

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ



ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

Тетяна ГОВОРУЩЕНКО
Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Стеганографія і комп'ютерна графіка

Призначення робочої програми – Для освітніх програм різних спеціальностей

Рівень вищої освіти – Перший (бакалаврський)

Обсяг дисципліни – 8 кредитів ЄКТС

Мова навчання – Українська

Статус дисципліни – Вибіркова

Факультет – Інформаційних технологій

Кафедра – Кібербезпеки

Форма здобуття освіти	Загальний обсяг		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота, у т.ч. ІРС	Залік
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		
Д	8	240	82	32	32	18	-	158	+
Разом ДФН	8	240	82	32	32	18	-	158	1

Примітка: *Вибіркову навчальну дисципліну, яку кафедра рекомендує для певного рівня вищої освіти / спеціальності, мають право вибирати здобувачі інших рівнів та спеціальностей університету

Робоча програма складена

Підпис

канд. техн. наук, доцент
Науковий ступінь, учене звання

Ігор МУЛЯР
Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри

Кібербезпеки

Протокол від 29.08.2025 № 1.

Зав. кафедри

Юрій КЛЬОЦ

3. Пояснювальна записка

Дисципліна «Стеганографія і комп'ютерна графіка» відноситься до циклу вибіркових дисциплін, що охоплює сучасні підходи в галузі обробки зображень двовимірних та тривимірних об'єктів за допомогою комп'ютера, та надає необхідні знання та навички створення та виявлення прихованого каналу передачі інформації в інформаційних та комунікаційних системах при вирішенні задач захисту інформації.

Мета дисципліни: Формування системи знань та розуміння сучасних комп'ютерних графічних технологій, їх можливостей по створенню, обробці і публікації різних видів зображень; отримання студентами необхідних знань та навиків створення та виявлення стеганоканалу передачі інформації в інформаційних та комунікаційних системах при вирішенні задач захисту інформації.

Предмет дисципліни. Сучасні методи обробки зображень, як засобами відповідних графічних редакторів, так і засобами візуальних мов програмування; створення та виявлення стеганоканалів передачі 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 пропускну 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; *вміти* створювати нові зображення і редагувати наявні, перетворювати формати комп'ютерних зображень та їхні колірні моделі, імпортувати належним чином підготовлені графічні зображення в офісні документи, у вебсторінки, у електронні та поліграфічні видання; *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

Назва розділу (теми)	Кількість годин, відведених на:			
	лекції	лабораторні	практичні	СРС
Тема 1. Комп'ютерна графіка	16	16	8	58
Тема 2. Стеганографічні алгоритми та програмне забезпечення	12	12	4	50
Тема 3. Основи стеганоаналізу	4	4	4	50
Разом за семестр:	32	32	18	158

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Комп'ютерна графіка	16
1	Основні поняття комп'ютерної графіки. Основні поняття комп'ютерної графіки (колір, роздільна здатність,). Області застосування. Растрова графіка (Растрова графіка, загальні відомості. Растрові представлення зображень. Види растрів. Фактори, що впливають на кількість пам'яті, займаної растровим зображенням. Переваги і недоліки растрової графіки. Геометричні характеристики растра (роздільна здатність, розмір растра, форма пікселів). Кількість кольорів растрового зображення.) Векторна графіка (загальні відомості, спосіб збереження зображення, елементи (об'єкти) векторної графіки, об'єкти і їхні атрибути). Фрактальна графіка. Найвідоміші графічні редактори. Мови програмування графіки. Літ.: [4] с.3-17, с.33-39, с.57-61; [22] с.29-70.	2
2	Колір та моделі кольору. Формати збереження графічних зображень. Основи теорії кольору. Характеристики кольору: колірний тон, яскравість, насиченість. Закони змішування кольорів. Колірне охоплення та колірні моделі: RGB, CMY та CMYC, HSB та HLS, Lab. Кодування кольору. Палітра, Типи растрових зображень. Графічні файли. Класифікація форматів. Растрові формати BMP, TIFF, PCX, GIF, JPRG, PNG, JBIG2, JPEG 2000, LWF. Приклади запису растрового зображення в різних форматах. Розвиток растрових форматів. Формати DXF, MIF-MID. Мета файли: CGM, EPS, PICT, WMF/EMF, CDR, FH7, FH5, PostScript. Призначення. Переваги та недоліки. Літ.: [6] с.26-50; [9] с.17-27.	2
3	Формат Jpeg. Структура формат Jpeg. Службові маркери. Просторова область зображення. Стиснення Jpeg. Дискретно-косинусне перетворення. Вейвлеті. Літ.: [9] с.50-56.	2
4	Математичні засоби комп'ютерної графіки. Перетворення на площині. Афінні перетворення на площині. Перехід від однієї координатної системи на площині до іншої. Поворот R (rotation). Розтягування (стискування) D (dilatation). Відображення відносно осі абсцис M (reflection). Перенос T (translation). Причини використання афінних перетворень. Матричний запис афінних перетворень. Од-норідні координати точки. Матриці перетворень. Технологія застосування мат-риць перетворень для реалізації графічних перетворень на площині. Літ.: [4] с.79-93; [10] с.83-164; [22] с.204-212.	2
5	Перетворення в просторі. Проеціювання. Афінні перетворення в просторі. Однорідні координати точки в просторі. Матриці перетворень в просторі. Поворот R (rotation) – навколо осей абсцис, ординат і аплікату. Розтягування (стискування) D (dilatation) – вздовж осей абсцис, ординат і аплікату. Відображення відносно осі абсцис M (reflection) – відносно площин ху, уз, хz. Перенос T (translation) – на вектор (х,у,з). . Технологія застосування матриць перетворень для реалізації графічних перетворень в просторі. Літ.: [9] с.49-63; [10] с. 95-140;	2

6	Класифікація алгоритмів комп'ютерної графіки Основні категорії алгоритмів комп'ютерної графіки за типом представлення даних та розмірністю простору. Класифікація алгоритмів растеризації примітивів, зокрема для побудови відрізків, кіл, еліпсів та заповнення областей. Алгоритми для відсікання та обрізання графічних об'єктів у двовимірному просторі. Літ.: [[10] с.83-124; [22] с.213-257.	2
7	Тривимірна графіка. Основні поняття. Моделювання і_рендеринг. Моделі опису поверхонь. Шейдери. Рендеринг. Матричні обчислення в тривимірній графіці. Програмне забезпечення. Фізичне представлення трьохвимірних об'єктів. Літ.: [7] с.91-118; [10] с.184-197	2
8	Проблема візуалізації тривимірних об'єктів. Основні підходи до моделювання освітлення та тонування поверхонь, включаючи локальні та глобальні моделі. Класифікація алгоритмів за обчислювальною складністю та компромісом між швидкістю виконання і якістю результату. Сучасні тренди, що визначають розвиток алгоритмів комп'ютерної графіки, зокрема GPU-обчислення, рендеринг реального часу та застосування машинного навчання. Літ.: [4] с.69-83; [10] с.113-154;	
	Тема 2. Стеганографічні алгоритми та програмне забезпечення	12
9	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 військовій стеганографії, зокрема військовій. 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 стегаканалу 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
10	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
11	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
12	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.	2

	Літ.: [1] с. 27-66; [3] с. 165-187; [5] с. 136-193; [5] с. 257-352; [27]	
13	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. Акрівірші та інші літературні методи приховування. Стеганографія у HTML та XML документах. Літ.: [2] с. 114-123; [11] [5] с. 353-370;	2
14	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. 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]	2
	Тема 3. 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:	32

5.2 Зміст практичних занять

№ з/п	Тема практичного заняття	Кількість годин
1	Використання генеративного ШІ для створення растрових зображень Літ.: [4] с. 31-147, с.257-323	2
2	Використання ШІ для редагування існуючих растрових зображень Літ.: [4] с. 349-403; [6] с. 97 – 193	2
3	Використання генеративного ШІ для створення векторних зображень Літ.: [4] с. 141-169	2
4	Використання генеративного ШІ для створення аудіо та відео контенту Літ.: [4] с. 375-429; [6] с. 193 – 280	2
5	Застосування технології OSINT для пошуку за зображенням Літ.: [4] с. 429-453; [6] с. 97 – 280	2
6	Створення стеганографічного інструменту з GUI та формування контейнеру з використанням ШІ Літ.: [1] с.140-156; [2] с.117-130	2
7	Статистичний стеганоаналіз, Chi-square та RS-аналіз Літ.: [1] с.170-186; [2] с.131-1145	2
8	Стеганоаналіз на основі machine learning, класифікація cover/stego Літ.: [1] с.190-198; [2] с.146-1180	2
9	Підсумкове заняття	2
Разом:		18

5.3 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кількість годин
1	Знайомство з інтерфейсом і інструментами Photoshop, створення простих зображень в графічному редакторі Adobe Photoshop Літ.: [7] с.43-57;	4
2	Складання колажу у програмі Adobe Photoshop. Літ.: [7] с.80-97;	4
3	Робота з графічним редактором Corel Draw – основні прийоми і правила Літ.: [7] с.97-108;	4
4	Виконання креслеників в Corel Draw. Літ.: Літ.: [7] с.106-119;	4
5	Приховування інформації у текстові та графічні файли за допомогою стеганографічних програм Літ.: [1] с.140-156; [2] с.117-130	4
6	Приховування інформації у аудіо- відеофайли за допомогою стеганографічних програм Літ.: [1] с.157-172; [2] с.117-130	4
7	Основи цифрової обробки зображень та просторова стеганографія методом LSB Літ.: [4] с.140-156;	4
8	Дослідження ефективності стегаоконтейнера, стеганоаналіз. Літ.: [3] с.10-56; [2] с.131-147	4
Разом:		32

5.4 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до практичних занять, тестування тощо. 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.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу. Підготовка до ЛР1 та ПЗ1. Підготовка до захисту ЛР1.	4
2	Опрацювання лекційного матеріалу.. Підготовка до захисту ЛР1.	6
3	Опрацювання лекційного матеріалу. Підготовка до ЛР2 та ПЗ2.	6
4	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР2.	10
5	Опрацювання лекційного матеріалу. Підготовка до ЛР3 та ПЗ3.	10
6	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР3.	12
7	Опрацювання лекційного матеріалу. Підготовка до ЛР4 та ПЗ4.	12
8	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР4	10
9	Опрацювання лекційного матеріалу. Підготовка до ЛР5 та ПЗ5.	10
10	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР5.	10
11	Опрацювання лекційного матеріалу. Підготовка до ЛР6 та ПЗ6.	10
12	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР6	10
13	Опрацювання лекційного матеріалу. Підготовка до ЛР7 та ПЗ7.	10
14	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР7.	10
15	Опрацювання лекційного матеріалу. Підготовка до ЛР8 та ПЗ8.	10
16	Опрацювання лекційного матеріалу. Підготовка до захисту ЛР8.	10
17	Опрацювання лекційного матеріалу. Підготовка до ПЗ9 та тестування.	10
	Разом:	160

Примітки: ЛР – лабораторна робота, ПЗ– практичне заняття.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів. Зокрема, лекції проводяться з використанням словесних, наочних, інтерактивних та проблемних методів з супроводом мультимедійних технологій та презентаційних матеріалів; практичні заняття – з використанням практичних методів; лабораторні роботи – з використанням практичних та частково-пошукових методів, методів проектної діяльності із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота – з використанням пояснювально-ілюстративних та частково-пошукових методів.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних та лабораторних 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 роботи на практичних заняттях (опитування теоретичного матеріалу, вирішення завдань, участь у обговоренні ситуацій);
- тестовий контроль засвоєння теоретичного та практичного матеріалу;
- оцінювання результатів захисту лабораторних робіт;

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, 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 практичних та лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами лабораторних робіт.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене лабораторне / практичне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять, захисту лабораторних робіт, тестування.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності 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, які сприяють формуванню 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 студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». 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.

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 навичками роботи з алгоритмами та структурами даних. 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, перекидає 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 студентів

Аудиторна робота								Контрольні заходи	Семестровий контроль
Лабораторні заняття №:								Тестовий контроль	Залік
1*	2	3	4	5	6	7	8	1-8	
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)									
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20
24-40								24-40	12-20
									За рейтингом
									60-100**

Примітки: *За набрану з будь-якого виду навчальної роботи з 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 на практичних заняттях. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; умінь професійно обґрунтовувати прийняті рішення при вирішенні завдань.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «Критерії оцінювання навчальних досягнень здобувача вищої освіти» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

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; повнота відповіді та знання.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

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 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.

У разі, якщо здобувач вищої освіти виявив рівень знань, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий залік виставляється 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.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	Іспит/диференційований залік
A	90-100	Зараховано	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
B	83-89		Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
D	66-72		
E	60-65		
FX	40-59	Незараховано	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
F	0-39		Незадовільно/Fail – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

- Напрямки криптографії та стеганографії.
- Структурна схема типової стеганосистеми цифрових водяних знаків.
- Класи систем вбудовування цифрових водяних знаків
- Поняття і типи контейнера стеганосистеми.
- Типи цифрових водяних знаків.
- Класифікація систем цифрової стеганографії.
- Потенційні сфери застосування стеганографії.
- Принцип вбудовування повідомлень в незначущі елементи контейнера-зображення.
- Протоколи стеганографії з відкритим ключем.
- Протоколи стеганографії виявлення цифрових водяних знаків з нульовим знанням.
- Способи впровадження в контейнер бітів цифрових водяних знаків.
- Переваги та недоліки мають стегоконтейнери зображень.
- Класифікація методів стеганографічного захисту.
- Методи текстової стеганографії.
- Приховування даних у частотній області зображень.
- Блокове приховування.
- Метод Коха-Жао та його модифікації.
- Метод Хсу – Ву. Метод Фрідріха.
- Приховування даних у нерухомих зображеннях за допомогою методів розширення спектра.
- Властивості людського зору потрібно враховувати при побудові стегоалгоритмів.
- Узагальнена схема впровадження даних в зображення..
- Високорівневі властивості людського зору.
- Принципи стиснення і відновлення зображень.
- Принципи приховування даних в просторовій області зображень.
- Алгоритм стегокодера із застосуванням ширококутних сигналів.
- Стегоалгоритми на основі лінійного вбудовування даних в зображення.
- Модель «сліпої» стеганосистеми.
- Принцип вбудовування інформації із застосуванням модуляції індексу квантування.
- Принцип застосування в схемі модуляції індексу квантування дізерізованого квантувача.
- Алгоритми вбудовування ЦВЗ з використанням скалярного квантування.
- Алгоритми вбудовування ЦВЗ з використанням векторного квантування.
- Вимоги до стегосистем вбудовування інформації в аудіосигнали.
- Блок-схема стегокодера і стегодекодера вбудовування інформації в аудіосигнал методом кодування з розширенням спектру.
- Принцип вбудовування інформації модифікацією фази аудіосигналу.
- Приховування даних у просторій множині аудіосигналу
- Приховування даних у частотній множині аудіосигналу (фазове кодування).
- Приховування даних в аудіосигналах за допомогою методів розширення спектра.
- Класифікація атак на стеганосистеми.

39. Практична оцінка стійкості стеганосистем.
40. Принцип вбудовування інформації за рахунок зміни часу затримки луна-сигналу.
41. Методи маскування ЦВЗ.
42. Малювання геометричних об'єктів.
43. Модельно-видові перетворення.
44. Матеріали і висвітлення.
45. Текстурування та робота з пікселями.
46. Шейдери та робота з ними.
47. Принципи стиснення і відновлення зображень.
48. Принципи приховування даних в просторовій області зображень.
49. Алгоритм стегокодера із застосуванням широкосмугових сигналів.
50. Принцип вбудовування інформації модифікацією фази аудіосигналу.
51. Приховування даних у просторій множині аудіосигналу
52. Приховування даних у частотній множині аудіосигналу (фазове кодування).
53. Приховування даних в аудіосигналах за допомогою методів розширення спектра.
54. Класифікація атак на стеганосистеми.
55. Практична оцінка стійкості стеганосистем.

11. Навчально-методичне забезпечення

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

1. Курс «Стеганографія та комп'ютерна графіка» <https://msn.khmn.edu.ua/course/view.php?id=6189>.

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК. Програмне забезпечення: програми Corel Draw, Photoshop, Python, OpenStego S-Tools, StegHide, Aletheia, StegExpose тощо. доступ до мережі Інтернет, робота з презентаціями.

13. Рекомендована література

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. Комп'ютерна графіка [Електронний ресурс] : конспект лекцій : навч. посіб. для здобувачів ступеня бакалавра за спец. 123 Комп'ютерна інженерія / Я. М. Клятченко, О. В.Тарасенко-Клятченко ; КНУ ім. Ігоря Сікорського. – Електрон. текст. дані (1 файл). – Київ : КНУ ім. Ігоря Сікорського, 2024. – 128 с.
5. Соколов А. В. Методологія розробки ефективної криптистеганографічної 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. Комп'ютерна графіка : конспект лекцій з курсу «Комп'ютерна графіка» / Укладач: Скиба О.П. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2019. – 88 с.
10. Євсєєв С. П., Шматко О. В., Король О. Г. Кібербезпека: криптографія з Python : навчальний посібник. Харків : Новий Світ – 2000, 2021. 120 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., Humenny 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., Soundrapandian 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., Сокальський 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 навчальних 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 навчальних 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.khnu.km.ua/course/view.php?id=6189>
2. Електронна бібліотека ХНУ. URL: <http://library.khmnu.edu.ua/>
3. Інституційний репозитарій ХНУ. URL : <https://elar.khmnu.edu.ua/home>

Стеганографія та комп'ютерна графіка

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Кількість встановлених кредитів ЄКТС	8
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. Особливості та відмінності растрової, векторної і фрактальної графіки; кольорні моделі, що використовуються в комп'ютерній графіці; види графічних файлів; математичні та алгоритмічні основи комп'ютерної графіки. 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.

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); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль.

Вид семестрового контролю: залік.

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 Комп'ютерна графіка [Електронний ресурс] : конспект лекцій : навч. посіб. для здобувачів ступеня бакалавра за спец. 123 Комп'ютерна інженерія / Я. М. Клятченко, О. В.Тарасенко-Клятченко ; КПІ ім. Ігоря Сікорського. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2024. – 128 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.khmnua.edu.ua/course/view.php?id=6189>

7 Електронна бібліотека ХНУ. Доступ до ресурсу: <http://lib.khmnua.edu.ua>

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