МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«___»_____ 20___р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«___»_____ 20___р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«___»_____ 20___р.

РОБОЧА ПРОГРАМА

з дисципліни

«СТЕГАНОГРАФІЧНІ МЕТОДИ»

ступінь вищої освіти – **магістр**

галузь знань – **12 Інформаційні технології**

спеціальність – **125 Кібербезпека та захист інформації**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. заняття (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	1	2	30	15	5	4	96	150	2
Заочна	1	2	8	4	-	-	138	150	2

Тернопіль - 2023

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 3 від 28 . 09 . 2023 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 2 від 02 . 10 . 2023 р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Василь ЯЦКІВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій

_____ Ігор ЯКИМЕНКО
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи

_____ Віктор ОСТРОВЕРХОВ
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового інституту новітніх освітніх технологій
_____Святослав ПИТЕЛЬ
«___» _____ 20___р.

РОБОЧА ПРОГРАМА

з дисципліни

«СТЕГАНОГРАФІЧНІ МЕТОДИ»

ступінь вищої освіти – **магістр**

галузь знань – **12 Інформаційні технології**

спеціальність – **125 Кібербезпека та захист інформації**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. заняття (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	1	2	30	15	5	8	92	150	2
Заочна	1	2	8	4	-	-	138	150	2

Тернопіль - 2023

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол №__ від ___.___. _____ р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №__ від ___.___. _____ р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Стеганографічні методи”

Дисципліна “Стеганографічні методи”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 3	спеціальність – 125 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 2* *Заочна – 2*
Кількість змістових модулів – 3	ступінь вищої освіти – магістр	Лекції (год): *Денна – 30* *Заочна - 8* Практичні заняття (год): *Денна – 15* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 100* (в т.ч. тренінг, КПІЗ – 8 год.) *Заочна - 138* Індивідуальна робота (год): *Денна – 5*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета й завдання вивчення дисципліни “Стеганографічні методи”

2.1. Мета завдання дисципліни

Метою вивчення дисципліни 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.

Вивчення курсу “Стеганографічні методи» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи програмування», «Кібернетична безпека», «Системи та технології кібербезпеки», «Архітектура комп’ютерних систем», «Математичний аналіз», «Фізика»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є систематизація інформації щодо розроблення, впровадження та експлуатації систем захисту інформації на об’єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- основні положення та терміни стеганографії;

− нормативно-методичну базу в галузі стеганографії;

− етапи організації та застосування стеганографії;
− підходи у визначені об’єктів захисту;
− типові джерела загроз стеганосистеми;
вміти:
− створювати стеганографічну модель системи захисту;
− складати окремі моделі стеганоконтейнерів.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Стеганографічні методи». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Стеганографічні методи» та формуванні у студентів цілісної системи теоретичних знань з курсу «Стеганографічні методи».

Завдання проведення практичних занять

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення практичних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

3. Програма навчальної дисципліни “Стеганографічні методи"

Змістовий модуль 1. Вступ до стеганографії.

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.

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.

Тема 3. Основні напрямки практичного використання стеганографічніх методів захисту інформації.

Класифікація стеганографічніх 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.

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.

Змістовий модуль 2. Приховування даних в зображеннях та відео

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.

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.

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.

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.

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.

Змістовий модуль 3. **Приховування даних в аудіосигналах та текстових файлах. Атаки на стегосистеми та протидія їм**

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.

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.

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.

Тема 13. Методи текстової стеганографії.

Аналіз реалізації методів. Методи текстової стеганографії. Порівняння методів текстової стеганографії.

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.

Тема 15. Практична оцінка стійкості стеганосистем.

Теоретико-складнісний підхід до оцінки стійкості стеганосистем. Імітостійкість систем передачі прихованих повідомлень. Класифікація атак зловмисника. Досконала стеганосистема.

4. Структура залікового кредиту дисципліни "Стеганографічні методи"

4.1 Структура залікового кредиту дисципліни "Стеганографічні методи" для ДФН

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Тренінг, КПІЗ	Контрольні заходи
Змістовий модуль 1. **Вступ до стеганографії.**						
Тема 1. Основні поняття та положення стеганографії.	2	1	6	-	2	Поточне опитування
Тема 2. Математична модель стеганосистеми. Практичні аспекти вбудування даних.	2	1	6	-		Поточне опитування
Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації.	2	1	7	-		Поточне опитування
Тема 4. Особливості зорової системи людини.	2	1	6	1		Поточне опитування
Змістовий модуль 2. ***Приховування даних в зображеннях та відео***						

Тема 5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).	2	1	6	-	3	Поточне опитування
Тема 6. Приховування даних у просторовій області зображень та відео.	2	1	7	-		Поточне опитування
Тема 7. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки	2	1	6	-		Поточне опитування
Тема 8. Приховування даних у просторової області зображень та відео методом блокового приховування, заміни палітри та квантування зображення	2	1	6	-		Поточне опитування
Тема 9. Приховування даних у частотній області зображень та відео.	2	1	7	2		Поточне опитування
Змістовий модуль 3. **Приховування даних в аудіосигналах та текстових файлах. Атаки на стегосистеми та протидія їм.**						
Тема 10. Особливості слухової системи людини (ССЛ).	2	1	6	-	3	Поточне опитування
Тема 11. Приховування даних у просторовій множині аудіосигналу.	2	1	6	-		Поточне опитування
Тема 12. Приховування даних в аудіосигналах за допомогою методів розширення спектра.	2	1	7	-		Поточне опитування
Тема 13. Методи текстової стеганографії.	2	1	6	-		Поточне опитування
Тема 14. Атаки на системи прихованої передачі повідомлень та методи протидії їм.	2	1	7	-		Поточне опитування
Тема 15. Практична оцінка стійкості стеганосистем.	2	1	7	2		Поточне опитування
Разом	30	15	92	5	8	

4.2 Структура залікового кредиту дисципліни “Стеганографічні методи” для ЗФН

	Кількість годин		
	Лекції	Практичні заняття	Самостійна робота
Змістовий модуль 1. **Вступ до стеганографії.**			
Тема 1. Основні поняття та положення стеганографії.	0,5	-	9
Тема 2. Математична модель стеганосистеми. Практичні аспекти вбудування даних.	0,5	-	9
Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації.	0,5	-	10
Тема 4. Особливості зорової системи людини.	0,5	-	9
Змістовий модуль 2. ***Приховування даних в зображеннях та відео***			
Тема 5. Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG).	0,5	-	10
Тема 6. Приховування даних у просторовій області зображень та відео.	0,5	-	10

Тема 7. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки	0,5	1	9
Тема 8. Приховування даних у просторової області зображень та відео методом блокового приховування, заміни палітри та квантування зображення	0,5	-	10
Тема 9. Приховування даних у частотній області зображень та відео.	0,5	-	10
Змістовий модуль 3. **Приховування даних в аудіосигналах та текстових файлах. Атаки на стегосистеми та протидія їм**			
Тема 10. Особливості слухової системи людини (ССЛ).	0,5	-	9
Тема 11. Приховування даних у просторовій множині аудіосигналу.	0,5	1	10
Тема 12. Приховування даних в аудіосигналах за допомогою методів розширення спектра.	1	-	10
Тема 13. Методи текстової стеганографії.	0,5	1	9
Тема 14. Атаки на системи прихованої передачі повідомлень та методи протидії їм.	0,5	-	10
Тема 15. Практична оцінка стійкості стеганосистем.	0,5	1	10
Разом	8	4	138

5. Тематика практичних занять.
5.1 Тематика практичних занять для ДФН.

Практичне заняття №1

Тема: Основні поняття та положення стеганографії. Математична модель стеганосистеми. Практичні аспекти вбудування даних.

Мета: Вивчення та дослідження основних понять та положень стеганографії, математичної моделі стеганосистеми.

Питання для обговорення:

1. Структура та зміст дисципліни, її зв’язок з іншими дисциплінами учбового плану.
2. Цифрова стеганографія. Предмет, термінологія, галузь використання.
3. Структура та зміст дисципліни, зв’язок з іншими дисциплінами учбового плану, призначення стеганографічної системи, основна термінологія та визначення, потенціальні області використання стеганографії.
4. Загальна структурна схема стеганосистеми як системи зв'язку.
5. Математична модель стеганосистеми.
6. Стеганографічні системи з відкритим та закритими ключами.
7. Стеганографічні протоколи.
8. Призначення стеганодектору.
9. Практичні аспекти вбудування даних

Література: 1-18.

Практичне заняття № 2

Тема: Основні напрямки практичного використання стеганографічніх методів захисту інформації. Особливості зорової системи людини

Мета: Вивчення та дослідження основних напрямків практичного використання стеганографічніх методів захисту інформації та особливостей зорової системи людини.

Питання для обговорення:

1. Класифікація стеганографічніх систем та стегоконтейнерів.
2. Основні напрями стегонографії.
3. Вбудовування інформації з метою її прихованої передачі; вбудовування цифрових водяних знаків, вбудовування ідентифікаційних номерів, вбудовування заголовків.
4. Загальна класифікацію контейнерів..

5. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.
6. Аналіз механізмів зорового сприйняття людини.
7. Низькорівневі властивості, що впливають на помітність стороннього шуму в зображенні.
8. Високорівневі властивості зорової системи людини.

Література: 1-18.

Практичне заняття №3

Тема: Цифрові формати нерухомих зображень (формати BMP, GIF, TIFF, JPEG). Приховування даних у просторовій області зображень та відео.

Мета: Вивчення та дослідження цифрових форматів нерухомих зображень (формати BMP, GIF, TIFF, JPEG) та методів приховування даних у просторовій області зображень та відео.

Питання для обговорення:

1. Особливості комп'ютерної обробки зображень.
2. Структура форматів BMP, GIF, TIFF, JPEG.
3. Структура файлів растрового зображення.
4. Дескриптор екрану у форматі GIF, термінатор GIF, розширений блок GIF.
5. Метод приховування в найменш значущому біті даних.
6. Приховування даних у просторовій області зображень.
7. Приховування даних у просторовій області відео.

Література: 1-18.

Практичне заняття №4

Тема: Приховування даних у просторовій області зображень та відео методами псевдовипадкової перестановки, **блокового приховування, заміни палітри та квантування зображення**

Мета: Вивчення та дослідження приховування даних у просторовій області зображень та відео методами псевдовипадкової перестановки, блокового приховування, заміни палітри та квантування зображення.

Питання для обговорення:

1. Метод псевдовипадкової перестановки для приховування даних у просторовій області зображень та відео.
2. Приховування даних у просторовій області зображень методом псевдовипадкової перестановки.
3. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.
4. Метод блокового приховування.
5. Метод заміни палітри.
6. Метод квантування зображення.

Література: 1-18.

Практичне заняття №5

Тема: Приховування даних у частотній області зображень та відео. Особливості слухової системи людини (ССЛ).

Мета: Вивчення та дослідження методів приховування даних у частотній області зображень та відео, а також особливостей слухової системи людини (ССЛ).

Питання для обговорення:

1. Метод Коха та Жао.
2. Приховування даних у частотній області зображень та відео.
3. Приховування даних у частотній області методом Коха та Жао.
4. Основні властивості ССЛ, що використовуються при приховуванні даних в аудіо сигналах.
5. Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis).
6. Особливості комп'ютерної обробки аудіо сигналів.
7. Класи аудиосигналів.
8. Опис форматів WAV, WMA, MP3, AAC, OGG Vorbis..

Література: 1-18.

Практичне заняття № 6

Тема: Приховування даних у просторовій множині аудіосигналу. Приховування даних в аудіосигналах за допомогою методів розширення спектра.

Мета: Вивчення та дослідження методів приховування даних у просторовій множині аудіосигналу, а також в аудіосигналах за допомогою методів розширення спектра.

Питання для обговорення:

1. Приховування даних у частотній множині аудіо сигналу.
2. Приховування в найменш значущому біті даних та за допомогою ехосигналів.Фазове кодування.
3. Призначеня стегакодера й стеганодекодера.
4. Вплив на ЦВДЗ застосування до аудіосигналу ковзного фільтра середніх частот.

Література: 1-18.

Практичне заняття № 7

Тема: Методи текстової стеганографії. Атаки на системи прихованої передачі повідомлень та методи протидії їм.

Мета: Вивчення та дослідження методів текстової стеганографії, атак на системи прихованої передачі повідомлень та методи протидії їм.

Питання для обговорення:

1. Аналіз реалізації методів.
2. Методи текстової стеганографії.
3. Порівняння методів текстової стеганографії.
4. Атаки на системи цифрових водяних знаків.
5. Класифікація атак на стеганосистеми цифрових відеознаків.
6. Атаки на стеганосистеми цифрових відео знаків.
7. Методи протидії атакам на системи цифрових водяних знаків.
8. Статистичний стегоаналіз та протидії.
9. Методи протідії атакам на системи цифрових водяних знаків.

Література: 1-18.

Практичне заняття №8

Тема: Практична оцінка стійкості стеганосистем.

Мета: Вивчення та дослідження практичної оцінки стійкості стеганосистем.

Питання для обговорення:

1. Теоретико-складнісний підхід до оцінки стійкості стеганосистем.
2. Імітостійкість систем передачі прихованих повідомлень.
3. Класифікація атак зловмисника.
4. Досконала стеганосистема.

Література: 1-18.

5.1 Тематика практичних занять для ЗФН.

Практичне заняття №1

Тема: Приховування даних у просторовій області зображень та відео методами псевдовипадкової перестановки, **блокового приховування, заміни палітри та квантування зображення**

Мета: Вивчення та дослідження приховування даних у просторовій області зображень та відео методами псевдовипадкової перестановки, блокового приховування, заміни палітри та квантування зображення.

Питання для обговорення:

1. Метод псевдовипадкової перестановки для приховування даних у просторовій області зображень та відео.
2. Приховування даних у просторовій області зображень методом псевдовипадкової перестановки.
3. Приховування даних у просторовій області зображень та відео методом псевдовипадкової перестановки.

4. Метод блокового приховування.
5. Метод заміни палітри.
6. Метод квантування зображення.

Література: 1-18.

Практичне заняття № 2

Тема: Приховування даних у просторовій множині аудіосигналу. Приховування даних в аудіосигналах за допомогою методів розширення спектра.

Мета: Вивчення та дослідження методів приховування даних у просторовій множині аудіосигналу, а також в аудіосигналах за допомогою методів розширення спектра.

Питання для обговорення:

1. Приховування даних у частотній множині аудіо сигналу.
2. Приховування в найменш значущому біті даних та за допомогою ехосигналів.Фазове кодування.
3. Призначеня стегакодера й стеганодекодера.
4. Вплив на ЦВДЗ застосування до аудіосигналу ковзного фільтра середніх частот.

Література: 1-18.

Практичне заняття № 3

Тема: Методи текстової стеганографії. Атаки на системи прихованої передачі повідомлень та методи протидії їм.

Мета: Вивчення та дослідження методів текстової стеганографії, атак на системи прихованої передачі повідомлень та методи протидії їм.

Питання для обговорення:

1. Аналіз реалізації методів.
2. Методи текстової стеганографії.
3. Порівняння методів текстової стеганографії.
4. Атаки на системи цифрових водяних знаків.
5. Класифікація атак на стеганосистеми цифрових відеознаків.
6. Атаки на стеганосистеми цифрових відео знаків.
7. Методи протидії атакам на системи цифрових водяних знаків.
8. Статистичний стегоаналіз та протидії.
9. Методи протідії атакам на системи цифрових водяних знаків.

Література: 1-18.

Практичне заняття №4

Тема: Практична оцінка стійкості стеганосистем.

Мета: Вивчення та дослідження практичної оцінки стійкості стеганосистем.

Питання для обговорення:

1. Теоретико-складнісний підхід до оцінки стійкості стеганосистем.
2. Імітостійкість систем передачі прихованих повідомлень.
3. Класифікація атак зловмисника.
4. Досконала стеганосистема.

Література: 1-18.

6. Комплексне практичне індивідуальне завдання (КПІЗ).

Індивідуальне завдання з курсу “Стеганографічні методи” виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є оволодіння навиками використання стеганографічних методів при вирішенні конкретних задач кібербезпеки. Студенти повинні дослідити та застосувати відповідні методи та алгоритми за одним із варіантів:

1. Загальна схема стеганографічної системи, призначеної для передачі даних.
2. Схема стеганографічної системи при наявності пасивного противника.
3. Основні відмінності схем при наявності пасивного і активного противника.
4. Поняття контейнера-носія.
5. Інформаційний підхід до визначення інформації і до оцінки стійкості систем.
6. Поняття ентропії, відносної й умовної ентропії. Теорема Неймана- Пірсона.
7. Правило прийняття рішення як двійкове відображення.

8. Поняття помилок першого і другого роду.
9. Необхідна умова стійкості.
10. Поняття абсолютно-стійкої системи.
11. Елементи теорії ігор, що застосовуються в стеганографії.
12. Гра двох учасників з нульовою сумою.
13. Ігри з кінцевою множиною стратегій.
14. Ігри з оптимальними стратегіями.
15. Матричні гри.
16. Поняття функції виграшу і чистої ціни гри.
17. Поняття протоколу, оракула, детермінованого оракула, запит і відповідь оракула.
18. Абстрактна обчислювальна машина з оракулом Алана Тьюринга, її схема.
19. Нескінченно мала функція і конкатенація двох строкових функцій.
20. Поріг приховування і поріг виявлення. Принцип виявлення прихованої інформації.
21. Універсальний стеганоаналітичний алгоритм.
22. Пропускна здатність каналів передачі інформації.
23. Застосування перетворення обертання в стеганосистемах для контролю спотворень.
24. Методи контролю спотворень, що застосовуються в сучасних комп'ютерних системах.
25. Алгоритми вбудовування та вилучення цифрових водяних знаків.
26. Призначення цифрових водяних знаків.
27. Захист за допомогою цифрових водяних знаків авторських прав на електронні твори.
28. Підвищення рівня захищеності за допомогою цифрового підпису.
29. Позитивна судова практика з використанням методів стеганографії.
30. Захист особистої, комерційної та державної інформації методами стеганографії.
31. Стегоалгоритми, які використовують фрактальне перетворення.

Виконання КПІЗ є одним із обов’язкових складових модулів залікового кредиту.

7. Самостійна робота та дуальна освіта

№ п/п	Тематика
1	Застосування контейнерів «не комп'ютерної» природи в методах стеганографії.
2	Молекула ДНК як стеганографічна модель приховування даних.
3	Алгоритм генерації фрагмента молекули ДНК.
4	Приклади успішного механізму поширення ДНК коду в стеганографії.
5	Метод приховування у вихідних даних зображення.
6	Метод приховування з використанням таблиць квантування.
7	Метод використання неправдивих таблиць квантування.
8	Метод приховування в спектрі зображення після квантування.
9	Дописування даних в кінець JPEG файлу.
10	Метод приховування інформації в графічних зображеннях з палітрою кольорів.
11	Метод приховування з використанням молодших біт даних зображення.
12	Метод приховування, заснований на наявності однакових елементів палітри.
13	Абсолютний поріг чутності.
14	Метод частотного маскування: маскування вперед і маскування назад.
15	Обчислення спектру потужності аудіосигналу.
16	Принцип видалення маскованих компонент.
17	Методи приховування інформації в найменших значущих бітах.
18	Впровадження переданого повідомлення в фазову частина аудіосигналу.
19	Метод формування сегмента з початковою фазою.
20	Метод приховування на основі шумоподібних сигналів.

21	Механізм зворотного перетворення.
22	Застосування методу зворотного перетворення на основі шумоподібних сигналів.

8. Організація та проведення тренінгу з дисципліни “Стеганографічні методи”

№п/п	Вид роботи	Порядок проведення тренінгу
1	Огляд сучасних комп’ютерних систем для реалізації цифрової стеганографії	− розгляд сучасних засобів проектування методів стеганографії; − вивчення можливостей проектування стеганографічних методів в різних програмних середовищах.
2	Розгляд процесу проектування системи для приховування цифрової інформації	− постановка задачі; − опис технічного завдання; − проектування схеми для приховування цифрової інформації
3	Розв’язування наскрізних задач, що охоплюють усі розділи дисципліни «Стеганографічні методи»	− опис наскрізної задачі; − розбиття задачі на окремі підзадачі; − об’єднання розв’язаних підзадач в єдине ціле з метою вирішення усієї задачі.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Застосування методів, засобів та алгоритмів для реалізації та дослідження стеганографічного приховування цифрової інформації.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Стеганографічні методи” використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– ректорська контрольна робота;
– комплексне практичне індивідуальне заняття (КПІЗ).

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни “Стеганографічні методи” визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту.

Семестр 2 – залік %

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ, враховуючи поточне опитування)
30%	40%	30%

1. Усне опитування на заняттях: 4 теми 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 теми по 6 балів – max 24 бали. 2. Письмова робота – max 52 балів. 3. Практичне завдання: 4 практичних завдання по 4 бали – max 24 бали.	1. Підготовка КПІЗ – max 35 балів. 2. Захист КПІЗ – max 35 балів. 3. Виконання завдань на тренінгах – max 30 балів

Шкала оцінювання:

За шкалою ТНЕУ	**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)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1-15
2	Методичні вказівки до виконання практичних робіт (електронний варіант)	1–15
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-15
4	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, Nod32, FoxitReader, AdobeReader, WinRAR, WinZip, MathCAD, MatLab, DjVu Viewer, Total Commander, C#, C++, MASM32, Java Server Pages, Servlets, EJB, Java Server Faces, JavaFX, BC3.0, .NET Framework, PHP, Visual C++, Symbian C++, ARIS, MS Project, IBM Rational, GPSS World, Visual Web Developer 2016 Express, SWI Prolog, Microsoft Project, Spider Project, Primavera Project Planner, SQL Server 2015 Enterprise, Visio Professional 2016, Project Professional 2016, Expression Studio 2, Visual Studio 2015, Visual Studio™ 2015, Visual Studio Team System 2015	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

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.