Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

**"ЗАТВЕРДЖУЮ"**

Проректор з науково-педагогічної роботи

_____ Антон ПАНТЕЛЕЙМОНОВ

"___" _____ 2020 р.

# Робоча програма навчальної дисципліни

## Стеганографія

рівень вищої освіти __перший (бакалаврський)__

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

спеціалізація

вид дисципліни ___обов'язкова__

факультет комп'ютерних наук

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)

"31" серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ: Кузнецов Олександр Олександрович, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій
_____ Рассомахін С.Г.

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Кібербезпека
назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Рассомахін Сергій Геннадійович

_____ Рассомахін С.Г.
(підпис) (прізвище та ініціали)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

_____ Бердніков А. Г.

## ВСТУП

Програма навчальної дисципліни "Стеганографія" складена відповідно до освітньої програми підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека», освітня програма «Кібербезпека»

## 1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є формування у студентів певних професійних компетенцій, знань та вмінь у галузі цифрової стеганографії, методів та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

1.2. Основні завдання вивчення дисципліни

Основними завданнями з вивчення навчальної дисципліни є отримання студентами необхідних базових знань з теоретичних основ побудови стеганографічних систем захисту інформації, моделей та методів стеганографічного перетворення та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

Предметом вивчення навчальної дисципліни є процеси, механізми, методи, системи та засоби стеганографічного захисту інформації в інформаційних системах (ІС) та інформаційно-телекомунікаційних системах (ІТС).

Програма навчальної дисципліни складається з таких розділів:

1. Вступ до цифрової стеганографії;
2. Стеганографічні методи приховування даних в контейнерах-зображеннях;
3. Стеганографічні методи приховування даних в аудіофайлах
4. Лінгвістична та технічна стеганографія.

1.3. Кількість кредитів 6

1.4. Загальна кількість годин 180

| 1.5. Характеристика навчальної дисципліни | |
|---|---|
| Нормативна | |
| Денна форма навчання | Заочна (дистанційна) форма навчання |
| Рік підготовки | |
| 4-й | -й |
| Семестр | |
| 7-й | -й |
| Лекції | |
| 32 год. | год. |
| Практичні, семінарські заняття | |
| 32 год. | год. |
| Лабораторні заняття | |
| 0год. | год. |
| Самостійна робота | |
| 116 год. | год. |
| Індивідуальні завдання | |
| розрахункова робота 10 год. | |

1.6. Заплановані результати навчання

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких результатів навчання:

ЗНАТИ:

- визначення, класифікацію та основні властивості стеганографічних систем;
- математичні моделі стеганографічних перетворень та абстрактне визначення стеганографічних систем;
- методи та обчислювальні алгоритми стеганографічного захисту інформації при вбудовуванні даних в графічні зображення, аудіосигнали, текстові документи;
- визначення, класифікацію та основні атаки на стеганосистеми та методи протидії.

ВМІТИ:

- практично реалізовувати обчислювальні алгоритми стегнаографічного перетворення, зокрема, алгоритми приховування та вилучення даних із графічних зображень, аудіосигналів, текстових документів;
- оцінювати пропускну спроможність каналів передавання схованої інформації, рівень внесених похибок в контейнери-оригінали та ймовірнісні властивості стеганографічних систем (ймовірність помилкового вилучення інформаційних повідомлень, тощо);
- оцінювати стійкість стенографічних систем до різних атак на стеганографічні системи.

## 2. Тематичний план навчальної дисципліни

**Розділ 1. Вступ до стеганографії**

Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання

1. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану
2. Цифрова стеганографія. Предмет, термінологія, галузь використання

Тема 2. Математична модель та структурна схема стеганосистеми

1. Структурна схема та формальне математичне визначення криптографічної (секретної) системи. Ймовірності показники та умова теоретично недешифрованої секретної системи.
2. Математична модель та структурна схема стеганографічної системи. Ймовірності показники та умова теоретично недетектованої стеганографічної системи.

Тема 3. Атаки на стегосистеми

1. Класифікація атак на секретні та стеганографічні системи
2. Атаки на системи прихованої передачі повідомлень та на системи цифрових водяних знаків (ЦВЗ).

**Розділ 2. Стеганографічні методи приховування даних в контейнерах-зображеннях**

Тема 4. Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень

1. Особливості ЗСЛ, які використовуються в стеганографії
2. Основні формати цифрових зображень. Растрові дані. Формат зображень Bitmap Picture (bmp)

Тема 5. Приховування даних у просторовій області нерухомих зображень

1. Методи приховування на основі модифікації найменш значущого біту даних (НЗБ)
2. Блокове приховування, метод квантування, метод «хреста»

Тема 6. Приховування даних із використанням технології прямого розширення спектру

1. Складні дискретні сигнали та технологія прямого розширення спектру
2. Приховування даних із застосуванням складних дискретних сигналів

Тема 7. Приховування даних у частотній області нерухомих зображень
1. Основні етапи алгоритму стиску зображень JPEG. Дискретно-косинусне перетворення
2. Метод Коха-Жао та його модифікації
3. Метод Фридріх

**Розділ 3. Стеганографічні методи приховування даних в аудіофайлах**

Тема 8. Особливості слухової системи людини (ССЛ), які використовуються в стеганографії. Основні формати аудіофайлів
1. Особливості ССЛ та їх застосування в стеганографії
2. Основні формати аудіофайлів. Формат аудіофайлів Waveform Audio Format (wav)

Тема 9. Приховування даних у просторовій області аудіо сигналів
1. Методи приховування на основі модифікації НЗБ
2. Метод кодування луна-сигналів

Тема 10. Приховування даних у частотній області аудіо сигналів
1. Основні властивості дискретного перетворення Фурье. Амплітудний, частотний та фазові спектри аудіосигналів
2. Метод фазового кодування

**Розділ 4. Лінгвістична та технічна стеганографія**

Тема 11. Приховування даних у текстових документах
1. Лінгвістичні властивості, які використовуються в стеганографії
2. Методи приховування даних на основі довільних інтервалів
3. Синтаксичні методи приховування даних
4. Семантичні методи приховування даних

Тема 12. Стеганографічні методи із застосуванням технологій 3D друку
1. Класифікація та основні властивості відомих технологій 3D друку
2. Штучна надмірність 3D моделей, яка використовується в стеганографії
3. Методи приховування даних із застосуванням технологій 3D друку

Тема 13. Приховування даних у кластерних файлових системах
1. Особливості побудови файлових систем зберігання даних
2. Штучна надмірність кластерних файлових систем, яка використовується в стеганографії
3. Методи приховування даних у кластерних файлових системах

Тема 14. Мережева стеганографія
1. Методи модифікації вмісту інформаційних пакетів
2. Методи модифікації полів заголовків телекомунікаційних протоколів
3. Гібридні методи

## 3. Структура навчальної дисципліни

| Назви розділів і тем | Кількість годин | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | | | заочна форма | | | | | |
| | усього | у тому числі | | | | | усього | у тому числі | | | | |
| | | л | п | лаб. | інд. | с. р. | | л | п | лаб. | інд. | с. р. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| **Розділ 1. Вступ до стеганографії** | | | | | | | | | | | | |
| Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання | 8 | 2 | 2 | | | 4 | | | | | | |
| Тема 2. Математична модель та структурна схема стеганосистеми. Критерії та показники ефективності стеганосистем | 12 | 2 | 2 | | | 8 | | | | | | |
| Тема 3. Атаки на стегосистеми | 12 | 2 | 2 | | | 8 | | | | | | |
| Разом за розділом 1 | 32 | 6 | 6 | | | 20 | | | | | | |
| **Розділ 2. Стеганографічні методи приховування даних в контейнерах-зображеннях** | | | | | | | | | | | | |
| Тема 4. Особливості ЗСЛ, які використовуються в стеганографії. Основні формати цифрових зображень | 14 | 2 | 2 | | | 10 | | | | | | |
| Тема 5. Приховування даних у просторовій області нерухомих зображень | 18 | 2 | 4 | | | 10 | | | | | | |
| Тема 6. Приховування даних із використанням технології прямого розширення спектру | 28 | 6 | 6 | | | 16 | | | | | | |
| Тема 7. Приховування даних у частотній області нерухомих зображень | 20 | 4 | 6 | | | 10 | | | | | | |
| Разом за розділом 2 | 78 | 14 | 18 | | | 46 | | | | | | |
| **Розділ 3. Стеганографічні методи приховування даних в аудіофайлах** | | | | | | | | | | | | |
| Тема 8. Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів | 8 | 2 | | | | 6 | | | | | | |
| Тема 9. Приховування даних у просторовій області аудіо сигналів | 11 | 2 | 2 | | | 7 | | | | | | |
| Тема 10. Приховування даних у частотній області аудіо сигналів | 11 | 2 | 2 | | | 7 | | | | | | |
| Разом за розділом 3 | 30 | 6 | 4 | | | 20 | | | | | | |
| **Розділ 4. Лінгвістична та технічна стеганографія** | | | | | | | | | | | | |
| Тема 11. Приховування даних у текстових документах | 5 | 1 | | | | 4 | | | | | | |
| Тема 12. Стеганографічні методи із застосуванням технологій 3D друку | 5 | 1 | | | | 4 | | | | | | |

| Назви розділів і тем | Кількість годин | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | | | заочна форма | | | | | |
| | усього | у тому числі | | | | | усього | у тому числі | | | | |
| | | л | п | лаб. | інд. | с. р. | | л | п | лаб. | інд. | с. р. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Тема 13. Приховування даних у кластерних файлових системах | 12 | 2 | 2 | | | 6 | | | | | | |
| Тема 14. Мережева стеганографія | 8 | 2 | 2 | | | 6 | | | | | | |
| Розрахункова робота | 10 | | | | | 10 | | | | | | |
| Разом за розділом 4 | 30 | 6 | 4 | | | 30 | | | | | | |
| ***Усього годин*** | 180 | 32 | 32 | | | 116 | | | | | | |

## 4. Теми семінарських (практичних, лабораторних) занять

| № з/п | Назва теми (форма поточного контролю) | Кількість годин |
|---|---|---|
| 1 | Цифрова стеганографія. Предмет, термінологія, галузь використання | 2 |
| 2 | Математична модель та структурна схема стеганосистеми. Атаки на стеганосистеми | 2 |
| 3 | Атаки на стегосистеми | 2 |
| 4 | Особливості ЗСЛ, які використовуються в стеганографії. Основні формати цифрових зображень | 2 |
| 5 | Приховування даних у просторовій області нерухомих зображень. Методи приховування на основі модифікації НЗБ | 2 |
| 6 | Приховування даних у просторовій області нерухомих зображень. Блокове приховування, метод квантування, метод «хреста» | 2 |
| 7 | Приховування даних із застосуванням складних дискретних сигналів та технології прямого розширення спектру | 6 |
| 8 | Приховування даних у частотній області нерухомих зображень. Метод Коха-Жао та його модифікації | 6 |
| 9 | Стеганографічні методи приховування даних в аудіофайлах. | 2 |
| 10 | Приховування даних у частотній області аудіо сигналів | 2 |
| 11 | Приховування даних у кластерних файлових системах | 2 |
| 12 | Мережева стеганографія | 2 |
| | Разом | 32 |

## 5. Завдання для самостійної роботи

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Підготовка до ПЗ: Цифрова стеганографія. Предмет, термінологія, галузь використання. Повторення лекційного матеріалу, розв’язання практичних завдань. | 4 |
| 2 | Підготовка до ПЗ :Математична модель та структурна схема стеганосистеми. Повторення лекційного матеріалу, розв’язання практичних завдань. | 8 |
| 3 | Підготовка до ПЗ :Атаки на стегосистеми. Повторення лекційного матеріалу, розв’язання практичних завдань. | 8 |
| 4 | Підготовка до ПЗ :Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень. Повторення лекційного матеріалу, розв’язання практичних завдань. | 10 |
| 5 | Підготовка до ПЗ :Приховування даних у просторовій області нерухомих зображень. Повторення лекційного матеріалу, розв’язання практичних завдань. | 10 |
| 6 | Підготовка до ПЗ, читання додаткової літератури :Приховування даних із використанням технології прямого розширення спектру. Повторення лекційного матеріалу, розв’язання практичних завдань. | 16 |

| | | |
|---|---|---|
| 7 | Підготовка до ПЗ :Приховування даних у частотній області нерухомих зображень. Повторення лекційного матеріалу, розв'язання практичних завдань. | 10 |
| 8 | Підготовка до ПЗ :Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів. Повторення лекційного матеріалу, розв'язання практичних завдань. | 6 |
| 9 | Підготовка до ПЗ :Приховування даних у просторовій області аудіо сигналів. Повторення лекційного матеріалу, розв'язання практичних завдань. | 7 |
| 10 | Підготовка до ПЗ :Приховування даних у частотній області аудіо сигналів. Повторення лекційного матеріалу, розв'язання практичних завдань. | 7 |
| 11 | Підготовка до ПЗ :Приховування даних у текстових документах. Повторення лекційного матеріалу, розв'язання практичних завдань. | 4 |
| 12 | Підготовка до ПЗ :Стеганографічні методи із застосуванням технологій 3D друку. Повторення лекційного матеріалу, розв'язання практичних завдань. | 4 |
| 13 | Підготовка до ПЗ :Приховування даних у кластерних файлових системах. Повторення лекційного матеріалу, розв'язання практичних завдань. | 6 |
| 14 | Підготовка до ПЗ :Мережева стеганографія. Повторення лекційного матеріалу, розв'язання практичних завдань. | 6 |
| 15 | Розрахункова робота. Розв'язання практичних завдань. | 10 |
| | Разом | 116 |

## 6. Індивідуальні завдання

Індивідуальні завдання студентів пов'язані з вивченням окремих, в тому іноземних джерел, за тематикою дисципліни, проведенням аналізу існуючих та перспективних засобів захисту інформації, дослідженням рівнів стійкості, розробленням імітаційних моделей та дослідженням ефективності в тому числі із застосуванням принципу масштабування. Теми індивідуальних завдань, як правило, пов'язуються з науковими та науково - методичними дослідженнями, які веде кафедра та інші підрозділи університету чи інші підприємства чи заклади тощо, фірми.

Основними формами реалізації результатів виконання індивідуального завдання є:

- доповідь чи виступ на семінарських чи практичних заняттях;
- доповідь на тематичних науково - практичних конференціях з опублікуванням тез чи доповідей;
- підготовка та опублікування наукових та науково - практичних статей;
- підготовка та подання результатів досліджень для використання в НДР та ДКР кафедри;
- участь в розробці науково - методичних та навчальних матеріалів;
- підготовка патентів на винаходи та корисні моделі;
- розробка та опис програмних продуктів та моделей тощо.

Індивідуальні завдання студентів - виконання розрахункових робот.

Бали за виконання розрахункових робот складаються з розрахунку: 2 бал за акуратність оформлення розрахункової робот, 8 балів за результат без помилок, з незначними помилками 7 балів, з певною кількістю помилок 5 балів, грубі помилки, нерозуміння суті роботи 0 балів . Максимальна кількість балів за курсову роботу складає 10 балів.

## 7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

## 8. Методи контролю

Вивчення дисципліни передбачає проведення оперативного та поточного контролю в межах загального обсягу годин, а також проведення підсумкового семестрового контролю.

**Для оперативного контролю** степені засвоєння матеріалу протягом семестру застосовуються наступні заходи:

- контроль присутності студентів (пропуск лекції без поважної причини – "мінус" чотири бали);
- контроль і оцінка виконання індивідуального завдання – перевірка роботи комп'ютерної програми та усна співбесіда (оцінюється індивідуально викладачем);
- контроль знання відповідей на контрольні питання (оцінюється індивідуально викладачем).

**Поточний контроль**.

Поточний контроль засвоювання теоретичного матеріалу під час проведення лекцій проводиться у формі усного опитування.

Для перевірки рівня підготовленості студента до виконання конкретної лабораторної роботи та під час проведення практичних занять здійснюється поточний контроль, який проводиться у формі письмових контрольних робіт (**КР**) в межах загального обсягу годин. Для перевірки результатів виконання лабораторної роботи проводиться поточний контроль, під час якого оцінюється оформлення індивідуального письмового звіту про виконану лабораторну роботу та його захист перед науково-педагогічним працівником (**ЛР**). Лабораторні заняття можуть проводитися дистанційно з використанням електронних засобів комунікації.

Поточний контроль за темами, при вивченні яких не заплановано проведення лабораторних робіт, проводиться у формі письмових контрольних робіт (**КР**) в межах загального обсягу годин.

Поточний контроль засвоєння навчального матеріалу, віднесеного до самостійної роботи, проводиться у формі усного опитування.

**Підсумковий семестровий контроль** проводиться з метою оцінки результатів навчання за дисципліну. Він проводиться у формі семестрового екзамену. Семестрові екзамени та заліки проводяться в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни, і в терміни, встановлені навчальним планом. Семестрові екзамени проводяться в письмовій формі (припускається використання контролю з використанням комп′ютерів, інформаційно-комунікативних технологій). Екзамени складаються студентами в період екзаменаційних сесій, передбачених навчальним планом. Екзамени проводяться згідно з розкладом, який доводиться до відома викладачів і студентів не пізніше, як за місяць до початку сесії. Результати складання екзамену оцінюються за національною шкалою ("відмінно", "добре", "задовільно", "незадовільно"), кількістю балів 1 … 100 і вносяться в екзаменаційну відомість та залікову книжку студента.

**Для оперативного контролю** степені засвоєння матеріалу протягом семестру застосовуються наступні заходи:

- контроль присутності студентів (пропуск лекції без поважної причини – "мінус" один бал);
- контроль і оцінка виконання індивідуального завдання практичного заняття – перевірка роботи комп'ютерної програми (Mathcad-документу) та усна співбесіда;
- контроль знання відповідей на контрольні питання.

Під час проведення підсумкового семестрового контролю виконується перевірка якості конспекту лекцій та практичних занять.

## 9. Схема нарахування балів

| Поточний контроль | | | | | | | | | | | | **розрахункова робота** | **Контрольна робота,(2)** | Разом 60 | Екзамен 40 | Сума 100 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| КР1 | ЛР1 | КР2 | ЛР2 | КР3 | ЛР3 | КР4 | ЛР4 | КР5 | ЛР5 | КР6 | КР7 | | | | | |
| 2 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | 10 | 5*2=10 | 60 | 40 | 100 |

**Примітка**:

КР# - поточний контроль у формі письмової контрольної роботи,

ЛР# - поточний контроль у формі лабораторної роботи,

# - номер роботи.

До кількості балів, отриманих студентом за кожну КР та ЛР, додається сума балів оперативного контролю, але загальна сума балів оперативного та поточного контролю не може перевищувати 60 балів та бути меншою 0 балів.

Результати складання екзамену оцінюються за 40-бальною шкалою. Сума балів (від 0 до 100 балів включно) є загальним результатом вивчення дисципліни, який вносяться в екзаменаційну відомість та залікову книжку студента відповідно до шкали оцінювання.

## Критерії оцінювання

Критерії оцінювання знань студентів на експрес - опитування

| Визначення | Кількість балів |
|---|---|
| Відповідь без помилок | 2 |
| Виконання відповіді з незначними помилками | 1 |
| Відповідь є з певною кількістю помилок, які не заважають достатньо повному висвітленню питання | 0,5 |
| Неправильна відповідь, мають місце грубі помилки, нерозуміння суті питання | 0 |

Критерії оцінювання знань студентів за виконання контрольній роботи

| Визначення | Кількість балів |
|---|---|
| Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки | 5 |
| У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки | 4 |
| У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки | 3 |
| У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки | 1 |
| У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки | 0,5 |

Критерії оцінювання знань студентів за виконання розрахункової роботи

| Визначення | Кількість балів |
|---|---|
| Робота виконана в повному обсязі, розрахунки виконані без помилок , показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки. | 10 |
| Робота виконана в повному обсязі, розрахунки виконані с незначними помилками , показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки. | 8 |
| Робота виконана в повному обсязі, розрахунки виконані при наявності суттєвих помилок, показано достатньо знання навчального матеріалу при наявності, зроблені висновки | 6 |

| | |
|---|---|
| Робота виконана в повному обсязі, розрахунки виконані при наявності принципових помилок, відсутні висновки | 4 |
| Робота виконана в повному обсязі, розрахунки виконані при наявності принципових помилок, відсутні висновки. Показано слабкі знання навчального матеріалу. | 2 |

Критерії оцінювання екзаменаційних робіт студентів

| Визначення | Кількість балів |
|---|---|
| При відповіді на екзаменаційний квиток теоретичні питання освітлені повністю, завдання вирішене правильно, зроблені висновки | 40 |
| При відповіді на екзаменаційний квиток теоретичні питання достатньо освітлені, завдання вирішене правильно з незначними помилками, зроблені висновки | 35-39 |
| При відповіді на екзаменаційний квиток теоретичні питання освітлені з помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки | 25-34 |
| При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене з помилками. Зроблені неповні висновки | 15-24 |
| При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене частково або не повністю. Висновки неповні або відсутні | 1-14 |

**Шкала оцінювання**

| Сума балів за всі види навчальної діяльності протягом семестру | Оцінка | |
|---|---|---|
| | для чотирирівневої шкали оцінювання | для дворівневої шкали оцінювання |
| 90 – 100 | відмінно | зараховано |
| 70-89 | добре | |
| 50-69 | задовільно | |
| 1-49 | незадовільно | не зараховано |

## 10. Рекомендована література
### Основна література


1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 878 с.
2. Есин В. И., Кузнєцов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
3. Кузнецов О.О. Семенов С.Г. Протоколи захисту інформації у комп'ютерних системах та мережах. Х.:ХНУРЕ, 2009р. – 184.
4. Грибунин В.Г., Оков И. Н., Туринцев И. В.. Цифровая стеганография. Серия: Аспекты защиты. – Солон-Пресс, 2002 г. – 272 с.
5. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. МК-Пресс, 2006г. – 288 с.
6. Simmons G.J. The prisoner`s problem and the subliminal channel, Proc. Workshop on Communications Security (Crypto`83), 1984, 51-67.
7. Pfitzmann B. Information Hiding Terminology, in Information Hiding, Springer Lecture Notes in Computer Science, v.1174, 1996, 347-350.
8. Aura T. Invisible communication. In Proc. of the HUT Seminar on Network Security '95, Espoo,

Finland, November 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.
9. Ross J. Anderson. Stretching the limits of steganography. In IH96 [3], pages 39-48.
10. Zollner J., Federrath H.,Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, 344-354.
11. E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.

**Допоміжна література**

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
2. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, vol. 31, no. 2, pp.26-34.
3. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM Systems Journal, 35(3 & 4):313{336, 1996.
4. Raymond B. Wolfgang and Edward J. Delp. A watermark for digital images. In International Conference on Images Processing, pages 219-222, Lausanne, Switzer-land, September 1996. IEEE.
5. Kahn D. The Codebreakers. N-Y, 1967.
6. Жельников В. Криптография от папируса до компьютера. М., 1996.
7. Радіотехніка. Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000 – 2015 рр.
8. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» 2006 – 2015 рр.

**Рекомендоване методичне забезпечення**

1. Методичні вказівки до практичних робіт з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІСТ.
2. Методичні вказівки до лабораторних робіт з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІСТ.
3. Приклади реалізації алгоритмів стеганографічного перетворення на мові символьної математики MathCad. Електронний ресурс кафедри БІСТ.
4. Плани проведення консультацій (друкований та електронній варіанти).
5. Навчальна програма з дисципліни "Стеганографічні системи". Електронний ресурс кафедри БІСТ.
6. Завдання до контрольних робіт (3 роботи). Електронний ресурс кафедри БІСТ.
7. Перелік питань до екзамену за дисципліною "Стеганографічні системи". Електронний ресурс кафедри БІСТ.
8. Екзаменаційні білети за дисципліною "Стеганографічні системи". Електронний ресурс кафедри БІСТ.

## 11. Посиланная на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. www.nist.gov
2. www.eprint.iacr.org
3. www.iso.org
4. www.springerlink.com
5. www.cacr.math.uwaterloo.ca
6. www.financialcryptography.com
7. www.austinlinks.com
8. www.world.std.com/~franl/crypto.html
9. www.cryptonessie.org
10. www.osti.gov/eprints