(Ф 03.02 – 110)

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Національний авіаційний університет**
Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних систем

УЗГОДЖЕНО
Декан ФАЕТ
_____ І. Мачалін
«___» _____ 2019 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ А. Гудманян
«___» _____ 2019 р.

Система менеджменту якості

# РОБОЧА ПРОГРАМА
## навчальної дисципліни
# «Захищені системи та мережі передавання інформації»

Галузь знань: 17 «Електроніка та телекомунікації»
Спеціальність: 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма: «Телекомунікаційні системи та мережі»

| Форма навчання | Семестр | Усього (годин / кредитів ECTS) | Лекції | Практичні заняття | Лабораторні заняття | Самостійна робота | ДЗ / РГР / К | КР / КП | Форма семестрового контролю |
|---|---|---|---|---|---|---|---|---|---|
| Денна: | 2 | 120/4,0 | 34 | – | 17 | 69 | 1 ДЗ – 2 сем. | – | екзамен – 2 сем. |
| Заочна: | 1,2 | 120/4,0 | 8 | – | 6 | 106 | 1 К – 2 сем. | – | екзамен – 2 сем. |

Індекс: РМ-2-3-172/19-3.2.11
Індекс: РМ-12-172/19-3.2.11

Робочу програму навчальної дисципліни «Захищені системи та мережі передавання інформації» розроблено на основі освітньої програми та робочих навчальних планів № РМ-2-3-172/19, № РМ-12-172/19 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю 172 «Телекомунікації та радіотехніка», освітньо-професійна програма «Телекомунікаційні системи та мережі», та відповідних нормативних документів.

Робочу програму розробили:

професор кафедри
телекомунікаційних систем _____ Г. Конахович

доцент кафедри
телекомунікаційних систем _____ О. Пузиренко

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 172 «Телекомунікації та радіотехніка» (освітньо-професійна програма «Телекомунікаційні системи та мережі») — кафедри телекомунікаційних систем, протокол № 11 від 04.XI.2019 р.

Завідувач кафедри _____ Г. Конахович

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету аеронавігації, електроніки та телекомунікацій, протокол № 3 від 05.XI.2019 р.

Голова НМРР _____ Р. Одарченко

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
**Контрольний примірник**

# ЗМІСТ

## ВСТУП

Робочу програму (РП) навчальної дисципліни розроблено на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених розпорядженням № 071/роз від 10.07.2019 р., і відповідних нормативних документів.

## 1. ПОЯСНЮВАЛЬНА ЗАПИСКА

### 1.1. Заплановані результати

Дана навчальна дисципліна є вибірковою (за вільним вибором здобувача вищої освіти) і вводиться кафедрою університету з метою задоволення освітніх і кваліфікаційних потреб майбутніх фахівців за спеціалізацією «Телекомунікаційні системи та мережі», посилення їх конкурентоспроможності та затребуваності на ринку праці, ефективного використання можливостей університету, сприяння академічній мобільності студента та його особистим інтересам; дозволяючи, у підсумку, здійснювати формування державних фахових компетенцій здобувача відповідно до актуальних вимог ринку праці у галузі телекомунікацій та радіотехніки.

Метою викладання дисципліни є розкриття сучасних наукових концепцій, понять, методів і технологій забезпечення захищеності інформаційних мереж і систем передавання інформації за умов її конфіденційності, доступності та цілісності; дослідження процесів безпечного передавання повідомлень, аналізу впливу на захищеність зв'язку завад, ідентифікації та оптимізації каналів захищеної телекомунікаційної мережі.

Завданнями вивчення навчальної дисципліни є:

- оволодіння базовими й концептуальними знаннями у сфері захисту інформації в сучасних телекомунікаційних системах та мережах (ТКСМ);
- оволодіння концепціями ідентифікації проблем захисту інформації в ТКСМ;
- дослідження надійності та стійкості сучасних і перспективних систем захисту інформації в ТКСМ;
- дослідження каналів зв'язку ТКСМ на предмет їхньої безпечності й оптимальності;
- оволодіння методами інформаційного опису захищуваних повідомлень, безпечного передавання й ретрансляції сигналів, ідентифікації та оптимізації безпечних каналів зв'язку ТКСМ.

У результаті вивчення навчальної дисципліни студент повинен набути наступні компетентності:

- *знати:*
  - методи і технології передавання приховуваних повідомлень, їх функціональних перетворень та захисту від пасивних і активних атак порушника;
  - методи і технології використання каналів сучасних телекомунікаційних систем та мереж з метою забезпечення інформаційної безпеки останніх і принципи їх оптимізації,
- *вміти самостійно:*
  - проводити дослідження процесів захисту і приховання повідомлень у типових каналах сучасних ТКСМ;
  - аналізувати реальні та потенційно досяжні характеристики трактів безпечного зв'язку;
  - проводити дослідження процесів передавання прихованих повідомлень з використанням програмних (алгоритмічних) моделей на ПЕОМ за запланованою програмою;
  - проводити дослідження впливу на рівень захищеності інформації в ТКСМ активних і пасивних атак порушника з використанням програмних (алгоритмічних) моделей на ПЕОМ за запланованою програмою.

Міждисциплінарні зв'язки навчальної дисципліни:

Знання і вміння, отримані студентом при вивченні навчальної дисципліни «Захищені системи та мережі передавання інформації» базується на знаннях таких дисциплін, як: «Технології доступу в авіаційних телекомунікаційних системах», «Методи обробки мультимедійної інформації», «Системи білінґу в телекомунікаційних системах», «Системи моніторингу в телекомунікаційних системах», «Системи широкосмугового радіозв'язку», «Системи з кодовим розподілом», «Перспективні системи електрозв'язку», «Методи цифрової обробки мовних сигналів», «Кодери звукових сигналів», «Методи компресії звукових сигналів», а також використовуються при паралельному вивченні наступних дисциплін: «Телекомунікаційні системи та мережі авіаційного транспорту», «Захист інформації в телекомунікаційних системах та мережах», «Безпека інформаційних мереж та систем», «Сучасні безпроводові мережі», «Високошвидкісні системи та мережі передавання інформації».

### 1.2. Програма навчальної дисципліни

Навчальний матеріал дисципліни «Захищені системи та мережі передавання інформації» структурований за модульним принципом і складається з одного однойменного навчального модуля, засвоєння якого передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

**Модуль № 1 «Захищені системи та мережі передавання інформації»**

***Тема 1.1.*** *Сфера інтересів захисту інформації в телекомунікаціях.* Категорії захисту інформації. Предмет, термінологія і сфери використання методів прихованого передавання. Місце останніх у сфері захисту інформації. Перспективи комплексного використання криптографії і стеганографії у типових системах зв'язку, а також в інших, схожих за вимогами автоматизованих системах інформаційного обміну.

***Тема 1.2.*** *Типові системи захисту інформації.* Структурна схема і математична модель типової системи захисту інформації. Базові протоколи систем захисту інформації.

***Тема 1.3.*** *Пасивні й активні атаки на системи захисту інформації.* Проблема стійкості систем захисту інформації. Класифікація можливих атак на телекомунікаційну систему або мережу. Абсолютно надійна система захисту інформації. Свідомо відкритий канал і його призначення. Комплексна модель інформаційного обміну у випадку активних атак.

***Тема 1.4.*** *Аналіз захищеності та стійкості системи захисту інформації від атак.* Визначальні принципи перетворень під час інформаційного обміну та їхній вплив на рівень захищеності та стійкості системи захисту інформації від атак. Перспективні напрямки практичного розвитку аналізу захищеності і стійкості телекомунікаційних систем і мереж. Оцінка якості системи захисту інформації від атак. Стійкість до активних і пасивних атак.

***Тема 1.5.*** *Особливості визначення пропускної здатності захищених каналів зв'язку.* Поняття пропускної здатності у контексті захисту інформації. Сутність каналу прихованого зв'язку і його прихованої пропускної здатності (ППЗ). Основні підходи до оцінки ППЗ. Задача інформаційного приховання. Теоретично досяжна швидкість достовірного передавання приховуваних даних. Умови унеможливлення оптимізації руйнівного впливу й оцінки його ефективності з боку порушника з огляду на значення ППЗ. Проблема врахування випадкових та умисних спотворень сигналів при оцінці ППЗ.

***Тема 1.6.*** *Пропускна здатність захищених каналів зв'язку при активній протидії порушника.* Формулювання задачі та узагальнена структурна схема інформаційного приховання при активній протидії порушника. Принципи перетворень для приховування. Оцінка прихованої пропускної здатності при активній протидії порушника і її властивості.

***Тема 1.7.*** *Стеганографічне приховання даних у просторовій області графічного контейнера.* Класифікація стеганографічних методів. Урахування психоакустичних і психовізуальних моделей систем людини. Сутність просторових, часових і частотних областей приховування. Метод заміни найменшого значущого біта. Метод приховування у блоках або сегментах. Методи заміни палітри. Метод квантування. Метод Дармстедтера-Делейгла. Методи псевдовипадкового інтервалу і псевдо-випадкового переставлення. Метод Куттера-Джордана-Боссена

***Тема 1.8.*** *Стеганографічне приховання даних у частотній області графічного контейнера.* Переваги і недоліки приховувань у частотних областях, порівняно з просторовими. Метод відносної заміни коефіцієнтів дискретного косинусного перетворення. Метод Сю-Ву. Метод Фрідріх. Базові принципи систем зв'язку на основі розширення спектра сигналу. Метод Сміта-Комісті.

***Тема 1.9.*** *Стеганографічне приховання даних у часовій області аудіоконтейнера.* Тривіальні методи приховування у звукових сигналах. Метод розширення спектру сигналу. Використання луно-сигналу.

***Тема 1.10.*** *Стеганографічне приховання даних у частотній області аудіоконтейнера.* Метод фазового кодування. Особливості використання частотних областей аудіоконтейнера.

***Тема 1.11.*** *Стеганографічне приховання даних у тексті.* Методи довільного інтервалу. Синтаксичні і семантичні методи. Комплексне використання способів вбудовування до графічних, звукових і текстових контейнерів під час обміну відеоінформацією.

## 2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### 2.1. Структура навчальної дисципліни

| № пор. | Назва теми | Обсяг навчальних занять (*год.*) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Денна форма навчання (ДФН) | | | | Заочна форма навчання (ЗФН) | | | |
| | | Усього | Лекції | Лабораторні заняття | СРС | Усього | Лекції | Лабораторні заняття | СРС |
| ***Модуль № 1 «Захищені системи та мережі передавання інформації»*** | | | | | | | | | |
| 1.1. | Сфера інтересів захисту інформації в телекомунікаціях. | **2-й семестр** | | | | **1-й семестр** | | | |
| | | 6 | 2 | — | 4 | 7 ½ | ½ | — | 7 |
| 1.2. | Типові системи захисту інформації. | 8 | 2 | 2 | 4 | 7 ½ | ½ | — | 7 |
| 1.3. | Пасивні й активні атаки на системи захисту інформації. | 6 | 2 | — | 4 | 7 ½ | ½ | — | 7 |
| 1.4. | Аналіз захищеності та стійкості системи захисту інформації від атак. | 8 | 2 | 2 | 4 | 7 ½ | ½ | — | 7 |
| 1.5. | Особливості визначення пропускної здатності захищених каналів зв'язку | 6 | 2 | — | 4 | **2-й семестр** | | | |
| | | | | | | 8 ½ | ½ | 1 | 7 |
| 1.6. | Пропускна здатність захищених каналів зв'язку при активній протидії порушника. | 8 | 2 | 2 | 4 | 5 ½ | ½ | — | 5 |
| 1.7. | Стеганографічне приховання даних у просторовій області графічного контейнера. | 12 | 4 | 2 | 6 | 13 | 1 | 1 | 11 |
| 1.8. | Стеганографічне приховання даних у частотній області графічного контейнера. | 14 | 4 | 2 | 8 | 13 | 1 | 1 | 11 |
| 1.9. | Стеганографічне приховання даних у часовій області аудіоконтейнера. | 12 | 4 | 2 | 6 | 13 | 1 | 1 | 11 |
| 1.10. | Стеганографічне приховання даних у частотній області аудіоконтейнера. | 12 | 4 | 2 | 6 | 13 | 1 | 1 | 11 |
| 1.11. | Стеганографічне приховання даних у тексті. | 14 | 4 | 3 | 7 | 10 | 1 | — | 9 |
| 1.12. | Домашнє завдання / контрольна (домашня) робота. | 8 | — | — | 8 | 8 | — | — | 8 |
| 1.13. | Модульна контрольна робота № 1 / підсумкова семестрова контрольна робота. | 6 | 2 | — | 4 | 6 | — | 1 | 5 |
| ***Усього за модулем / навчальною дисципліною*** | | ***120*** | ***34*** | ***17*** | ***69*** | ***120*** | ***8*** | ***6*** | ***106*** |

### 2.2. Лекційні заняття, їхня тематика й обсяг

| № пор. | Назва теми | Обсяг навчальних занять (*год.*) | | | |
|---|---|---|---|---|---|
| | | ДФН | | ЗФН | |
| | | Лекції | СРС | Лекції | СРС |
| *1* | *2* | *3* | *4* | *5* | *6* |
| ***Модуль № 1 «Захищені системи та мережі передавання інформації»*** | | | | | |
| 1.1. | Сфера інтересів захисту інформації в телекомунікаціях. | **2-й семестр** | | **1-й семестр** | |
| | | 2 | 4 | ½ | 7 |
| 1.2. | Типові системи захисту інформації. | 2 | 2 | ½ | 7 |
| 1.3. | Пасивні й активні атаки на системи захисту інформації. | 2 | 4 | ½ | 7 |
| 1.4. | Аналіз захищеності та стійкості системи захисту інформації від атак. | 2 | 2 | ½ | 7 |
| 1.5. | Особливості визначення пропускної здатності захищених каналів зв'язку | 2 | 4 | **2-й семестр** | |
| | | | | ½ | 5 |
| 1.6. | Пропускна здатність захищених каналів зв'язку при активній протидії порушника. | 2 | 2 | ½ | 5 |
| 1.7. | Стеганографічне приховання даних у просторовій області графічного контейнера — тривіальні методи. | 2 | 2 | ½ | 5 |
| 1.8. | Стеганографічне приховання даних у просторовій області графічного контейнера — методи з використання криптографії. | 2 | 2 | ½ | 4 |
| 1.9. | Стеганографічне приховання даних у частотній області графічного контейнера. | 2 | 3 | ½ | 5 |
| 1.10. | Стеганографічне приховання даних у графічному контейнері шляхом розширення спектра. | 2 | 3 | ½ | 4 |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 1.11. | Тривіальні методи приховування в аудіо-сигналах. Метод розширення спектру сигналу. | 2 | 2 | ½ | 5 |
| 1.12. | Стеганографічне приховування з використанням луно-сигналу. | 2 | 2 | ½ | 4 |
| 1.13. | Метод фазового кодування аудіосигналу. | 2 | 2 | ½ | 5 |
| 1.14. | Використання частотних областей аудіо-контейнера. | 2 | 2 | ½ | 4 |
| 1.15. | Синтаксичні і семантичні методи стеганографічного приховання у тексті. | 2 | 2 | ½ | 5 |
| 1.16. | Стеганографічний аналіз. | 2 | 2 | ½ | 4 |
| 1.17. | Модульна контрольна робота. | 2 | 4 | — | — |
| ***Усього за модулем / навчальною дисципліною*** | | ***34*** | ***44*** | ***8*** | ***83*** |

### 2.3. Лабораторні заняття, їхня тематика й обсяг

| № пор. | Назва теми | Обсяг навчальних занять (*год.*) | | | |
|---|---|---|---|---|---|
| | | ДФН | | ЗФН | |
| | | Лабор. заняття | СРС | Лабор. заняття | СРС |
| ***Модуль № 1 «Захищені системи та мережі передавання інформації»*** | | | | | |
| 1.1. | Математична модель сучасної системи захисту інформації. | **2-й семестр** | | **1-й семестр** | |
| | | 2 | 2 | — | — |
| 1.2. | Якість системи захисту інформації від атак. | 2 | 2 | — | — |
| 1.3. | Прихована пропускна здатність каналу зв’язку. | 2 | 2 | **2-й семестр** | |
| | | | | 1 | 2 |
| 1.4. | Метод заміни найменш значущого біта у пікселях зображення. | 2 | 2 | 1 | 2 |
| 1.5. | Метод псевдовипадкового обрання пікселів зображення. | 2 | 2 | 1 | 2 |
| 1.6. | Метод вбудовування до частотних областей зображення. | 2 | 2 | 1 | 2 |
| 1.7. | Метод заміни найменш значущого біта у відліках звуку. | 2 | 2 | 1 | 2 |
| 1.8. | Метод луно-кодування у звуці. | 2+1 | 3 | — | — |
| 1.9. | Підсумкова семестрова контрольна робота. | — | — | 1 | 5 |
| ***Усього за модулем / навчальною дисципліною*** | | ***17*** | ***17*** | ***6*** | ***15*** |

### 2.4. Самостійна робота студента, її зміст й обсяг

| № пор. | Зміст самостійної роботи студента | Обсяг СРС (*год.*) | |
|---|---|---|---|
| | | ДФН | ЗФН |
| 1. | Опрацювання лекційного матеріалу. | 40 | 83 |
| 2. | Підготовка до лабораторних занять. | 17 | 10 |
| 3. | Виконання домашнього завдання / контрольної (домашньої) роботи. | 8 | 8 |
| 4. | Підготовка до модульних / підсумкової семестрової контрольних робіт. | 4 | 5 |
| ***Усього за навчальною дисципліною*** | | ***69*** | ***106*** |

#### *2.4.1. Домашнє завдання*

Домашнє завдання (ДЗ) виконується протягом 12-15 навчальних тижнів 2-го семестру, згідно затверджених у встановленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента з навчальної дисципліни «Захищені системи та мережі передавання інформації».

Конкретна *мета* ДЗ полягає у набутті навичок дослідження надійності та стійкості довільної цифрової системи захисту інформації (мультимедійних даних) в ТКСМ.

Для успішного виконання ДЗ студент має *знати* методи й технології передавання приховуваних повідомлень, їх функціональних перетворень і захисту від пасивних і активних атак порушника, методи і технології використання каналів сучасних ТКСМ з метою захисту останніх, а також принципи їх оптимізації, концепції захисту інформаційних ресурсів; вміти самостійно проводити дослідження процесів захисту і приховання повідомлень у типових каналах сучасних авіаційних телекомунікаційних мереж, аналізувати реальні й потенційно досяжні характеристики трактів безпечного зв’язку (у тому числі — з використанням сучасних апаратно-програмних засобів).

Виконання, оформлення і захист ДЗ здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання ДЗ, — до 8 годин СРС.

### *2.4.2. Завдання на контрольну (домашню) роботу (ЗФН)*

Контрольна (домашня) робота (КДР) виконується у 2-му семестрі, відповідно до затверджених у встановленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента з тем модуля № 1 «Захищені системи та мережі передавання інформації».

Конкретна *мета* КДР полягає у набутті навичок дослідження надійності та стійкості довільної цифрової системи захисту інформації (мультимедійних даних) в ТКСМ.

Для успішного виконання ДЗ студент має *знати* методи й технології передавання приховуваних повідомлень, їх функціональних перетворень і захисту від пасивних і активних атак порушника, методи і технології використання каналів сучасних ТКСМ з метою захисту останніх, а також принципи їх оптимізації, концепції захисту інформаційних ресурсів; вміти самостійно проводити дослідження процесів захисту і приховання повідомлень у типових каналах сучасних авіаційних телекомунікаційних мереж, аналізувати реальні й потенційно досяжні характеристики трактів безпечного зв'язку (у тому числі — з використанням сучасних апаратно-програмних засобів).

Виконання, оформлення і захист КДР здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання КДР, — до 8 годин СРС.

### *2.4.3. Перелік питань для підготовки до екзамену*

Перелік питань та зміст завдань для підготовки до екзамену доводяться викладачем до студента індивідуально і є розробленими провідним викладачем з даної дисципліни та затвердженими протоколом засідання кафедри.

## 3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

### 3.1. Методи навчання

Однією з найважливіших форм процесу викладання навчальної дисципліни є *лекційна робота*. Її рівень у багато чому визначає якість вивчення і розуміння предмету, ефективність проведення інших форм навчальної роботи. Читання лекцій з навчальної дисципліни «Захищені системи та мережі передавання інформації» відбувається у традиційній формі — у вигляді усного обговорення винесеної на заняття теми для всього потоку слухачів, супроводжуючись задиктовуванням ключових для розуміння теми тезисів, наведенням формул, таблиць і графіків за допомогою проектора або на дошці.

Робота на *лабораторних заняттях* проводиться у групах (підгрупах) і передбачає розв'язок ситуаційних завдань з використанням прикладного програмного забезпечення для імітаційного математичного моделювання процесів, винесених в якості предмету дослідження в лабораторних роботах.

Навчально-методичний комплекс з дисципліни розміщується у відповідному класі на базі вебсервісу *Google Classroom* (див. підрозділ 3.3). Приватний ключ доступу до класу видається викладачем на першому занятті з дисципліни. Через Ґугл-клас видаються вихідні дані до передбачених програмою навчальних робіт, проводяться додаткові консультації, відстежується прогрес кожного студента у засвоєнні матеріалів.

### 3.2. Рекомендована література (базова й допоміжна)

***Базова література***

3.2.1. Конахович Г. Ф. *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних* / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. — К. : «Центр навчальної літератури», 2018. — 558 с.

3.2.2. Конахович Г. Ф. *Компьютерная стеганография. Теория и практика* / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : «МК-Пресс», 2006. — 288 с.

3.2.3. *Защита информации в телекоммуникационных системах* / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. — К. : «МК-Пресс», 2005. — 288 с.

3.2.4. Юдін О.К., Корченко О.Г., Конахович Г.Ф. *Захист інформації в мережах передачі даних*. — К. : «НВП "Інтерсервіс"», 2009. — 716 с.

3.2.5. *Основи комп'ютерної стеганографії:* [навч. посіб. для студентів і аспірантів] / Хорошко В. О., Азаров О. Д., Шелест М. Є., Яремчук Ю. Є.; за ред. В. О. Хорошка. — Вінниця : ВДТУ, 2003. — 143 с.

3.2.6. Грибунин В. Г. *Цифровая стеганография* / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2002. — 272 с.

3.2.7. Горбенко І. Д., Гріненко Т. О. *Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч. 1. Криптографічний захист інформації*. — Харків : ХНУРЕ, 2004. — 368 с.

3.2.8. Юдін О. К., Корченко О. Г., Конахович Г. Ф. *Захист інформації в мережах передачі даних*. — К. : «НВП "Інтерсервіс"», 2009. — 716 с.

3.2.9. Лукацкий А. В. *Обнаружение атак*. — СПб. : БХВ-Петербург, 2001. — 624 с.

3.2.10. Гулак Г. Н., Мухачев В. А., Хорошко В. А. *Основы криптографической защиты информации*. — К. : ГУИКТ, 2009. — 228 с.
3.2.11. Попов О. Б. *Цифровая обработка сигналов в трактах звукового вещания* / О. Б. Попов, С. Г. Рихтер. — М. : «Горячая линия-Телеком», 2007. — 341 с.
3.2.12. Сэломон Д. *Сжатие данных, изображения и звука* / Дэвид Сэломон; пер. с англ. В. В. Чепыжова. — М. : «Техносфера», 2006. — 368 с.
3.2.13. Рабинер Л. Р. *Цифровая обработка речевых сигналов* / Л. Р. Рабинер, Р. В. Шафер; пер. с англ. под ред. М. В.Назарова, Ю. Н. Прохорова. — М. : «Радио и связь», 1981. — 496 с.
3.2.14. Кинтцель Т. *Руководство программиста по работе со звуком* / Тим Кинтцель; пер. с англ. И. Г. Злобина. — М. : «ДМК Пресс», 2000. — 432 с.
3.2.15. Ковалгин Ю. А. *Цифровое кодирование звуковых сигналов* / Ю. А. Ковалгин, Э. И. Вологдин. — СПб. : «Корона-принт», 2004. — 240 с.
3.2.16. Радзишевский А. Ю. *Основы аналогового и цифрового звука* — М. : «Вильямс», 2006. — 288 с.

***Допоміжна література***

3.2.17. Конахович Г. Ф., Мачалін І. О., Пузиренко О. Ю. *Теорія електричного зв'язку*: [навч. посіб.] — [2-е вид.] — К. : ТОВ «НВП "Інтерсервіс"», 2013. — 368 с.
3.2.18. Скляр Б. *Цифровая связь. Теоретические основы и практическое применение* / Бернард Скляр; пер. с англ. под ред. А. В. Назаренко. — [2-е изд., исправл.] — М. : «Вильямс», 2003. — 1104 с.
3.2.19. Прокис Дж. *Цифровая связь*. Пер. с англ. / Под ред. Д. Д. Кловского. — М. : «Радио и связь», 2000. — 800 с.
3.2.20. Дубов Д.В., Ожеван М.А. *Кібербезпека: світові тенденції та виклики для України*. — К. : НІСД, 2011. — 30 с.

### 3.3. Інформаційні ресурси в Інтернеті

3.3.1. Стандарт вищої освіти:
*http://mon.gov.ua/activity/education/reforma-osviti/naukovo-metodichna-rada-ministerstva/proekti-standartiv-vishhoyi-osviti.html*

3.3.2. Веб-сторінка кафедри: *http://tks.nau.edu.ua/*

3.3.3. Система управління навчанням *Google Classroom*: *https://classroom.google.com/*

3.3.4. Цифрові допоміжні посібники:
*http://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf*
*http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf*
*http://tks.nau.edu.ua/wp-content/uploads/2017/02/Steganografichna-obrobka-kontentu-tsyfrovogo-movlennya.pdf*

## 4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Оцінювання окремих видів виконаної студентом навчальної роботи[1] здійснюється у балах згідно табл. 4.1.

Таблиця 4.1

*Оцінювання окремих видів навчальної роботи студента*

| ***Модуль № 1 «Захищені системи та мережі передавання інформації»*** | | | | | |
|---|---|---|---|---|---|
| Вид навчальної роботи | Макс. кількість балів | | Вид навчальної роботи | Макс. кількість балів | |
| | ДФН | ЗФН | | ДФН | ЗФН |
| Виконання і захист ЛР № 1 | 5 | — | Виконання і захист ЛР № 4 (2) | 5 | 7 |
| | | | Виконання і захист ЛР № 5 (3) | 5 | 7 |
| Виконання і захист ЛР № 2 | 5 | — | Виконання і захист ЛР № 6 (4) | 5 | 7 |
| | | | Виконання і захист ЛР № 7 (5) | 5 | 7 |
| Виконання і захист ЛР № 3 (1) | 5 | 7 | Виконання і захист ЛР № 8 | 5 | — |
| | | | Виконання і захист ДЗ / КДР | 5 | 10 |
| *Для допуску до виконання МКР № 1 студент ДФН має набрати не менше 27 балів* | | | | | |
| | | | Виконання МКР № 1 / ПСКР | 15 | 15 |
| | | | **Усього за модулем № 1** | **60** | 60 |
| | | | **Семестровий екзамен** | **40** | |
| | | | **Усього за семестр (за дисципліною)** | **100** | |

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку (табл. 4.2).

[1] Тут і надалі прийнято наступні абревіатури: ЛР — лабораторна робота, ДЗ — домашнє завдання, КДР — контрольна (домашня) робота, МКР — модульна контрольна робота, ПСКР — підсумкова семестрова контрольна робота.

Таблиця 4.2

*Відповідність рейтингових оцінок за окремі види навчальної і контрольної роботи у балах оцінкам за національною шкалою*

| Рейтингова оцінка у балах | | | | | | Оцінка за національною шкалою |
|---|---|---|---|---|---|---|
| Виконання і захист ЛР | | Виконання та захист ДЗ | Виконання та захист КДР | Виконання МКР | Виконання ПСКР | |
| ДФН | ЗФН | | | | | |
| 5 | 7 | 5 | 9-10 | 14-15 | 14-15 | «Відмінно» |
| 4 | 6 | 4 | 8 | 12-13 | 12-13 | «Добре» |
| 3 | 4-5 | 3 | 6-7 | 9-11 | 9-11 | «Задовільно» |
| менше 3 | менше 4 | менше 3 | менше 6 | менше 9 | менше 9 | «Незадовільно» |

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить поточну модульну рейтингову оцінку, що заноситься до відомості модульного контролю.

4.4. Сума поточної модульної та контрольної рейтингових оцінок (для студентів ДФН) або поточна модульна оцінка (для студентів ЗФН) становить підсумкову модульну рейтингову оцінку (табл. 4.3), якій відповідає певний рівень оцінки за національною шкалою, що у балах і за національною шкалою заносяться до відомості модульного контролю.

Таблиця 4.3

*Відповідність підсумкової модульної рейтингової оцінки у балах оцінці за національною шкалою*

| Бали за модуль № 1 | | Оцінка за національною шкалою |
|---|---|---|
| ДФН | ЗФН | |
| 54-60 | 41-45 | «Відмінно» |
| 45-53 | 34-40 | «Добре» |
| 36-44 | 27-33 | «Задовільно» |
| менше 36 | менше 27 | «Незадовільно» |

4.5. Підсумкова модульна рейтингова оцінка (для студентів ДФН) або сума підсумкової модульної рейтингової і семестрової контрольної оцінок (для студентів ЗФН) у балах становить підсумкову семестрову модульну рейтингову оцінку, що перераховується в оцінку за національною шкалою (табл. 4.4).

4.6. Сума підсумкової семестрової модульної (табл. 4.4) та екзаменаційної (табл. 4.5) рейтингових оцінок у балах становить підсумкову семестрову рейтингову оцінку, що перераховується в оцінки за національною шкалою та шкалою *ECTS* (табл. 4.6).

4.7. Підсумкова семестрова рейтингова оцінка у балах, за національною шкалою та шкалою *ECTS* заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента. Наприклад, так: *99/Відм./A, 88/Добре/B, 77/Добре/C, 67/Задов./D, 66/Задов./E* тощо.

4.8. Підсумкова рейтингова оцінка дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена оцінка заноситься до Додатку до диплома.

Таблиця 4.4

*Відповідність підсумкової семестрової модульної рейтингової оцінки у балах оцінці за національною шкалою*

| Оцінка у балах | | Оцінка за націон. шкалою |
|---|---|---|
| ДФН | ЗФН | |
| 54-60 | 54-60 | «Відмінно» |
| 45-53 | 45-53 | «Добре» |
| 36-44 | 36-44 | «Задовільно» |
| менше 36 | менше 36 | «Незадовільно» |

Таблиця 4.5

*Відповідність екзаменаційної рейтингової оцінки у балах оцінці за національною шкалою*

| Оцінка у балах | Оцінка за націон. шкалою |
|---|---|
| 36-40 | «Відмінно» |
| 30-35 | «Добре» |
| 24-29 | «Задовільно» |
| менше 24 | «Незадовільно» |

Таблиця 4.6

*Відповідність підсумкової семестрової рейтингової оцінки у балах оцінці за національною шкалою та шкалою ECTS*

| Оцінка у балах | Оцінка за націон. шкалою | Оцінка за шкалою *ECTS* | |
|---|---|---|---|
| | | Оцінка | Пояснення |
| 90-100 | «Відмінно» | *A* | *Відмінно* (відмінне виконання лише з незначною кількістю помилок) |
| 82-89 | «Добре» | *B* | *Дуже добре* (вище середнього рівня з кількома помилками) |
| 75-81 | | *C* | *Добре* (загалом вірне виконання з певною кількістю суттєвих помилок) |
| 67-74 | «Задовільно» | *D* | *Задовільно* (непогано, але зі значною кількістю недоліків) |
| 60-66 | | *E* | *Достатньо* (виконання задовольняє мінімальним критеріям) |
| 35-59 | «Незадовільно» | *FX* | *Незадовільно* (з можливістю повторного складання) |
| 1-34 | | *F* | *Незадовільно* (з обов'язковим повторним курсом) |

(Ф 03.02 – 01)

**АРКУШ ПОШИРЕННЯ ДОКУМЕНТА**

| № прим. | Куди передано (підрозділ) | Дата видачі | П.І.Б. отримувача | Підпис отримувача | Примітки |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

(Ф 03.02 – 02)

**АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ**

| № пор. | Прізвище, ім’я, по батькові | Підпис ознайомленої особи | Дата ознайомлення | Примітки |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

(Ф 03.02 – 03)

**АРКУШ ОБЛІКУ ЗМІН**

| № зміни | № сторінки | | | | Підпис особи, яка внесла зміну | Дата внесення зміни | Дата введення зміни |
|---|---|---|---|---|---|---|---|
| | Зміненого | Заміненого | Нового | Анульо-ваного | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

(Ф 03.02 – 04)

**АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ**

| № пор. | Прізвище, ім’я, по батькові | Дата ревізії | Підпис | Висновок щодо адекватності |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

(Ф 03.02 – 32)

**УЗГОДЖЕННЯ ЗМІН**

| | Підпис | Ініціали, прізвище | Посада | Дата |
|---|---|---|---|---|
| Розробник | | | | |
| Узгоджено | | | | |
| Узгоджено | | | | |
| Узгоджено | | | | |
| Узгоджено | | | | |