



Силабус курсу СТЕГАНОГРАФІЧНІ МЕТОДИ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Дисципліна циклу: вибіркова
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

ППП

Контактна інформація

Керівник курсу

Михайло КАСЯНЧУК

kmm@wunu.edu.ua

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. / лаб	Тема	Результати навчання	Завдання
4/ -	Основні поняття та положення стеганографії.	Визначають сутність стеганографії та відмінності від криптографії. Описують основні терміни (стегоносій, повідомлення, контейнер, стегоканал). Усвідомлюють роль стеганографії в інформаційній безпеці.	Поточне опитування
2 / 2	Математична модель стеганосистеми. Практичні аспекти вбудовування даних.	Розуміють формальні моделі стеганосистем. Пояснюють принципи вбудовування прихованих даних у цифрові носії. Аналізують співвідношення між місткістю, стійкістю та непомітністю.	Поточне опитування

2 / -	Основні напрямки практичного використання стеганографічних методів захисту інформації.	Наводять приклади застосування стеганографії у військовій, комерційній та особистій сфері. Аналізують переваги й недоліки різних методів застосування. Оцінюють актуальність використання стеганографії у сучасних мережах і сервісах.	Поточне опитування
2 / 2	Особливості зорової системи людини.	Описують психофізіологічні особливості зорового сприйняття. Визначають принципи, що використовуються для непомітного приховування зображень. Розуміють поняття чутливості до кольору, яскравості, контрасту.	Поточне опитування
2 / -	Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).	Описують структуру найпоширеніших графічних форматів. Розуміють можливості та обмеження форматів у стеганографії. Вміють обирати оптимальний формат для приховування даних.	Поточне опитування
2 / 2	Приховування даних у просторовій області зображень та відео.	Пояснюють методи прямої модифікації пікселів. Виконують прості приклади приховування у зображеннях. Аналізують якість та непомітність стеганографічного вбудовування.	Поточне опитування
2 / -	Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.	Розуміють принцип використання ключа для псевдовипадкової зміни позицій даних. Аналізують ефективність методу у забезпеченні стійкості. Виконують практичні приклади реалізації.	Поточне опитування
2 / 2	Приховування даних у просторовій області зображень та відео методом блокового приховування, заміни палітри та квантування зображення.	Пояснюють принципи роботи кожного з методів. Порівнюють їх ефективність залежно від типу зображень.	Поточне опитування

		Виконують практичні вправи з використанням цих методів.	
2 / -	Приховування даних у частотній області зображень та відео.	Розуміють принципи перетворень (ДКП, ДХП, вейвлети). Оцінюють переваги приховування у частотній області для підвищення стійкості. Виконують базові приклади вбудовування даних у частотну область.	Поточне опитування
2 / 2	Особливості слухової системи людини.	Пояснюють фізіологічні особливості слухового сприйняття. Розуміють принципи маскування звуку. Використовують ці властивості для приховування даних в аудіо.	Поточне опитування
2 / -	Приховування даних у просторовій множині аудіосигналу.	Описують методи прямої модифікації семплів аудіо. Аналізують якість сигналу після вбудовування. Виконують прості приклади приховування в аудіо.	Поточне опитування
2 / 2	Приховування даних в аудіосигналах за допомогою методів розширення спектра.	Пояснюють суть спектрального розширення. Виконують приклади приховування з використанням шумоподібних сигналів. Оцінюють стійкість цього підходу до атак.	Поточне опитування
2 / -	Методи текстової стеганографії.	Розуміють основні прийоми: зміна пробілів, шрифтів, формату. Аналізують ефективність приховування у текстових даних. Виконують приклади побудови простих стеготекстів.	Поточне опитування
2 / 2	Атаки на системи прихованої передачі повідомлень та методи протидії їм.	Описують основні види атак: статистичні, візуальні, структурні. Аналізують вразливості різних методів стеганографії. Пропонують способи	Поточне опитування

		підвищення стійкості стеганосистем.	
2 / -	Практична оцінка стійкості стеганосистем.	Виконують аналіз місткості, непомітності й стійкості систем. Застосовують метрики для оцінювання якості (PSNR, SSIM, BER). Формують висновки щодо надійності конкретних реалізацій.	Поточне опитування

Рекомендовані джерела інформації

1. Stallings, W., & Brown, L. Computer Security: Principles and Practice (4th ed.). Pearson. 2022. 384 p.
2. Ya.M.Nykolaychuk, M.M.Kasianchuk, I.Z.Yakymenko. Symmetric Crypt algorithms in the Residue Number System/ // Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. 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/
5. 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.
6. Ахмет'єва 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.
7. 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.
8. Mahbuba Begum, Mohammad Shorif Uddin. Analysis of Digital Image Watermarking Techniques through Hybrid Methods, Advances in Multimedia. 2020. Volume 2020. P. 1-12.
9. Sunesh R. Rama Kishore. A Novel and Efficient Blind Image Watermarking in Transform Domain. Procedia Computer Science. 2020. No. 167. P. 1505-1514.
10. Rand A. Watheq, Fadi Almasalha, Mahmoud H. Qutut. A New Steganography Technique using JPEG Images. International Journal of Advanced Computer Science and Applications. 2020. Vol. 9, No. 11. P. 751-760.

Політика оцінювання

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

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

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за

погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

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

Шкала оцінювання

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