammad Shorif Uddin. Analysis of Digital Image Watermarking Techniques through Hybrid Methods, Advances in Multimedia. 2020. Volume 2020. P. 1-12.

14. Sunesh R. Rama Kishore. A Novel and Efficient Blind Image Watermarking in Transform Domain. Procedia Computer Science. 2020. No. 167. P. 1505-1514.

15. Rand A. Watheq, Fadi Almasalha, Mahmoud H. Qutqut. A New Steganography Technique using JPEG Images. International Journal of Advanced Computer Science and Applications. 2020. Vol. 9, No. 11. P. 751-760.