СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЦИФРОВА СТЕГАНОГРАФІЯ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Спеціальність	125 Кібербезпека та захист інформації
	Тривалість викладання	15 чверть
	Заняття:	весняний семестр
	лекції:	3 години
	практичні заняття:	2 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5408

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладача:

Герасіна Олександра Володимирівна	доцент, к.т.н.
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/gerasina.php
E-mail:	**herasina.o.v@nmu.one**

1. Анотація до курсу

Сучасні комп'ютерні технології обробки даних дозволили суттєво підвищити рівень інформаційної та кібербезпеки безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. На відміну від криптографічного захисту інформації, стеганографічні підходи намагаються у першу чергу приховати сам факт існування конфіденційної інформації. Методи стеганографії дозволяють не лише приховано передавати дані, але й успішно вирішувати задачі завадостійкої аутентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку тощо.

Наразі переважна більшість досліджень в галузі стеганографії так або інакше пов'язана з цифровою обробкою сигналів – секретні повідомлення вбудовуються у цифрові дані, які, як правило, мають аналогову природу (мова, зображення, аудіо- і відео). Все це дозволяє говорити про **цифрову стеганографію**.

Цифрова стеганографія містить у собі такі напрями: вбудовування інформації з метою її прихованої передачі, вбудовування цифрових водяних знаків, вбудовування ідентифікаційних номерів, вбудовування заголовків.

Послідовність вивчення матеріалу курсу **«Цифрова стеганографія»** підпорядкована наступним етапам. По-перше, це загальні відомості про історію і сучасний розвиток стеганографії, принципи побудови стеганографічних систем прихованої передачі даних, а також стеганографічного аналізу. По-друге –

стеганографічні методи приховування даних в контейнерах різних форматів (зображення, текст, аудіо). По-третє – організація прихованих каналів в комп'ютерних системах і мережах, цифрові водяні знаки та цифрові відбитки.

2. Мета та завдання курсу

Мета дисципліни – формування у студентів компетентностей щодо принципів використання цифрової стеганографії у сучасному інформаційному просторі: особливостей побудови стеганографічних систем прихованої передачі інформації та цифрових водяних знаків, стеганографічного аналізу, аналізу атак на стеганоконтейнери та оцінювання стійкості, а також методів приховування даних в різних контейнерах.

Завдання курсу:

– ознайомити здобувачів вищої освіти із загальними відомостями про стеганографію;

– ознайомити здобувачів вищої освіти з принципами побудови, проблемами стійкості та протоколами стеганографічних систем;

– ознайомити здобувачів вищої освіти з видами атак на стеганографічну систему, принципами стеганографічного аналізу, а також з процедурою оцінювання стійкості стеганосистеми;

– ознайомити здобувачів вищої освіти з класифікацією методів приховування даних та основними властивостями зорової системи людини;

– ознайомити здобувачів вищої освіти з методами приховування даних у нерухомих зображеннях: просторовими, частотними, розширення спектру та іншими;

– ознайомити здобувачів вищої освіти з методами приховування даних у тексті.

– ознайомити здобувачів вищої освіти з методами приховування даних в аудіосигналах;

– ознайомити здобувачів вищої освіти з поняттям пропускної здатності каналів передачі приховуваних даних, підходами до організації прихованих каналів в комп'ютерних системах і мережах;

– ознайомити здобувачів вищої освіти з принципами побудови, класифікацією і вимогами до систем цифрових водяних знаків, а також із методами ЦВЗ;

– ознайомити здобувачів вищої освіти із поняттям про цифрові відбитки та схемами реєстрації цифрового відбитка.

3. Результати навчання

- забезпечувати процеси захисту авторських прав, прав інтелектуальної власності або конфіденційних даних від несанкціонованого доступу в інформаційно-комунікаційних (автоматизованих) системах;

- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах із використанням стеганографічних методів;

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах із використанням стеганографічних методів.

4. Структура курсу

ЛЕКЦІЇ

1. Загальні відомості про стеганографію.
   1.1 Історія і сьогодення стеганографії.
   1.2 Класифікація стеганографічних методів.
2. Особливості побудови стеганографічних систем.
   2.1 Предмет, термінологія, області застосування стеганографії.
   2.2 Проблема стійкості стеганографічних систем.
   2.3 Структурна схема і математична модель стеганосистеми.
   2.4 Протоколи стеганографічних систем.
3. Принципи стеганографічного аналізу.
   3.1 Види атак на стеганографічну систему.
   3.2 Основні етапи практичного стеганоаналізу.
   3.3 Оцінювання якості стеганосистеми.
   3.4 Абсолютно надійна стеганосистема.
   3.5 Стійкість стеганосистем до пасивних та активних атак.
   3.6 Свідомо відкритий стеганографічний канал.
4. Стеганографічні методи приховування даних.
   4.1 Класифікація методів приховування даних
   4.2 Приховування даних у нерухомих зображеннях. Основні властивості зорової системи людини, які враховують при побудові стеганоалгоритмів. Приховування даних у просторовій та частотній області зображення. Методи розширення спектру. Статистичні і структурні методи.
   4.3 Приховування даних у тексті.
   4.4 Приховування даних в аудіосигналах.
5. Приховані канали в комп'ютерних системах і мережах.
   5.1 Поняття пропускної здатності каналів передачі приховуваних даних.
   5.2 Приховування даних у невикористаних і зарезервованих полях, у виконуваних файлах та в операційних системах.
   5.3 Організація прихованих каналів криптографічними засобами.
   5.4 Поняття про клептографію.
6. Цифрові водяні знаки.
   6.1 Приклади використання цифрових водяних знаків.
   6.2 Узагальнена модель системи цифрових водяних знаків.
   6.3 Класифікація і вимоги до систем цифрових водяних знаків.
   6.4 Методи цифрових водяних знаків.
7. Цифрові відбитки.
   7.1 Термінологія і основні положення.
   7.2 Схеми реєстрації цифрового відбитка: статистична, асиметрична, анонімна.

ПРАКТИЧНІ ЗАНЯТТЯ

1. Приховування та вилучення інформації за допомогою програми OpenPuff.
2. Вбудовування цифрового водяного знаку за допомогою програми OpenPuff.
3. Приховування та вилучення інформації у файлах формату JPEG за допомогою програми JPHS.
4. Приховування та вилучення інформації у графічних файлах за допомогою програми S-Tools.
5. Приховування та вилучення інформації в аудіо файлах за допомогою програми S-Tools.

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

Безкоштовне програмне забезпечення OpenPuff, JPHS, S-Tools.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	40	25	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі білетів диференційного заліку у весняному семестрі. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі

виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 балів – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи:

8 балів – достатня зрозумілість відповіді;

6 балів – добра зрозумілість відповіді;

3 бали – задовільна зрозумілість відповіді;

0 балів – незадовільна зрозумілість відповіді.

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни «Цифрова стеганографія». За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 Рекомендовані джерела інформації

1. Хорошко В.О. Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець. − Вінниця: ВНТУ, 2017. − 155 с.
2. Конахович Г.Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник / Г.Ф. Конахович, Д.О. Прогонов, О.Ю. Пузиренко. – К. : «Alex Print Centre», 2018. – 558 с.
3. Кузнецов О.О. Стеганографія: навчальний посібник / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
4. Технології захисту інформації: підручник / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ЦК «Компринт», 2021. – 296 с.
5. Євсеєв С.П. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.П. Євсеєв, С.Е. Остапов, О.Г. Король. – Львів: "Новий Світ- 2000", 2019. – 678..
6. Захист інформації в комп'ютерних системах: підручник. / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.
7. Кібербезпека: основи кодування та криптографії / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.