Силабус курсу
Стеганографічні методи

Ступінь вищої освіти – магістр
Освітня програма «Кібербезпека»

Дні занять: _____, _____, ауд. ____; _____, _____, ауд. ____
Консультації: _____ _____, ауд. ____

Рік навчання: Семестр: II

Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП д.т.н., професор, професор кафедри кібербезпеки **Михайло КАСЯНЧУК**

Контактна інформація kmm@wunu.edu.ua, +38 (0352) 47 50 50 *6501

Опис дисципліни

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

Структура курсу

Години (лек. / сем.)	Тема	Результати навчання	**Завдання**
2 / 1	**Тема 1.** Основні поняття та положення стеганографії.	Структура та зміст дисципліни, її зв'язок з іншими дисциплінами учбового плану. Цифрова стеганографія. Предмет, термінологія, галузь використання Структура та зміст дисципліни, зв'язок з іншими дисциплінами учбового плану, призначення стеганографічної системи, основна термінологія та визначення, потенціальні області використання стеганографії.	Тести, задачі, питання
2 / 1	**Тема 2.** Математична модель стеганосистеми. Практичні аспекти вбудування даних.	Загальна структурна схема стеганосистеми як системи зв'язку. Математична модель стеганосистеми. Стеганографічні системи з відкритим та закритими ключами. Стеганографічні протоколи. Призначення стеганодектору. Практичні аспекти вбудування даних.	Тести, задачі, питання
2 / 1	**Тема 3.** Основні напрямки практичного використання стеганографічних методів захисту інформації.	Класифікація стеганографічних систем та стегоконтейнерів. Основні напрями стегонографії. Вбудовування інформації з метою її прихованої передачі; вбудовування цифрових водяних знаків, вбудовування ідентифікаційних номерів, вбудовування заголовків. Загальна класифікацію контейнерів.	Тести, задачі, питання

2 / 1	**Тема 4.** Особливості зорової системи людини.	Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях. Аналіз механізмів зорового сприйняття людини. Низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні. Високорівневі властивості зорової системи людини..	Тести, задачі, питання
2 / 1	**Тема 5.** Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).	Особливості комп'ютерної обробки зображень. Структура форматів BMP, GIF, TIFF, JPEG. Структура файлів растрового зображення. Дескриптор екрану у форматі GIF, термінатор GIF, розширений блок GIF.	Тести, задачі, питання
2 / 1	**Тема 6.** Приховування даних у просторовій області зображень та відео.	Метод приховування в найменш значущому біті даних. Приховування даних у просторовій області зображень. Приховування даних у просторовій області відео.	Тести, задачі, питання
2 / 1	**Тема 7.** Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.	Метод псевдовипадкової перестановки для приховування даних у просторовій області зображень та відео. Приховування даних у просторовій області зображень методом псевдовипадкової перестановки. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.	Тести, задачі, питання
2 / 1	**Тема 8.** Приховування даних у просторовій області зображень та відео методом блокового приховування, заміни палітри та квантування зображення.	Метод блокового приховування. Метод заміни палітри. Метод квантування зображення.	Тести, задачі, питання
2 / 1	**Тема 9.** Приховування даних у частотній області зображень та відео.	Метод Коха та Жао. Приховування даних у частотній області зображень та відео. Приховування даних у частотній області методом Коха та Жао.	Тести, задачі, питання
2 / 1	**Тема 10.** Особливості слухової системи людини (ССЛ).	Основні властивості ССЛ, що використовуються при приховуванні даних в аудіо сигналах Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis). Особливості комп'ютерної обробки аудіо сигналів. Класи аудиосигналів.Опис форматів WAV, WMA, MP3, AAC, OGG Vorbis.	Тести, задачі, питання
2 / 1	**Тема 11.** Приховування даних у просторовій множині аудіосигналу.	Приховування даних у частотній множині аудіо сигналу.Приховування в найменш значущому біті даних та за допомогою ехосигналів.Фазове кодування.	Тести, задачі, питання
2 / 1	**Тема 12.** Приховування даних в аудіосигналах за допомогою методів розширення спектра.	Призначеня стегакодера й стеганодекодера. Вплив на ЦВДЗ застосування до аудіосигналу ковзного фільтра середніх частот.	Тести, задачі, питання

2 / 1	**Тема 13.** Методи текстової стеганографії.	Аналіз реалізації методів. Методи текстової стеганографії. Порівняння методів текстової стеганографії.	Тести, задачі, питання
2 / 1	**Тема 14.** Атаки на системи прихованої передачі повідомлень та методи протидії їм.	Атаки на системи цифрових водяних знаків. Класифікація атак на стеганосистеми цифрових відеознаків Атаки на стеганосистеми цифрових відео знаків. Методи протидії атакам на системи цифрових водяних знаків. Статистичний стегоаналіз та протидії. Методи протідії атакам на системи цифрових водяних знаків.	Тести, задачі, питання
2 / 1	**Тема 15.** Практична оцінка стійкості стеганосистем.	Теоретико-складнісний підхід до оцінки стійкості стеганосистем. Імітостійкість систем передачі прихованих повідомлень. Класифікація атак зловмисника. Досконала стеганосистема.	Тести, задачі, питання

Літературні джерела

1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К.: Центр навчальної літератури, 2018. — 558 с.
2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
3. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
4. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
5. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
6. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
7. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
8. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
9. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
10. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
11. Ахмаметьєва Г.В., Кирилюк В.О. Розробка стеганографічного методу вбудови бінарного цифрового водяного знаку в зображення на основі дискретного косинусного перетворення. Інформатика та математичні методи в моделюванні. 2021. Том 11, № 1-2. С.5-14.
12. Manasha Saqib, Sameena Naaz. An Improvement in Digital Image Watermarking Scheme Based on Singular Value Decomposition and Wavelet Transform. Asian Journal of Computer Science and Technology. 2019. Vol. 8, No. 1. P. 62-68.
13. Jayashree N., Bhuvaneswaran R.S. A Robust Image Watermarking Scheme Using Z-Transform, Discrete Wavelet Transform and Bidiagonal Singular Value Decomposition. CMC-Tech Science Press. 2019. Volume 58, No. 1. P. 263-285.

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

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

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

17. Rand A. Watheq, Fadi Almasalha, Mahmoud H. Qutqut. A New Steganography Technique using JPEG Images. International Journal of Advanced Computer Science and Applications. 2018. Vol. 9, No. 11. P. 751-760.

18. Osama F. Abdel Wahab, Aziza I. Hussein, Hesham F.A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf, Hanafy M. Ali. Hiding data in images using steganography techniques with compression algorithms. TELKOMNIKA. 2019. Vol. 17, No. 3. P. 1168-1175

Політика оцінювання

- **Політика щодо дедлайнів та перескладання**: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності**: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
- **Політика щодо відвідування**: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
30%	40%	30%
1. Усне опитування на заняттях: 4 заняття по 6 балів – max 24 балів. 2. Письмова робота – max 52 бали. 3. Практичне завдання: 4 практичних завдання по 6 балів – max 24 бали.	1. Усне опитування на заняттях: 4 заняття по 6 балів – max 24 бали. 2. Письмова робота – max 52 балів. 3. Практичне завдання: 4 практичних завдання по 6 балів – max 24 бали.	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Виконання завдань на тренінгах – max 30 балів

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом