ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Стеганографія і стеганоаналіз

Галузь знань – F Інформаційні технології
Спеціальність – F5 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 5 кредитів ЄКТС
Шифр дисципліни – ОФП.07
Мова навчання – Українська
Статус дисципліни – Обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	2	4	5	150	50	16	34	-	-	100	-	-	-	+
Разом ДФН			**5**	**150**	**50**	**16**	**34**	-	-	**100**	-	-	-	**1**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю F5 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доцент Ігор МУЛЯР
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Стеганографія та стеганоаналіз» є однією із дисциплін фахової підготовки здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

Пререквізити: ОФП.02 Математичні основи захисту інформації; ОФП.03 Теорія інформації та кодування.

***Постреквізити*:** ОФП.09 Прикладна криптологія; ОФП.15 Виробнича практика 1.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ЗК01 Здатність застосовувати знання у практичних ситуаціях; ЗК02 Знання та розуміння предметної області і розуміння професійної діяльності; ЗК02 Знання та розуміння предметної області та розуміння професії ЗК03 Здатність спілкуватися іноземною мовою; ФК02 Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

***програмних результатів навчання*:** ПРН04 Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН07 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки; ПРН09 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації;

Мета дисципліни. Формування системи знань та навиків створення та виявлення стеганоканалу передачі інформації в інформаційних та комунікаційних системах при вирішенні задач захисту інформації, розуміння принципів побудови стійких стеганографічних систем і систем протидії приховуванню даних.

Предмет дисципліни. Сучасні методи, теоретичні основи, алгоритми та програмні засоби приховування, виявлення та аналізу прихованих даних у цифрових носіях інформації.

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для засвоєння теоретичних основ стеганографії та стеганоаналізу; ознайомлення з сучасними підходами до приховування даних у цифрових середовищах (зображення, аудіо, відео, мережеві протоколи, потоки IoT); вивчення методів оцінювання непомітності, стійкості та пропускної здатності стеганографічних систем; оволодіння практичними навичками побудови алгоритмів приховування та виявлення даних; формування здатності аналізувати ефективність і безпечність технологій приховування інформації в контексті інформаційної безпеки.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *вміти застосовувати* принципи та властивості основних методів стеганографії та стеганоаналізу на практиці, *спілкуватися* державною мовою усно і письмово, а також використовувати програмні інструменти для реалізації та тестування стеганографічних методів; *обирати* математичні та статистичні методи для оцінки непомітності та стійкості стеганосистем, *адаптуватися* до нових умов, *застосовувати* сучасні технології захисту інформації, критично оцінювати ризики застосування стеганографії у сфері кібербезпеки; інтегрувати стеганографічні методи у системи захисту інформації з урахуванням сучасних викликів.

4. Структура залікових кредитів дисципліни

IV семестр

Назва розділу (теми)	лекції	лабора-торні роботи	СРС
Тема 1. Стеганографічні алгоритми та програмне забезпечення	12	20	76
Тема 2. Основи стеганоаналізу	4	14	24
Разом:	**16**	**34**	**100**

5. Програма навчальної дисципліни

5.1 зміст лекційного курсу

Перелік лекцій (IVсеместр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Стеганографічні алгоритми та програмне забезпечення	**12**
1	**Основи стеганографії, історія, принципи та класифікація методів** Історія стеганографії від давніх часів до сучасності. Визначення стеганографії та її відмінності від криптографії. Базова термінологія та її класифікаційний характер у воєнній стеганографії, зокрема воєнній. Основні принципи приховування інформації, непомітність, ємність, стійкість. Класифікація стеганографічних методів за типом контейнерів: текст, зображення, аудіо, відео, мережеві протоколи. Основні вимоги до стеганографічних систем. Моделі стеганографічних систем, трикутник Сіммонса (задача ув'язнених). Поняття стегоканалу та його характеристики. Застосування стеганографії. IoT та стеганографія, приховування даних у потоках сенсорів. Стеганографія для захисту медичних даних, DICOM зображення, телемедицина. Етичні та правові аспекти використання стеганографії. Літ.: [1] с. 8-20; [2] с. 9-54; [5] с. 43-57; [6] с. 17-42; [11]; [12]; [33-35]	2
2	**Просторові стеганографічні методи у цифрових зображеннях** Основи цифрової обробки зображень: формати, кольорові моделі, представлення пікселів. Метод найменш значущих бітів (LSB) та його принцип роботи, переваги та недоліки. Модифікації LSB методу: випадковий LSB, LSB matching, адаптивний LSB. Методи на основі різниці значень пікселів (PVD). Методи заміщення модулем (Modulus Substitution). Метрики PSNR, SSIM, MSE для оцінки якості стегозображення. Аналіз стійкості до статистичних атак. Практичні реалізації просторових методів стеганографії. Порівняльний аналіз різних просторових методів за критеріями ємності, непомітності та стійкості. Літ.: [2] с. 221-230; [3] с. 1-62; [5] с. 94-131; [6] с. 93-1612; [12]; [31]	2
3	**Приховування даних у частотній множині зображень** Основи частотних перетворень: дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT). Стеганографія у JPEG зображеннях. Структура формату JPEG, вбудовування у коефіцієнти DCT. Методи мінімізації детектування (matrix embedding, syndrome coding). Стеганографія на основі вейвлет-перетворення: вибір коефіцієнтів для вбудовування. Методи адаптивного вбудовування у частотній області. Стійкість частотних методів до стиску та обробки зображень. Стеганографія у форматі JPEG2000. Порівняння просторових та частотних методів. Гібридні підходи, що поєднують просторові та частотні методи. Літ.: [2] с. 23-235; [3] с. 65-143; [5] с. 212-241; [5] с. 163-234; [12]; [31]	2
4	**Аудіо- та відеостеганографія** Особливості аудіостеганографії, властивості людського слухового сприйняття. Методи аудіостеганографії: LSB у аудіофайлах, фазове кодування, spread spectrum. Стеганографія у форматах MP3 та WAV, особливості та обмеження. Психоакустична модель для адаптивного вбудовування. Відеостеганографія. Використання надмірності відеопотоку. Методи вбудовування у відеокадри. Застосування мультимедійної стеганографії у реальному часі. Літ.: [1] с. 27-66; [3] с. 165-187; [5] с. 136-193; [5] с. 257-352; [27]	2
5	**Текстова та лінгвістична стеганографія** Специфіка текстової стеганографії. Обмеженість можливостей модифікації. Методи форматування тексту: пробіли, шрифти, міжрядкові інтервали. Лексична стеганографія. Синтаксична стеганографія. Семантична стеганографія. Генеративна лінгвістична стеганографія на основі мовних моделей. Використання GPT та BERT для генерації стеготекстів. Акровірші та інші літературні методи приховування. Стеганографія у HTML та XML документах. Літ.: [2] с. 114-123; [11] [5] с. 353-370;	2
6	**Практичне застосування та майбутнє стеганографії** Воєнна стеганографія. Система алгоритму пріоритетності. Цифрові водяні знаки, принципи, застосування для захисту авторських прав. Відмінності між стеганографією та цифровими водяними знаками. Квантумна стеганографія.	2

	Використання генетичних алгоритмів. Застосування у цифровій криміналістиці та форензиці Стеганографія та штучний інтелект, генерація синтетичних стегоконтейнерів. Генеративно-змагальні мережі (GAN) для стеганографії, архітектура та принципи навчання. Протидія зловмисному використанню стеганографії. Стандарти та бенчмарки для оцінки стеганографічних систем. Літ.: [1] с. 20-26; [67-104]; [2] с.97-146, 243-265; [3] с. 215-237, 321-344; [4]; [13]; [15]; [19]; [20]	
Тема 2. Основи стеганоаналізу		**4**
7	**Вступ до стеганоаналізу** Визначення стеганоаналізу як науки про виявлення прихованої інформації. Історичний розвиток стеганоаналізу від ручних методів до автоматизованих систем. Завдання стеганоаналізу. Детектування наявності прихованої інформації, визначення алгоритму вбудовування, оцінка обсягу вбудованих даних, вилучення прихованого повідомлення. Модель стеганоаналізу. Класифікація методів стеганоаналізу. Цільовий (Targeted steganalysis) та універсальний (universal steganalysis). Пасивний (passive steganalysis) та активний (active steganalysis) з модифікацією даних. Літ.: [2] с. 221-243; [3] с. 259-294; [5] с. 347-357; [6] с. 43-55; 373-399; [9]; [25]; [37-39]	2
8	**Статистичний та структурний стеганоаналіз** Chi-square (χ^2) атака для детектування LSB стеганографії. Принцип роботи, обчислення статистики, інтерпретація результатів. RS-аналіз (Regular-Singular groups analysis), його теоретичні основи, алгоритм виявлення, оцінка довжини повідомлення. Аналіз кореляцій між пікселями та коефіцієнтами перетворень. Виявлення порушень природних статистичних властивостей зображень. Аналіз блочності у JPEG зображеннях. Метрики оцінки ефективності. True Positive Rate (TPR), False Positive Rate (FPR), точність, повнота, F-міра. Порівняння різних методів стеганоаналізу за ефективністю. Використання ШІ для стегоаналізу. Літ.: [3] с. 295-344; [6] с. 56-61, 400-443; [12]; [16]; [20]; [26]; [36]	2
	Разом за семестр:	**16**

5.2 Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Стеганографічні алгоритми та програмне забезпечення		**12**
1	Приховування інформації у текстові та графічні файли за допомогою стеганографічних програм	4
2	Приховування інформації у аудіо- відеофайли за допомогою стеганографічних програм	4
3	Основи цифрової обробки зображень та просторова стеганографія методом LSB	4
4	Стеганографія у частотній області DCT та DWT методи	4
5	Стеганографія у JPEG зображеннях та її аналіз	4
6	Створення стеганографічного інструменту з GUI та формування конейнеру з використанням ШІ	4
Тема 2. Основи стеганоаналізу		**10**
7	Статистичний стеганоаналіз, Chi-square та RS-аналіз	4
8	Стеганоаналіз на основі machine learning, класифікація cover/stego	4
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до практичних занять, підготовці до тестування. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього, до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

№ тижня	Теми самостійної роботи (IV семестр)	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до лабораторної роботи №1.	6
2	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Виконання лабораторної роботи №1.	6

3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до лабораторної роботи №2.	6
4	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Виконання лабораторної роботи №2.	6
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до лабораторної роботи №3.	6
6	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Виконання лабораторної роботи №3.	6
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Підготовка до лабораторної роботи №4.	6
8	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Виконання лабораторної роботи №4.	6
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до лабораторної роботи №5.	6
10	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Виконання лабораторної роботи №5.	6
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до лабораторної роботи №6.	6
12	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Виконання лабораторної роботи №6.	6
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до лабораторної роботи №7.	6
14	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Виконання лабораторної роботи №7.	6
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до лабораторної роботи №8.	6
16	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Виконання лабораторної роботи №8.	6
17	Підготовка до тестування за пройденим матеріалом.	4
	Разом за семестр:	100

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; практичні заняття – з використанням практичних методів; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування), з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час лабораторних та практичних занять. а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль;
- оцінювання результатів виконання практичних завдань.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо) та практичних занять (вивчення теоретичного матеріалу з теми, активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне або практичне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін,

але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи, практичні завдання, тестування з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання здобувачів освіти

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у IV семестрі

Аудиторна робота	**Контрольні заходи**	**Семестровий контроль**

Лабораторні роботи:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 4-5		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100**
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (дисципліни) кількість балів нижче встановленого мінімуму здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС»**.

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів виконання практичних завдань

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування на знання теоретичного матеріалу з теми; вільне володіння спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні завдань; самостійність та правильність виконання.

Результат виконання кожного лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

Оцінювання результатів тестового контролю

Тест, передбачений робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60	65	70	75	80	85	90	95	100
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання.

Семестровий залік вставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали*** **(середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10

Теоретичне питання № 2	6	8	10
Практичне завдання	12	16	20
Разом:	**24**		**40**

Примітка. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній нижче таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній здобувачем сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="4">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="2">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td><td rowspan="2">Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

10. Питання для самоконтролю результатів навчання

1. Що таке стеганографія і чим вона відрізняється від криптографії?
2. Назвіть три основні вимоги до стеганографічних систем.
3. Що таке стегоканал і які його основні характеристики?
4. Класи систем вбудовування цифрових водяних знаків
5. Поняття і типи контейнера стегосистеми.
6. Типи цифрових водяних знаків.
7. Класифікація систем цифрової стеганографії.
8. Потенційні сфери застосування стеганографії.
9. Трикутник Сіммонса (задача ув'язнених) у контексті стеганографії.
10. Які основні типи контейнерів використовуються у стеганографії?
11. Що таке ємність контейнера і від чого вона залежить?
12. Яка різниця між активною та пасивною атакою на стеганографічну систему?
13. Що означає статистична непомітність стеганографічного вбудовування?
14. Назвіть три основні сфери застосування стеганографії.
15. Що таке payload у контексті стеганографії?
16. Поясніть принцип роботи методу LSB (Least Significant Bit).
17. Чому використовуються саме найменш значущі біти для вбудовування інформації?
18. Як обчислити максимальну ємність зображення для LSB стеганографії?
19. Що таке метрика PSNR і що вона вимірює?
20. Що таке метод PVD (Pixel Value Differencing)?
21. Які переваги має адаптивне вбудовування перед рівномірним?
22. Чому формат BMP краще підходить для LSB методу ніж JPEG?
23. Що таке DCT (Discrete Cosine Transform) і де воно використовується?
24. Чому частотні методи стійкіші до стиснення ніж просторові?
25. Які коефіцієнти DCT найкраще підходять для вбудовування інформації?
26. Що таке DWT (Discrete Wavelet Transform)?
27. Назвіть основні субсмуги вейвлет-розкладання.
28. Яка структура JPEG файлу?
29. Що таке квантування у JPEG стисненні?
30. Поясніть принцип роботи алгоритму JSteg.
31. Що таке стеганоаналіз і які його основні завдання?
32. Яка різниця між targeted та universal стеганоаналізом?
33. Поясніть принцип chi-square (χ^2) атаки.
34. Що таке пари значень (Pairs of Values) у контексті chi-square?
35. Як працює RS-аналіз (Regular-Singular groups)?
36. Що таке дискримінаційна функція у RS-аналізі?
37. Що таке Sample Pairs Analysis (SPA)?
38. Які обмеження має chi-square атака?
39. Чому RS-аналіз може виявити LSB matching?
40. Що таке ROC-крива і для чого вона використовується?
41. Чому JPEG формат популярний для стеганографії?
42. Що таке AC та DC коефіцієнти у DCT?
43. Що таке calibration attack у стеганоаналізі JPEG?
44. Як створити калібрувальне зображення для calibration attack?
45. Які аномалії виникають у гістограмі DCT при JSteg вбудовуванні?
46. Що таке кореляція між пікселями і як вона використовується у стеганоаналізі?
47. Які типи кореляцій аналізуються у зображеннях?
48. Що таке GLCM (Gray Level Co-occurrence Matrix)?
49. Поясніть принцип neighborhood prediction методів.
50. Що таке prediction errors у контексті стеганоаналізу?
51. Що таке Local Binary Patterns (LBP)?
52. Як обчислюється локальна складність зображення?
53. Що таке адаптивна стеганографія і чому вона ефективніша?
54. Що таке distortion function у адаптивних методах?
55. Що таке Syndrome-Trellis Codes (STC)?
56. Як оцінити складність текстури для адаптивного вбудовування?
57. Чому у складних областях можна вбудовувати більше інформації?
58. Які метрики використовуються для порівняння адаптивних методів?
59. Що таке embedding efficiency у стеганографії?
60. Яка різниця між security та capacity у стеганографічних системах?

61. Принцип вбудовування повідомлень в незначущі елементи контейнера-зображення.
62. Способи впровадження в контейнер бітів цифрових водяних знаків.
63. Класифікація методів стеганографічного захисту.
64. Методи текстової стеганографії.
65. Приховування даних у частотній області зображень.
66. Блокове приховування.
67. Метод Коха-Жао та його модифікації.
68. Приховування даних у нерухомих зображеннях за допомогою методів розширення спектра.
69. Властивості людського зору потрібно враховувати при побудові стегоалгоритмів.
70. Узагальнена схему впровадження даних в зображення.
71. Високорівневі властивості людського зору.
72. Принципи стиснення і відновлення зображень.
73. Принципи приховування даних в просторовій області зображень.
74. Алгоритм стегокодера із застосуванням широкосмугових сигналів.
75. Принцип вбудовування інформації модифікацією фази аудіосигналу.
76. Приховування даних у просторій множині аудіосигналу
77. Приховування даних у частотній множині аудіосигналу (фазове кодування).
78. Приховування даних в аудіосигналах за допомогою методів розширення спектра**.**
79. Класифікація атак на стеганосистеми.
80. Практична оцінка стійкості стеганосистем.

11. Методичне забезпечення

Освітній процес з дисципліни «Стеганографія та стеганоаналіз» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Стеганографія та стеганоаналіз»: https://msn.khmnu.edu.ua/course/view.php?id=6789.

12. Матеріально-технічне та програмне забезпечення

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення:, OS MS Windows 10 або вище, MS Visual Studio 22 або вище, Python, OpenStego S-Tools, StegHide, Aletheia, StegExpose тощо.

13. Рекомендована література

Основна

1. Лісовська Ю. П., Лісовський П. М. Воєнна стеганографія: квантова симуляція та космічна гіперспектроскопія : навчальний посібник. Дніпро : Ліра-К, 2024. 134 с.
2. Digital Watermarking and Steganography: Fundamentals and Techniques / Edited by Frank Y. Shih. – CRC Press, 2020. – 270 p
3. Huang F., Shi Y. Q., Cox I. J. Digital media steganography: theory and practice. Singapore : Springer, 2020. 351 p.
4. Євсеєв С. П., Шматко О. В., Король О. Г. Кібербезпека: криптографія з Python : навчальний посібник. Харків : Новий Світ – 2000, 2021. 120 с.
5. Соколов А. В. Методологія розробки ефективної криптостеганографічної системи : дис. ... д-ра техн. наук : 05.13.21 / Нац. ун-т «Одеська політехніка» ; Нац. ун-т «Львівська політехніка». Львів, 2023. 377 с.

Додаткова

6. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. – 558 с
7. Методичні вказівки до виконання лабораторних робіт при вивченні дисципліни «Стеганографія» / укладач В.В. Лукічов, А.В. Остапенко-Боженова. – Вінниця: ВНТУ, 2019. – 78с.
8. Steganography Techniques for Digital Images / Edited by Abid Yahya. – Springer International Publishing AG, 2019. – 131 p
9. Apau R., Asante M., Twum F., Hayfron-Acquah J. B., Peasah K. O. Image steganography techniques for resisting statistical steganalysis attacks: a systematic literature review. PLoS ONE. 2024. Vol. 19, No. 9.
10. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; 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.
11. Noor Azam M. H., Ridzuan F., Mohd Sayuti M. N. S., Azni A. H., Zakaria N. H., Potdar V. A systematic review on cover selection methods for steganography: trend analysis, novel classification and analysis of the elements. Computer Science Review. 2025. Vol. 56. Article 100726. DOI: 10.1016/j.cosrev.2025.100726
12. Бараннік Д. В. Метод структурного стеганографічного перетворення для підвищення пропускної здатності прихованого каналу передачі даних : дис. ... д-ра філософії : 172 / Харків. нац. ун-т радіоелектроніки. Харків, 2024. 206 с.
13. Muliar I., Anikin V., Yatskiv V., Kulyna S., Humennyy P., Kulyna H. Construction of nonlinear cryptographic protocol based on multiple linear cryptosystems. 2024 14th International Conference on Advanced Computer Information Technologies (ACIT). Serik, September 26–28, 2024. Piscataway : IEEE, 2024. P. 500–504. DOI: 10.1109/acit62333.2024.10712536
14. Haverkamp I., Sarmah D. K. Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. International Journal of Information Security. 2024. Vol. 23, No. 4. P. 2607–2635. DOI: 10.1007/s10207-024-00853-9
15. Anikin V., Lienkov S., Muliar I., Dzhulii V., Sieliukov O., Yaroslav M. The concept of nonlinear cryptographic primitives, their steganographic applications, and related areas of use. EUREKA: Physics and Engineering. 2025. No. 5. P. 190–204. DOI: 10.21303/2461-4262.2025.003945
16. Dalal M., Juneja M. Steganography and steganalysis (in digital forensics): a cybersecurity guide. Multimedia Tools and Applications. 2021. Vol. 80, No. 4. P. 5723–5771. DOI: 10.1007/s11042-020-09929-9
17. Kumar S., Soundrapandiyan R. Digital video steganography: an overview. Computational Methods and Data Engineering / eds. V. K. Asari, V. Singh, R. Rajasekaran, R. B. Patel. Singapore : Springer, 2023. P. 557–566. (Lecture Notes on Data Engineering and Communications Technologies ; vol. 139). DOI: 10.1007/978-981-19-3015-7_42
18. Wendzel S. et al. Combining different existing methods for describing steganography hiding methods. Availability, Reliability and Security / eds. B. Coppens, B. Volckaert, V. Naessens, B. De Sutter. Cham : Springer, 2025. P. 238–253. (Lecture Notes in Computer Science ; vol. 15996). DOI: 10.1007/978-3-032-00635-6_16
19. Li Z., Zhang M., Liu J. Robust image steganography framework based on generative adversarial network. Journal of Electronic Imaging. 2021. Vol. 30, No. 2. Article 023006. DOI: 10.1117/1.JEI.30.2.023006

20. Guan Z., Jing J., Deng X., Xu M., Jiang L., Zhang Z., Li Y. DeepMIH: Deep invertible network for multiple image hiding. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. Vol. 45, No. 1. P. 372–390. DOI: 10.1109/TPAMI.2022.3141725

21. Bui T., Agarwal S., Yu N., Collomosse J. RoSteALS: Robust steganography using autoencoder latent space. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Vancouver, June 17–24, 2023. Piscataway : IEEE, 2023. P. 933–942.

22. Kobozeva A. A., Sokolov A. V. The sufficient condition for ensuring the reliability of perception of the steganographic message in the Walsh-Hadamard transform domain. Problemele Energeticii Regionale. 2022. Vol. 54, No. 2. P. 84–100.

23. Kobozeva A. A., Sokolov A. V. Robust steganographic method with code-controlled information embedding. Problemele Energeticii Regionale. 2021. No. 4 (52). P. 115–130.

24. M. Dalal, M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimed Tools Appl 80 (2021) 5723–5771. doi:10.1007/s11042-020-09929-9

25. Джулій В. М., Кльоц Ю. П., Муляр І. В., Чешун В. М. Ітераційно-геометричний метод для стійкого перцептуального хешування зображення. Вісник Хмельницького національного університету. Серія: Технічні науки. 2020. № 1. С. 76–79.

26. Кошкіна Н. В. Стеганоаналіз J-UNIWARD. Кібернетика та системний аналіз. 2021. Т. 57, № 3. С. 184–192.

27. Трифонова К. О., Трифонова Е. А., Сокальський С. М., Сокальский С. Н. Стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення. Інформатика та математичні методи в моделюванні. 2022. Т. 12, № 1-2. С. 104–113.

28. Яворський О. О., Соколов А. В. Підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації при роботі з цифровим відео. Інформатика та математичні методи в моделюванні. 2023. Т. 13, № 1-2. С. 173–179.

29. Кобозєва А. А., Соколов А. В. Стеганографічний метод з кодовим управлінням вбудовуванням інформації на основі багаторівневих кодових слів. Вісті вищих учбових закладів. Радіоелектроніка. 2024. Т. 67, № 4. С. 209–221. DOI: 10.20535/S0021347023040052

30. Бобок І. І., Кобозєва А. А. Локалізація області збурень формальних параметрів стеганографічного контейнера для забезпечення стійкості стеганосистеми. Вісті вищих учбових закладів. Радіоелектроніка. 2024. Т. 67, № 8. С. 452–467. DOI: 10.20535/S0021347024090024

31. Dalal M., Juneja M. Steganography and steganalysis (in digital forensics): a cybersecurity guide. Multimedia Tools and Applications. 2021. Vol. 80, No. 4. P. 5723–5771. DOI: 10.1007/s11042-020-09929-9

32. Kobozeva A. A., Bobok I. I., Kushnirenko N. I. Method for distinguishing the digital images in different formats. Problemele Energeticii Regionale. 2022. Vol. 1, No. 53. P. 109–124.

33. Eid W. M., Alotaibi S. S., Alqahtani H. M., Saleh S. Q. Digital image steganalysis: current methodologies and future challenges. IEEE Access. 2022. Vol. 10. P. 92321–92336. DOI: 10.1109/ACCESS.2022.3202905

34. Bouzegza M., Belatreche A., Bouridane A., Tounsi M. A comprehensive review of video steganalysis. IET Image Processing. 2022. Vol. 16, No. 13. P. 3407–3425. DOI: 10.1049/ipr2.12573

35. PYTHON. URL: https://www.python.org/ (дата звернення: 25.08.2025).

36. OpenStego. Відкрите програмне забезпечення для стеганографії та цифрових водяних знаків URL: https://www.openstego.com (дата звернення: 24.08.2025)

37. StegHide. Інструмент для приховування даних у зображеннях та аудіофайлах URL: http://steghide.sourceforge.net (дата звернення: 24.08.2025)

38. DeepSteg. Ралізація стеганографії на основі глибокого навчання URL: https://github.com/alexandremuzio/deepsteg (дата звернення: 24.08.2025)

39. Aletheia. Інструмент для стеганоаналізу зображень URL: https://github.com/daniellerch/aletheia (дата звернення: 24.08.2025)

40. StegExpose. Детектор стеганографії у зображеннях URL: https://github.com/b3dk7/StegExpose (дата звернення: 27.08.2025)

41. ALASKA Dataset. Набір для досліджень стеганографії та стеганоаналізу URL: https://www.kaggle.com/datasets (дата звернення: 27.08.2025)

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6789
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

СТЕГАНОГРАФІЯ ТА СТЕГАНОАНАЛІЗ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Четвертий
Кількість встановлених кредитів ЄКТС	5
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *вміти застосовувати* принципи та властивості основних методів стеганографії та стеганоаналізу на практиці, *спілкуватися* державною мовою усно і письмово, а також використовувати програмні інструменти для реалізації та тестування стеганографічних методів; *обирати* математичні та статистичні методи для оцінки непомітності та стійкості стеганосистем, *адаптуватися* до нових умов, *застосовувати* сучасні технології захисту інформації, критично оцінювати ризики застосування стеганографії у сфері кібербезпеки; інтегрувати стеганографічні методи у системи захисту інформації з урахуванням сучасних викликів.

Зміст навчальної дисципліни. Основи стеганографії, історія, принципи та класифікація методів. Просторові та частотні стеганографічні методи у цифрових зображеннях. Гібридні підходи, що поєднують просторові та частотні методи. Аудіо- та відеостеганографія. Текстова та лінгвістична стеганографія. Текстова та лінгвістична стеганографія. Порівняльний аналіз різних методів за критеріями ємності, непомітності та стійкості. Практичне застосування та майбутнє стеганографії. Воєна стеганографія. Застосування у цифровій криміналістиці та форензиці Стеганографія та штучний інтелект. Вступ до стеганоаналізу. Модель стеганоаналізу. Класифікація методів стеганоаналізу. Порівняння різних методів стеганоаналізу за ефективністю.

Пререквізити: ОФП.02 Математичні основи захисту інформації; ОФП.03 Теорія інформації та кодування.

Постреквізити: ОФП.09 Прикладна криптологія; ОФП.15 Виробнича практика 1.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для першого (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); практичні заняття (з використанням практичних методів); лабораторні роботи (з використанням практичних, частково-пошукових та ігрових методів); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання на практичних заняттях; оцінювання результатів захисту лабораторних робіт; тестовий контроль; оцінювання результатів підсумкового семестрового контролю (іспит).

Вид семестрового контролю: залік**,** іспит.

Навчальні ресурси:

1. Лісовська Ю. П., Лісовський П. М. Воєнна стеганографія: квантова симуляція та космічна гіперспектроскопія : навчальний посібник. Дніпро : Ліра-К, 2024. 134 с.
2. Digital Watermarking and Steganography: Fundamentals and Techniques / Edited by Frank Y. Shih. – CRC Press, 2020. – 270 p
3. Huang F., Shi Y. Q., Cox I. J. Digital media steganography: theory and practice. Singapore : Springer, 2020. 351 p.
4. Євсеєв С. П., Шматко О. В., Король О. Г. Кібербезпека: криптографія з Python : навчальний посібник. Харків : Новий Світ – 2000, 2021. 120 с.
5. Соколов А. В. Методологія розробки ефективної криптостеганографічної системи : дис. ... д-ра техн. наук : 05.13.21 / Нац. ун-т «Одеська політехніка» ; Нац. ун-т «Львівська політехніка». Львів, 2023. 377 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6789
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: канд. техн. наук, доцент Ігор МУЛЯР.