МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри .

Венгерський П.С.

Силабус з навчальної дисципліни
“Цифрова стеганографія ”,
що викладається в межах ОПП Кібербезпека
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	Цифрова стеганографія
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Пелешко Дмитро Дмитрович, Професор кафедри кібербезпеки
Контактна інформація викладачів	Dmytro.peleshko@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	
Інформація про дисципліну	Дисципліна “Цифрова стеганографія ” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека та захист інформації, яка викладається в 8-му семестрі в обсязі 6-и кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на вивчення процесів механізмів, методів та засобів стеганографічного захисту цифрової інформації в інформаційних системах.
Мета та цілі дисципліни	Метою курсу є формування у студентів професійних компетенцій, знань та вмінь у галузі цифрової стеганографії Основними завданнями з вивчення навчальної дисципліни є отримання студентами необхідних базових знань з теоретичних основ побудови стеганографічних систем захисту інформації, методів та алгоритмів приховування інформації у різноманітних цифрових носіях.
Література для вивчення дисципліни	Основна література 1. Gerardus Blokdyk. Steganography Third Edition Paperback. 5STARCooks , 2022. 303 p. 2. Sunil Tanna. Codes, Ciphers, Steganography & Secret Messages. Independently published. 2021. 173p 3. V. Verma, S. K. Muttoo and V. B. Singh, "Enhanced payload and trade-off for image steganography via a novel pixel digits alteration", Multimedia Tools Appl., vol. 79, no. 11, pp. 7471-7490, Mar. 2020. 4. O. Evsutin; A. Melman; R. Meshcheryakov. "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions". 2020. doi:10.1109/ACCESS.2020.3022779 5. Principles and Overview of Network Steganography [Електронний ресурс] – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1207/1207.0917.pdf.. 6. Implementation of LSB Steganography and its Evaluation for Various File Formats [Електронний ресурс] – Режим доступу до ресурсу: https://pdfs.semanticscholar.org/3dce/b6307cee042b687b7f377ec1d5de

	91ce20b0.pdf 7. Data Hiding using Graphical Code based Steganography Technique [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/282403473_Data_Hiding_using_Graphical_Code_based_Steganography_Technique. 8. An Overview of Steganography for the Computer Forensics Examiner [Електронний ресурс] – Режим доступу до ресурсу: https://www.garykessler.net/library/fsc_stego.html. 9. Steganography and Digital Watermarking: a global view [Електронний ресурс] – Режим доступу до ресурсу: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf. Додаткова література 10. CURRENT TRENDS IN STEGANALYSIS: A CRITICAL SURVEY [Електронний ресурс] – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.331.3139&rep=rep1&type=pdf. 11. Unicode Steganography with Zero-Width Characters [Електронний ресурс] – Режим доступу до ресурсу: https://330k.github.io/misc_tools/unicode_steganography.html. 12. Detection of HTML Steganography Based on Statistics and SVM Classification [Електронний ресурс] – Режим доступу до ресурсу: http://xwxt.sict.ac.cn/EN/abstract/abstract2372.shtml 13. DeepSound. [Електронний ресурс]. – Режим доступа: 53 http://jpinsoft.net/DeepSound/Overview.aspx (дата звернення 20.02.2022). 14. Xiao Steganography. [Електронний ресурс]. – Режим доступа: http://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html (дата звернення 20.02.2022). 15. SilentEye. [Електронний ресурс]. – Режим доступа: http://silenteye.v1kings.io/index.html?i1s1 (дата звернення 20.02.2022). 16. StegoStick beta. [Електронний ресурс]. – Режим доступа: https://sourceforge.net/projects/stegostick/ (дата звернення 20.02.2022). 17. Digital Invisible Ink Toolkit. [Електронний ресурс]. – Режим доступа: https://sourceforge.net/projects/diit/?source=typ_redirect (дата звернення 20.02.2022).
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 110 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • визначення стеганографічних систем; • класифікацію та основні властивості стеганографічних систем; • математичні моделі стеганографічних операцій; • методи та алгоритми стеганографічного захисту цифрових зображення, • методи та алгоритми стеганографічного захисту аудіо сигналів; • методи та обчислювальні алгоритми стеганографічного захисту текстових документів; • визначення, класифікацію та методи стеганоаналізу. **вміти:**

	• практично реалізовувати стеганографічний захист цифрових зображень, аудіо файлів та текстових документів; • оцінювати інвізибільність (невидимість) результатів стеганографічного захисту; • оцінювати стійкість (робастність) стеганографічних систем до різних атак. Курс забезпечує набуття таких компетентностей: ІК, ЗК 1, ЗК 2, ЗК 3, ЗК 5, ФК 2, ФК 3, ФК 9, ФК 11; та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 11, ПРН 12, ПРН 13, ПРН 15, ПРН 15, ПРН 17, ПРН 18, ПРН 19, ПРН 20, ПРН 33, ПРН 34.
Ключові слова	стеганозахист, приховування інформації, невидимість, робастність приховування, стеганоатаки, захист цифрових зображень, аудіофайлів, наймеш значущий біт, спектр вигналу
Формат курсу	Очний
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	залік у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін як: • Програмування • Основи обробки сигналів. • Лінійна алгебра • Дискретна математика
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, опитування теоретичного матеріалу під час лабораторних робіт, контрольна робота (модуль).
Необхідне обладнання	Комп'ютерний клас із вільно-доступним програмним забезпеченням, локальна комп'ютерна мережа, доступ до Internet мережі.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: написання двох контрольних робіт (модулів): по 25% семестрової оцінки; максимальна кількість балів 50. лабораторні роботи: 50% семестрової оцінки; максимальна кількість балів 50. Підсумкова максимальна кількість балів – 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недобро-

	чесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до контролю	1. Математична модель та структурна схема стеганосистеми 2. Атаки на стеганосистеми 3. Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень 4. Приховування даних у просторовій області нерухомих зображень. 5. Методи приховування на основі модифікації НЗБ 6. Приховування даних у просторовій області нерухомих зображень. 7. Блокове приховування, метод квантування, метод «хреста» 8. Приховування даних із використанням технології прямого розширення спектру 9. Приховування даних із застосуванням складних дискретних сигналів та технології прямого розширення спектр 10. Приховування даних у частотній області нерухомих зображень. Метод Коха-Жао та його модифікації 11. Стеганографічні методи приховування даних в аудіофайлах 12. Приховування даних у просторовій області аудіо сигналів 13. Приховування даних у частотній області аудіо сигналів 14. Приховування даних у текстових документах 15. Приховування даних у кластерних файлових системах 16. Мережева стеганографія
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдан-ня, год.	Термін виконання
1-2	**Тема 1. Цифрова стеганографія** (предмет, термінологія, галузь, основні визначення та базові поняття, модель та структурна схема стеганосистеми)	лекція, самостійна робота лаб	[1, 2 6, 9]	4 14 4	2 тижні
3-4	**Тема 2. Стеганоаналіз Розподілені системи** (види атак, критерії та показники ефективності стеганосистем)	лекція, самостійна робота лаб	[1, 2, 8, 10]	4 14 6	2 тижні
5-7	**Тема 3. Стеганозахист цифрових зображень(** основні поняття цифрових зображень, просторові методи, спектральні методи)	лекція, самостійна робота лаб	[3,4,7, 16, 17]	6 30 4	5 тижнів
5-7	**Тема3. Стегано захист цифрових зображень у частотній області**	лаб		4	3 тижні
8	**Тема 4. Стеганозахист аудіофайлів** (основні поняття теорії аудіосигналів, просторові методи, спектральні методи)	лекція, самостійна робота лаб	[1, 2, 13, 15]	6 22 2	4 тижні
9-10	**Тема 4. Стегано захист аудіофайлів у просторовій області**	лаб		6	2 тижні
11	**Тема 5. Стеганозахист цифрових текстових документів** (приховування даних у текстових документах)	лекція, самостійна робота	[1, 2, 11]	4 10	1 тиждень
12	**Тема 5. Приховування даних у текстових документах**	лаб		6	2 тижні
13	**Тема 6. Мережева стеганографія** (організація приховування в електронних транзакціях)	лекція, самостійна робота лаб	[1, 2, 5]	2 10 4	1 тиждень
14	**Тема 6. Основи стеганозахисту відеотоків** (класифікація методів, аналіз просторових методи)	лекція, самостійна робота	[1, 2, 14]	2 10	1 тиждень
14	**Тема 6. Мережева стеганографія**	лаб		6	1 тиждень