МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
Навчально-науковий інститут автоматики і електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
роботи, к.т.н., доцент
_____ С.О. Слободян
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Academic Discipline

Цифрова стеганографія

Digital Steganography

Рівень вищої освіти перший (бакалаврський)
Тип дисципліни вибіркова
Мова викладання українська

Миколаїв – 2023

Робоча програма навчальної дисципліни «Цифрова стеганографія» є однією зі складових комплексної підготовки фахівців на першому (бакалаврському) рівні технічних спеціальностей.
«2» 02 2023 р. – 16 с.

Розробник: к.т.н., доцент Козирєв С.С., доцент кафедри комп'ютерних технологій та інформаційної безпеки (КТІБ).

Проєкт робочої програми навчальної дисципліни «Цифрова стеганографія» розглянуто на засіданні кафедри КТІБ.
Протокол від «2» 02 2023 р. № 7.

Завідувач кафедри КТІБ, к.т.н., доцент _____ С.М. Нужний

Проєкт робочої програми навчальної дисципліни «Цифрова стеганографія» розглянуто методичною комісією Навчально-наукового інституту автоматики і електротехніки.
Протокол від «14» 02 2023 р. № 6.

Голова, к.т.н., доцент _____ Д.О. Жук

Проєкт робочої програми навчальної дисципліни «Цифрова стеганографія» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент _____ А.В. Лабарткава

Робочу програму навчальної дисципліни «Цифрова стеганографія» затверджено Навчально-методичною радою НУК ім. адм. Макарова.
Протокол від «22» 02 2023 р. № 1.

Голова Навчально-методичної ради НУК ім. адм. Макарова,
д.т.н., професор _____ Є.І. Трушляков

© Козирєв С.С., 2023 рік
© НУК, 2023 рік

Анотація

Навчальна дисципліна «Цифрова стеганографія» є вибірковою навчальною дисципліною та забезпечує набуття знань з базових основ аналізу та синтезу сучасних стеганографічних систем у відповідності до задач та вимог щодо захисту інформації.

В наш час використання та розробка стеганографічних систем захисту інформації є невід'ємною складовою науково-технічного процесу. Курс знайомить студентів з поняттям цифрової стеганографії; моделями стеганосистем; основними вимогами до стеганосистем; відкритими, напівзакритими та закриті стеганосистемами. Ознайомлення студентів з основами побудови сучасних стеганографічних систем розширить їх можливості з обрання найбільш надійних інформаційних систем для використання у своїй сфері діяльності.

Отримані навички надають основу для подальшого освоєння методів побудови стеганографічних систем захисту інформації більш високого рівня.

Курс призначений для студентів всіх спеціальностей.

Ключові слова: цифрова стеганографія, захист інформації, стеганосистеми.

Abstract

The discipline "Digital Steganography" is a selective discipline which provides knowledge on the basic principles of analysis and synthesis of modern steganographic systems in accordance with the tasks and requirements of information security.

Currently, the use and development of steganographic information security systems is an integral part of the scientific and technical process. The course introduces students to the concept of digital steganography; models of steganosystems; basic requirements for steganosystems; open, semi-closed and closed steganosystems. Familiarization of students with the basics of building modern steganographic systems will expand their ability to select the most reliable information systems for use in their field of activity.

The acquired skills provide a basis for further mastering the methods of building steganographic security systems of a higher level.

The course is intended for students of all majors.

Key words: digital steganography, information security, steganosystems.

ЗМІСТ

1. Опис навчальної дисципліни 5
2. Мета вивчення навчальної дисципліни 6
3. Передумови для вивчення навчальної дисципліни 6
4. Очікувані результати навчання 6
5. Програма навчальної дисципліни 7
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування 12
7. Форми поточного та підсумкового контролю 13
8. Критерії оцінювання результатів навчання 15
9. Засоби навчання 15
10. Рекомендовані джерела інформації 16

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="3">–</td><td colspan="2">Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td><td>–</td></tr>
<tr><td rowspan="6">Електронна адреса РПНД на сайті Університету
_____
Індивідуальне науково-дослідне завдання не передбачено</td><td rowspan="6">–</td><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>30 год.</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td rowspan="2">–</td><td colspan="2">Практичні</td></tr>
<tr><td>30 год.</td><td>–</td></tr>
<tr><td rowspan="5">Тижневих годин для денної форми навчання:
- аудиторних: 4;
- самостійної роботи: 6.</td><td rowspan="5">Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Самостійна робота</td></tr>
<tr><td>90</td><td>–</td></tr>
<tr><td colspan="2">Індивідуальне завдання не передбачено</td></tr>
<tr><td colspan="2">Вид контролю:
залік.</td></tr>
<tr><td colspan="2">Форма контролю:
усна, письмова.</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

- для денної форми навчання – 2:3.

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни «Цифрова стеганографія» є формування у здобувачів вищої освіти компетентностей, необхідних для аналізу та синтезу сучасних цифрових стеганографічних систем у відповідності до задач та вимог щодо захисту інформації в професійній сфері.

Елементи компетентностей:

- знати основні методи, системи та засоби забезпечення стеганографічного захисту інформації;
- знати моделі цифрових стеганосистем та основні вимоги до стеганосистем;
- знати методи побудови цифрових стеганографічних систем захисту інформації;
- уміти працювати з відкритими, напівзакритими та закритими цифровими стеганосистемами;
- уміти розробляти вимоги та обирати для застосування цифрові стеганосистеми та стеганопротоколи, що мінімізують впливи порушників.

3. Передумови для вивчення навчальної дисципліни

Передумов для вивчення навчальної дисципліни «Цифрова стеганографія» немає.

4. Очікувані результати навчання

Програмні результати навчання полягають в наступному:

- знання основ цифрової стеганографії та основних вимог до стеганосистем;
- знання моделей цифрових стеганосистем;
- знання класифікації систем цифрової стеганографії та можливостей їх використання;
- мати уяву про метод модифікації найменшого значущого біта;
- мати уяву про цифрові водяні знаки (ЦВЗ) та їх класифікацію;
- уміння виявляти можливі атаки на стеганосистеми і протидіяти їм;
- уміння застосовувати стандартні пакети при розв’язанні прикладних задач моделювання цифрових стеганосистем, ключових систем і стеганографічних протоколів.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основи цифрової стеганографії. Практичні аспекти побудови стеганосистем

Тема 1. Предмет цифрової стеганографії, основні терміни та визначення, галузі застосування.

Тема 2. Математична модель та структурна схема цифрової стеганографічної системи.

Тема 3. Приховування даних у нерухомих зображеннях. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Особливості комп'ютерної обробки зображень.

Тема 4 Основні етапи алгоритму стиску зображень JPEG. Атаки на стеганосистеми із застосуванням JPEG.

Тема 5. Приховування даних у просторовій множині зображень. Методи приховування в найменш значущому біті даних.

Тема 6. Приховування даних у частотній множині зображень.

Тема 7. Приховування даних у текстових файлах. Методи текстової стеганографії.

Змістовий модуль 2. Атаки на цифрові стеганосистеми та методи протидії

Тема 5. Класифікація атак на стеганосистеми цифрових відеознаків (ЦВДЗ).

Тема 6. Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків (ЦВЗ).

Тема 7. Методи протидії атакам на стеганосистеми. Статистичний стегааналіз та метод протидії.

Тема 8. Практична оцінка стійкості стеганосистем. Імітостійкість систем передачі прихованих повідомлень.

Тема 9. Візуальна атака на стеганосистеми.

Тема 10. Статистичні атаки на стеганосистеми із зображеннями-контейнерами.

Тема 11. Напрями підвищення захищеності стеганосистем від статистичних атак.

Тема 12. Імітостійкість системи передачі приховуваних повідомлень.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма навчання					Заочна форма навчання				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		лек.	пр.	лаб.	с.р.		лек.	пр.	лаб.	с.р.
Змістовий модуль 1. Базові інструменти технічних розрахунків										
Тема 1. Предмет цифрової стеганографії, основні терміни та визначення, галузі застосування.	10	2	2	–	6	–	–	–	–	–
Тема 2. Математична модель та структурна схема цифрової стеганографічної системи.	10	2	2	–	6	–	–	–	–	–
Тема 3. Приховування даних у нерухомих зображеннях. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Особливості комп'ютерної обробки зображень.	10	2	2	–	6	–	–	–	–	–
Тема 4. Основні етапи алгоритму стиску зображень JPEG. Атаки на стеганосистеми із застосуванням JPEG.	10	2	2	–	6	–	–	–	–	–
Тема 5. Приховування даних у просторовій множині зображень. Методи приховування в найменш значущому біті даних.	10	2	2	–	6	–	–	–	–	–

Назви змістових модулів і тем	Денна форма навчання					Заочна форма навчання				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		лек.	пр.	лаб.	с.р.		лек.	пр.	лаб.	с.р.
Тема 6. Приховування даних у частотній множині зображень.	10	2	2	–	6	–	–	–	–	–
Тема 7. Приховування даних у текстових файлах. Методи текстової стеганографії.	10	2	2	–	6	–	–	–	–	–
Разом за змістовим модулем 1	***70***	***14***	***14***	**–**	***42***	–	–	–	–	–
Змістовий модуль 2. Атаки на цифрові стеганосистеми та методи протидії										
Тема 8. Класифікація атак на стеганосистеми цифрових відеознаків (ЦВДЗ).	10	2	2	–	6	–	–	–	–	–
Тема 9. Атаки проти систем прихованої передачі повідомлень. Атаки на системи цифрових водяних знаків (ЦВЗ).	10	2	2	–	6	–	–	–	–	–
Тема 10. Методи протидії атакам на стеганосистеми. Статистичний стегааналіз та метод протидії.	10	2	2	–	6	–	–	–	–	–

Назви змістових модулів і тем	Денна форма навчання					Заочна форма навчання				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		лек.	пр.	лаб.	с.р.		лек.	пр.	лаб.	с.р.
Тема 11. Практична оцінка стійкості стеганосистем. Імітостійкість систем передачі прихованих повідомлень.	10	2	2	–	6	–	–	–	–	–
Тема 12. Візуальна атака на стеганосистеми.	10	2	2	–	6	–	–	–	–	–
Тема 13. Статистичні атаки на стеганосистеми із зображеннями-контейнерами.	10	2	2	–	6	–	–	–	–	–
Тема 145. Напрями підвищення захищеності стеганосистем від статистичних атак.	10	2	2	–	6	–	–	–	–	–
Тема 15. Імітостійкість системи передачі приховуваних повідомлень.	10	2	2	–	6	–	–	–	–	–
Разом за змістовим модулем 2	***80***	***16***	***16***	**–**	***48***	–	–	–	–	–
Разом за курсом	**150**	**30**	**30**	**–**	**90**	–	–	–	–	–

Теми практичних занять

№	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
Змістовий модуль 1			
1	Ознайомлення з типами програм для цифрової стеганографії	2	–
2	Методи модифікації LSB (Least Significiant Bit, найменший значущий біт)	4	–
3	Програма для приховування інформації в зображеннях OpenStego	4	–
4	Програма стеганографії SilentEye для приховування інформації зображеннях та аудіо файлах	2	–
5	Програма стеганографії OpenPuff для приховування інформації в медіа файлах із використанням криптографії	2	
Змістовий модуль 2			
6	Програма стеганографії DarkCryptTC, яка підтримує різні симетричні та асиметричні криптоалгоритми	4	–
7	Освоєння методів протидії атакам на системи цифрових водяних знаків (ЦВЗ).	2	–
8	Освоєння методів протидії статистичному стегааналізу	4	–
9	Освоєння методів протидії статистичним атакам на стеганосистеми зі зображеннями-контейнерами	4	–
10	Освоєння методів оцінки стійкості стеганографічних систем	2	
	Разом	**30**	

За необхідністю можуть проводитись групові та індивідуальні консультації за розкладом кафедри в тому числі із застосуванням дистанційних технологій навчання. Це сприяє роз'ясненню найбільш складних питань дисципліни та підвищенню якості виконання завдань.

Практичні заняття проводяться в лабораторіях кафедри з використанням комп'ютерної техніки. Допускається виконання практичних завдань в дистанційному режимі із застосуванням персонального комп'ютерна за межами лабораторій кафедри.

Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, включається в завдання поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Денна форма навчання

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 год. занять;
- підготовка та виконання практичних робіт – 3 год. /1 робота;
- підготовка до контрольних заходів – 15 год. на 1 захід.

Заочна форма навчання

Викладання навчальної дисципліни для здобувачів вищої освіти заочної форми навчання не передбачено.

Завдання для самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	15	–
2	Самостійне опрацювання окремих тем навчальної дисципліни	15	–
3	Виконання практичних робіт	30	–
4	Підготовка до модульних контрольних робіт	30	–
Усього годин за модуль 1 (разом за курсом)		**90**	–

Індивідуальне науково-дослідне завдання

Виконання індивідуального науково-дослідного завдання робочою програмою не передбачено.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Методи навчання:

- лекція - усний виклад навчального матеріалу з використанням слайдів, інтернет-ресурсів, рекламних матеріалів виробників програмних продуктів, базових програмних засобів;

- робота з літературою - опрацювання різних видів джерел, спрямоване на формування нових знань у сфері цифрової стеганографії, їх закріплення;

- практична робота - вивчення в спеціалізованих лабораторіях методів і засобів цифрової стеганографії з використанням спеціального програмного забезпечення.

Засобами оцінювання результатів навчання є:

- звіти з практичних робіт;
- модульні контрольні роботи;
- залік.

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з практичних робіт;
- проходження поточного та підсумкового контролю.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету. Підсумкова оцінка навчального курсу включає в себе оцінки з поточного та підсумкового контролю.

Поточний контроль здійснюється в наступних формах:

- перевірка та проведення процедури захисту звітів з практичних робіт;
- проведення та перевірка модульних контрольних робіт;

Підсумковий контроль здійснюється в формі заліку – підсумкова оцінка формується як сума оцінок, отриманих в результаті поточного та підсумкового контролю і становить до 100 балів включно.

Розподіл балів за формами контролю,
при яких результати навчання вважаються досягнутими

№	Форма контролю	Максимальна/мінімальна кількість балів	
		Денна форма навчання	Заочна форма навчання
Модуль 1			
1	Перевірка та проведення процедури захисту звітів з практичних робіт	60/36	–
2	Проведення та перевірка модульних контрольних робіт (2 контрольні роботи)	20/12	–
3	Залік у формі тестування	20/12	–
	Разом за модуль 1	100/60	–

Практична робота	
Кількість балів	Критерії оцінювання
6	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках проведена коректна інтерпретація результатів.
5	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані мета та завдання досліджень. Коректно застосовано необхідне програмне забезпечення. Досягнуто результатів, що відповідають поставленому завданню. У висновках при інтерпретації результатів допущено неточності.
4	Робота виконана з порушенням встановлених термінів. Студент виконує практичну роботу самостійно; складений звіт містить неточності у висновках.
3	Робота виконана з порушенням встановлених термінів. Студент виконує практичну роботу самостійно; складений звіт містить неточності у висновках та помилки.
2	Робота виконана з порушенням встановлених термінів. Складений звіт містить неточності у висновках та помилки.
0	Робота не виконана.
	Максимальна кількість балів за даний компонент програми 60 балів (10 робіт по 6 балів).

Поточний модульний контроль у формі тестування

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

Підсумковий контроль (залік у формі тестування)

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	20	18	16	14	12	10	8	6	4	2

8. Критерії оцінювання результатів навчання

Розподіл балів за змістовими модулями

		Вид роботи	Кількість балів
Змістовий модуль 1	Тема 1 -7	Практична робота № 1	6
		Практична робота № 2	6
		Практична робота № 3	6
		Практична робота № 4	6
		Практична робота № 5	6
Поточний контроль		Тестування	10
Змістовий модуль 2	Тема 8-15	Практична робота № 6	6
		Практична робота № 7	6
		Практична робота № 8	6
		Практична робота № 9	6
		Практична робота № 10	6
Поточний контроль		Тестування	10
Підсумковий контроль		Залік у формі тестування	20
Сума			**100**

Шкала оцінювання: національна та ECTS

Сума балів за результатом підсумкового контролю	Оцінка ECTS	Оцінка за національною шкалою
90 – 100	A	Відмінно
82 – 89	B	Дуже добре
74 – 81	C	Добре
64 – 73	D	Посередньо
60 – 63	E	Достатньо
35 – 59	FX	Незадовільно з можливістю повторного складання
0 – 34	F	Незадовільно з обов’язковим повторним вивченням дисципліни

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп’ютер (настільний або ноутбук).

Системне програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційну систему.

Прикладне програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає некомерційні програми стеганографії, що знаходяться у вільному доступі: OpenStego; SilentEye; OpenPuff; DarkCryptTC. Текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному вигляді).

10. Рекомендовані джерела інформації

Основні:

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К.: "МК-Пресс", 2006. – 288 с.
2. Оков И. Н. Электронные водяные знаки как средство аутентификации передаваемых сообщений / И. Н. Оков, Р. М. Ковалев // Защита информации. Конфидент. – 2001. – № 3. – С. 80–85.
3. Основи комп'ютерної стеганографії: навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця: ВДТУ, 2003. – 143 с.
4. Стеганографія: навч. посібн. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: Вид. ХНЕУ, 2011. – 232 с.

Допоміжні:

5. Термінологічний довідник з питань технічного захисту інформації / В. О. Хорошко, І. М. Огаркова, Д. В. Чирков та ін. ; за ред. проф. Хорошка В. О. – 3-тє вид., доп. і перероб. – К.: ТОВ "ПоліграфКонсалтинг", 2003. – 286 с.
6. Стасєв Ю. В. Основи теорії побудови сигналів / Ю. В. Стасєв. – Х.: ХВУ, 1999. – 87 с.

Інформаційні ресурси мережі Інтернет:

1. https://www.openstego.com/
2. https://achorein.github.io/silenteye/
3. https://embeddedsw.net/OpenPuff_Steganography_Home.html
4. https://www.ghisler.ch/wiki/index.php/DarkCryptTC

Доцент кафедри КТІБ,
к.т.н., доцент _____ С.С. Козирєв