

**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**

**«Забезпечення інформаційної безпеки авіаційних  
 телекомунікаційних мереж»**

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 РГР – 2 сем.	–	диф. залік – 2 сем.
Заочна:	1,2	120/4,0	8	–	6	106	1 К – 2 сем.	–	диф. залік – 2 сем.

Індекс: РМ-2-3-172/19-3.2.13

Індекс: РМ-12-172/19-3.2.13



Робочу програму навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж» 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 № 3 від 09.IX.2019 р.

Завідувач кафедри \_\_\_\_\_

Г. Конахович

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету аеронавігації, електроніки та телекомунікацій, протокол № 1 від 11.IX.2019 р.


Голова НМРР \_\_\_\_\_

Р. Одарченко



## ЗМІСТ

	стор.
ВСТУП .....	4
1. ПОЯСНЮВАЛЬНА ЗАПИСКА .....	4
1.1. Заплановані результати .....	4
1.2. Програма навчальної дисципліни .....	5
2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ .....	6
2.1. Структура навчальної дисципліни .....	6
2.2. Лекційні заняття, їх тематика й обсяг .....	7
2.3. Лабораторні заняття, їх тематика й обсяг .....	8
2.4. Самостійна робота студента, її зміст й обсяг .....	8
2.4.1. Розрахунково-графічна робота .....	8
2.4.2. Завдання на контрольну (домашню) роботу (ЗФН) .....	9
2.4.3. Перелік питань для підготовки до підсумкового контролю .....	9
3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ .....	9
3.1. Методи навчання .....	9
3.2. Рекомендована література (базова й допоміжна) .....	9
3.3. Інформаційні ресурси в Інтернеті .....	10
4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ .....	11

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 4 з 13	

## 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 вводить кафедру 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 авіаційних телекомунікаційних мереж за умов конфіденційності, доступності і цілісності інформації, що в ній циркулює; дослідження процесів безпечного передавання повідомлень, аналізу впливу на захищений зв'язок завад, ідентифікації та оптимізації каналів захищеної телекомунікаційної мережі.

Завданнями вивчення навчальної дисципліни є:

- оволодіння базовими і концептуальними знаннями у сфері забезпечення інформаційної безпеки у галузі телекомунікацій та радіотехніки;
- оволодіння концепціями ідентифікації проблем інформаційної безпеки в сучасних авіаційних телекомунікаційних мережах;
- дослідження надійності і стійкості типових систем забезпечення інформаційної безпеки сучасних авіаційних телекомунікаційних мереж;
- дослідження каналів зв'язку на предмет їхньої безпечності та оптимальності;
- оволодіння методами інформаційного опису захищуваних повідомлень, безпечного передавання і ретрансляції сигналів, ідентифікації та оптимізації безпечних каналів зв'язку.


У результаті вивчення даної навчальної дисципліни студент повинен набути такі компетентності:

*знати:*

- програмно-апаратні комплекси міжмережного захисту інформаційних ресурсів;
- принципи забезпечення безпеки інформаційних ресурсів;
- комплексні системи захисту інформації в корпоративних інформаційних системах;
- методи і технології захисту інформації на мережевому рівні;
- методи і технології передавання приховуваних повідомлень, їх функціональних перетворень та захисту від пасивних і активних атак порушника;
- методи і технології використання каналів сучасних авіаційних телекомунікаційних мереж з метою забезпечення інформаційної безпеки останніх і принципи їх оптимізації,

*вміти:*

- самостійно обирати оптимальну політику міжмережної взаємодії, схему підключення міжмережного екрана, параметри функціонування брандмауера;
- самостійно досліджувати і застосовувати на практиці методи й алгоритми автентифікації, аудиту та авторизації користувача;
- самостійно організовувати безпечне використання базових моделей Web-серверів;
- самостійно встановлювати брандмауер в локальну мережу;
- самостійно забезпечувати антивірусний захист поштової системи й протоколювання подій на серверах і робочих станціях за допомогою Log-сервера;
- самостійно застосовувати режими протоколу IPsec;
- самостійно налаштовувати і користуватися алгоритмами відправлення й приймання повідомлень PGP (Pretty Good Privacy);
- самостійно проводити дослідження процесів захисту й приховання повідомлень у типових каналах сучасних авіаційних телекомунікаційних мереж;
- самостійно аналізувати реальні та потенційно досяжні характеристики трактів безпечного зв'язку;

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 5 з 13	

- самостійно проводити дослідження процесів передавання прихованих повідомлень з використанням програмних (алгоритмічних) моделей на ПЕОМ за запланованою програмою;
- самостійно проводити дослідження впливу на рівень інформаційної безпеки 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 «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж» базується на знаннях таких дисциплін, як: «Технології доступу в авіаційних телекомунікаційних системах», «Методи обробки мультимедійної інформації», «Системи білінгу 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». Знання і вміння, отримані студентом при вивченні даної навчальної дисципліни, використовуються при паралельному вивченні наступних дисциплін: «Телекомунікаційні системи та мережі авіаційного транспорту», «Захищені системи та мережі передавання інформації», «Корпоративні системи та мережі передавання інформації», «Безпека інформаційних мереж та систем», «Захист інформації в телекомунікаційних системах та мережах» тощо.

## 1.2. Програма навчальної дисципліни

Навчальний матеріал дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж» структурований за модульним принципом і складається з двох навчальних модулів, а саме:

- *навчального модуля № 1 «Побудова криптографічних систем забезпечення інформаційної безпеки»;*
- *навчального модуля № 2 «Стеганографічні методи забезпечення інформаційної безпеки»,*

кожен з яких є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

### Модуль № 1 «Побудова криптографічних систем забезпечення інформаційної безпеки»

**Тема 1.1. Програмно-апаратні комплекси міжмережного захисту інформаційних ресурсів.** Функції міжмережного екранування. Базові функції брандмауера. Екранувальні шлюзи прикладного і сеансового рівнів. Політика міжмережної взаємодії. Схеми підключення міжмережного екрана. Параметри функціонування брандмауера.


**Тема 1.2. Принципи забезпечення безпеки інформаційних ресурсів.** Концепція трьох «А»: автентифікація, аудит, авторизація. Домен інфокомунікаційної системи і мережі. Методи і алгоритми ідентифікації та автентифікації користувача. Процедура управління доступом. Базові моделі Web-серверів.

**Тема 1.3. Трансляція мережних адрес.** Особливості встановлення брандмауера в локальну мережу. Принципи перетворення мережних адрес (NAT – Network Address Translation). Різновиди трансляції мережних адрес. «Демілітаризована зона» у складі мережних ресурсів організації.

**Тема 1.4. Комплексні системи захисту інформації в корпоративних інформаційних системах.** Переваги використання другого міжмережного екрана і другого поштового сервера. Антивірусний захист поштової системи. Протоколювання системних подій на серверах і робочих станціях за допомогою Log-сервера.

**Тема 1.5. Протоколи захисту інформації на мережному рівні.** Автентифікація, перевірка цілісності і шифрування IP-пакетів за протоколом IPsec. Тунельний і транспортний, основний і агресивний режими протоколу IPsec. Протокол безпечних з'єднань SSL (Secure Sockets Layer) і стек протоколів SSL. Протокол захисту на транспортному рівні TLS (Transport Layer Security).

**Тема 1.6. Гібридна криптосистема PGP (Pretty Good Privacy).** Механізм роботи і функції системи PGP. Алгоритми відправлення і приймання повідомлень PGP. Криптографічні додатки системи PGP.

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 6 з 13	

## Модуль № 2 «Стеганографічні методи забезпечення інформаційної безпеки»

**Тема 2.1. Класифікація і передумови застосування методів стеганографічного приховання даних.** Класифікація методів приховання даних. Урахування психоакустичних і психовізуальних моделей систем людини для можливості організації систем прихованого обміну даними. Сутність просторових, часових і частотних областей приховування.

**Тема 2.2. Стеганографічне приховання даних у просторовій області графічного контейнера — тривіальні методи.** Метод заміни найменшого (або найменших) значущих бітів. Метод приховування у блоках або сегментах. Методи заміни палітри кольорів. Метод квантування зображення. Метод Дармстедтера-Делейгла.

**Тема 2.3. Стеганографічне приховання даних у просторовій області графічного контейнера — методи з використання криптографії.** Метод псевдовипадкового інтервалу. Метод псевдовипадкового переставлення. Метод Куттера-Джордана-Боссена.

**Тема 2.4. 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-Бу. Метод Фрідріх.

**Тема 2.5. Стеганографічне приховання даних у графічному контейнері шляхом розширення спектра.** Базові принципи систем зв'язку на основі розширення спектру сигналу. Метод Сміта-Коміскі.

**Тема 2.6. Статистичні і структурні методи стеганографічного приховання даних у графічному контейнері.** Особливості статистичних і структурних методів стеганографічного приховання даних у зображеннях. Статистичний метод Пітаса. Структурний метод Шелеста.

**Тема 2.7. Стеганографічне приховання даних у часовій області аудіо контейнера.** Тривіальні методи приховування у звукових сигналах. Метод розширення спектру сигналу. Використання луно-сигналу.

**Тема 2.8. 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.


**Тема 2.9. Стеганографічне приховання даних у частотній області аудіо контейнера.** Метод фазового кодування. Особливості й переваги використання частотних областей аудіоконтейнера.

## 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	
1	2	3	4	5	6	7	8	9	10	
<b>МОДУЛЬ № 1 «Побудова криптографічних систем забезпечення інформаційної безпеки»</b>										
1.1.	Програмно-апаратні комплекси міжмережного захисту інформаційних ресурсів.	<b>1-й семестр</b>				<b>1-й семестр</b>				
		4	2	—	2	6 ½	½	—	6	
1.2.	Принципи забезпечення безпеки інформаційних ресурсів.	9	2	2	5	8 ½	½	—	8	
1.3.	Трансляція мережних адрес.	4	2	—	2	6 ½	½	—	6	
1.4.	Комплексні системи захисту інформації в корпоративних інформаційних системах.	9	2	2	5	8 ½	½	—	8	
1.5.	Протоколи захисту інформації на мережному рівні.	4	2	—	2	<b>2-й семестр</b>				
						7 ½	½	1	6	
1.6.	Гібридна криптосистема <i>PGP (Pretty Good Privacy)</i> .	9	2	2	5	10 ½	½	2	8	
1.7.	Модульна контрольна робота № 1.	5	2	—	3	—	—	—	—	
<b>Усього за модулем № 1</b>		<b>44</b>	<b>14</b>	<b>6</b>	<b>24</b>	<b>48</b>	<b>3</b>	<b>3</b>	<b>42</b>	
<b>МОДУЛЬ № 2 «Стеганографічні методи забезпечення інформаційної безпеки»</b>										
2.1.	Класифікація і передумови застосування методів стеганографічного приховання даних.	8	2	2	4	5 ½	½	—	5	




	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 7 з 13	

1	2	3	4	5	6	7	8	9	10
2.2.	Стеганографічне приховання даних у просторовій області графічного контейнера — тривіальні методи.	4	2	—	2	5 ½	½	—	5
2.3.	Стеганографічне приховання даних у просторовій області графічного контейнера — методи з використанням криптографії.	8	2	2	4	9 ¾	¾	1	8
2.4.	Стеганографічне приховання даних у частотній області графічного контейнера.	5	2	—	3	5 ½	½	—	5
2.5.	Стеганографічне приховання даних у графічному контейнері шляхом розширення спектра.	9	2	2	5	5 ½	½	—	5
2.6.	Статистичні і структурні методи стеганографічного приховання даних у графічному контейнері.	4	2	—	2	5 ½	½	—	5
2.7.	Стеганографічне приховання даних у часовій області аудіоконтейнера.	9	2	2	5	5 ½	½	—	5
2.8.	Стеганографічне приховання даних у частотній області аудіоконтейнера.	10	2	2 1	5	9 ¾	¾	1	8
2.9.	Стеганографічне приховання даних у тексті.	4	2	—	2	5 ½	½	—	5
2.10.	Розрахунково-графічна / контрольна робота.	10	—	—	10	8	—	—	8
2.11.	Модульна контрольна робота № 2 / підсумкова семестрова контрольна робота.	5	2	—	3	6	—	1	5
<i>Усього за модулем № 2</i>		<b>76</b>	<b>20</b>	<b>11</b>	<b>45</b>	<b>72</b>	<b>5</b>	<b>3</b>	<b>64</b>
<b>Усього за навчальною дисципліною</b>		<b>120</b>	<b>34</b>	<b>17</b>	<b>69</b>	<b>120</b>	<b>8</b>	<b>6</b>	<b>106</b>

## 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
<b>Модуль № 1 «Побудова криптографічних систем забезпечення інформаційної безпеки»</b>					
1.1.	Програмно-апаратні комплекси міжмережного захисту інформаційних ресурсів.	<b>1-й семестр</b>		<b>1-й семестр</b>	
1.2.	Принципи забезпечення безпеки інформаційних ресурсів.	2	2	½	8
1.3.	Трансляція мережних адрес.	2	2	½	6
1.4.	Комплексні системи захисту інформації в корпоративних інформаційних системах.	2	2	½	8
1.5.	Протоколи захисту інформації на мережному рівні.	2	2	<b>2-й семестр</b>	
1.6.	Гібридна криптосистема <i>PGP (Pretty Good Privacy)</i> .	2	2	½	4
1.7.	Модульна контрольна робота № 1.	2	3	—	—
<b>Усього за модулем № 1</b>		<b>14</b>	<b>15</b>	<b>3</b>	<b>36</b>
<b>Модуль № 2 «Стеганографічні методи забезпечення інформаційної безпеки»</b>					
2.1.	Класифікація і передумови застосування методів стеганографічного приховання даних.	2	2	½	5
2.2.	Стеганографічне приховання даних у просторовій області графічного контейнера — тривіальні методи.	2	2	½	5
2.3.	Стеганографічне приховання даних у просторовій області графічного контейнера — методи з використанням криптографії.	2	2	¾	6
2.4.	Стеганографічне приховання даних у частотній області графічного контейнера.	2	3	½	5
2.5.	Стеганографічне приховання даних у графічному контейнері шляхом розширення спектра.	2	2	½	5
2.6.	Статистичні і структурні методи стеганографічного приховання даних у графічному контейнері.	2	2	½	5
2.7.	Стеганографічне приховання даних у часовій області аудіоконтейнера.	2	2	½	5
2.8.	Стеганографічне приховання даних у частотній області аудіоконтейнера.	2	2	¾	6

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 8 з 13	

1	2	3	4	5	6
2.9.	Стеганографічне приховання даних у тексті.	2	2	½	5
2.10.	Модульна контрольна робота № 2.	2	3	—	—
<b>Усього за модулем № 2</b>		<b>20</b>	<b>22</b>	<b>5</b>	<b>47</b>
<b>Усього за навчальною дисципліною</b>		<b>34</b>	<b>37</b>	<b>8</b>	<b>83</b>

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

№ пор.	Назва теми	Обсяг навчальних занять (год.)			
		ДФН		ЗФН	
		Лабор. заняття	СРС	Лабор. заняття	СРС
<b>Модуль № 1 «Побудова криптографічних систем забезпечення інформаційної безпеки»</b>					
		<b>1-й семестр</b>		<b>2-й семестр</b>	
1.1.	Алгоритм ідентифікації та автентифікації користувача.	2	3	1	2
1.2.	Перетворення мережних адрес.	2	3	1	2
1.3.	Криптосистема PGP.	2	3	1	2
<b>Усього за модулем № 1</b>		<b>6</b>	<b>9</b>	<b>3</b>	<b>6</b>
<b>Модуль № 2 «Стеганографічні методи забезпечення інформаційної безпеки»</b>					
2.1.	Метод заміни найменш значущого біта у пікселях зображення.	2	2	—	—
2.2.	Метод псевдовипадкового обрання пікселів зображення.	2	2	1	2
2.3.	Метод вбудовування до частотних областей зображення.	2	3	—	—
2.4.	Метод заміни найменш значущого біта у відліках звуку.	2	3	—	—
2.5.	Метод луно-кодування у звуці.	2 1	3	1	2
2.6.	Підсумкова семестрова контрольна робота.	—	—	1	5
<b>Усього за модулем № 2</b>		<b>11</b>	<b>13</b>	<b>3</b>	<b>9</b>
<b>Усього за навчальною дисципліною</b>		<b>17</b>	<b>22</b>	<b>6</b>	<b>15</b>

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

№ пор.	Зміст самостійної роботи студента	Обсяг СРС (год.)	
		ДФН	ЗФН
1.	Опрацювання лекційного матеріалу.	31	83
2.	Підготовка до лабораторних занять.	22	10
3.	Виконання розрахунково-графічної / контрольної роботи.	10	8
4.	Підготовка до модульних / підсумкової семестрової контрольних робіт.	6	5
<b>Усього за навчальною дисципліною</b>		<b>69</b>	<b>106</b>

#### 2.4.1. Розрахунково-графічна робота


Розрахунково-графічна робота (РГР) виконується протягом 12-15 навчальних тижнів 2-го семестру, відповідно до затверджених у встановленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента з тем модуля № 2 «Стеганографічні методи забезпечення інформаційної безпеки» навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж».

Конкретна *мета* РГР полягає у набутті навичок дослідження надійності і стійкості довільної цифрової системи забезпечення інформаційної безпеки.

Для успішного виконання РГР студент має *знати* методи і технології передавання приховуваних повідомлень, їх функціональних перетворень і захисту від пасивних і активних атак порушника, методи і технології використання каналів сучасних авіаційних телекомунікаційних мереж з метою забезпечення інформаційної безпеки останніх і принципи їх оптимізації, а також 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 безпечної зв'язку (у тому числі — з використанням сучасних апаратно-програмних засобів).

Виконання, оформлення і захист РГР здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання РГР, — до 10 годин СРС.



	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 9 з 13	

#### 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 № 2 «Стеганографічні методи забезпечення інформаційної безпеки» навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж».

Конкретна *мета* КДР полягає у набутті навичок дослідження надійності і стійкості довільної цифрової системи забезпечення інформаційної безпеки.

Для успішного виконання КДР студент має *знати* методи і технології передавання приховуваних повідомлень, їх функціональних перетворень і захисту від пасивних і активних атак порушника, методи і технології використання каналів сучасних авіаційних телекомунікаційних мереж з метою забезпечення інформаційної безпеки останніх і принципи їх оптимізації, а також 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 контрольної (домашньої) роботи здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання роботи, — до 8 годин СРС.

#### 2.4.3. Перелік питань для підготовки до підсумкового контролю

Перелік питань та зміст завдань для підготовки до підсумкового контролю 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 «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж» 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 веб-сервісу *Google Classroom* (див. підрозділ 3.3). Приватний ключ доступу до класу видається викладачем на першому занятті з дисципліни. Через Гугл-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. Горбенко І. Д., Гріненко Т. О. *Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч. 1. Криптографічний захист інформації.* — Харків : ХНУРЕ, 2004. — 368 с.
- 3.2.2. Юдін О. К., Корченко О. Г., Конахович Г. Ф. *Захист інформації в мережах передачі даних.* — К. : «НВП “Інтерсервіс”», 2009. — 716 с.
- 3.2.3. Лукацкий А. В. *Обнаружение атак.* — СПб. : БХВ-Петербург, 2001. — 624 с.
- 3.2.4. Гулак Г. Н., Мухачев В. А., Хорошко В. А. *Основы криптографической защиты информации.* — К.: ГУИКТ, 2009. — 228 с.

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 10 з 13	


- 3.2.5. Конахович Г. Ф. *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних*: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. — К. : «Центр учбової літератури», 2018. — 558 с.
- 3.2.6. Конахович Г. Ф. *Компьютерная стеганография. Теория и практика* / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : «МК-Пресс», 2006. — 288 с.
- 3.2.7. *Защита информации в телекоммуникационных системах* / [Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов]. — К. : «МК-Пресс», 2005. — 288 с.
- 3.2.8. Юдін О.К., Корченко О.Г., Конахович Г.Ф. *Захист інформації в мережах передачі даних*. — К. : «НВП “Інтерсервіс”», 2009. — 716 с.
- 3.2.9. *Основы компьютерной стеганографии*: [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.
- 3.2.10. Грибунин В. Г. *Цифровая стеганография* / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2002. — 272 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. Цифровий посібник: <http://tks.nau.edu.ua/wp-content/uploads/2016/05/Steganografiya.pdf>
- 3.3.5. Цифровий підручник: <https://books.google.com.ua/books?id=-clDwAAQBAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false>

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 11 з 13	

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

4.1. Оцінювання окремих видів виконаної студентом навчальної роботи<sup>1</sup> здійснюється у балах згідно табл. 4.1.

Таблиця 4.1

*Оцінювання окремих видів навчальної роботи студента*

Модуль № 1			Модуль № 2			Макс. кількість балів
Вид навчальної роботи	Макс. кількість балів		Вид навчальної роботи	Макс. кількість балів		
	ДФН	ЗФН		ДФН	ЗФН	
Виконання і захист ЛР № 1.1	8	12	Виконання і захист ЛР № 2.1	8	—	
			Виконання і захист ЛР № 2.2 (2.1)	8	12	
Виконання і захист ЛР № 1.2	8	12	Виконання і захист ЛР № 2.3	8	—	
			Виконання і захист ЛР № 2.4	8	—	
Виконання і захист ЛР № 1.3	8	12	Виконання і захист ЛР № 2.5 (2.2)	8	12	
			Виконання і захист РГР / КДР	10	16	
<i>Для допуску до виконання МКР № 1 студент ДФН має набрати не менше 15 балів</i>			<i>Для допуску до виконання МКР № 2 студент ДФН має набрати не менше 31 балу</i>			
Виконання МКР № 1	12	—	Виконання МКР № 2 / ПСКР	14	24	
<b>Усього за модулем № 1</b>	<b>36</b>	<b>36</b>	<b>Усього за модулем № 2</b>	<b>64</b>	<b>40</b>	
<b>Семестровий диференційований залік</b>						<b>100</b>
<b>Усього за семестр (за дисципліною)</b>						<b>100</b>

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку (табл. 4.2). Залікова рейтингова оцінка (у балах і за національною шкалою) визначається за результатами виконання всіх видів навчальної роботи протягом семестру.

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 РГР	Виконання та захист КДР	Виконання МКР № 1	Виконання МКР № 2	Виконання ПСКР	
ДФН	ЗФН						
8	11-12	9-10	15-16	11-12	13-14	22-24	«Відмінно»
6-7	9-10	8	12-14	9-10	11-12	18-21	«Добре»
5	7-8	6-7	10-11	7-8	9-10	15-17	«Задовільно»
менше 5	менше 7	менше 6	менше 10	менше 7	менше 9	менше 15	«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.


Таблиця 4.3

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

Бали за модуль № 1		Бали за модуль № 2		Оцінка за національною шкалою
ДФН	ЗФН	ДФН	ЗФН	
33-36	33-36	58-64	36-40	«Відмінно»
27-32	27-32	48-57	30-35	«Добре»
22-26	22-26	38-47	24-29	«Задовільно»
менше 22	менше 22	менше 38	менше 24	«Незадовільно»

4.5. Сума підсумкових модульних рейтингових оцінок у балах становить підсумкову семестрову модульну рейтингову оцінку, що перераховується в оцінку за національною шкалою (табл. 4.4).

<sup>1</sup> Тут і надалі прийнято наступні аббревіатури: ЛР — лабораторна робота, РГР — розрахунково-графічна робота, КДР — контрольна (домашня) робота, МКР — модульна контрольна робота, ПСКР — підсумкова семестрова контрольна робота.

	Система менеджменту якості. Робоча програма навчальної дисципліни «Забезпечення інформаційної безпеки авіаційних телекомунікаційних мереж»	Шифр документа	СМЯ НАУ РП 22.01.02 – 01-2019
		стор. 12 з 13	

Таблиця 4.4

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

Оцінка у балах		Оцінка за національною шкалою
ДФН	ЗФН	
90-100	68-76	«Відмінно»
75-89	57-67	«Добре»
60-74	46-56	«Задовільно»
менше 60	менше 46	«Незадовільно»

4.6. У семестрі з диференційованим заліком підсумкова семестрова модульна рейтингова оцінка (для студентів ДФН) або сума підсумкової семестрової модульної рейтингової оцінки із підсумковою семестровою контрольною роботою (для студентів ЗФН) у балах становить підсумкову семестрову рейтингову оцінку, що перераховується в оцінку за національною шкалою і шкалою *ECTS* (табл. 4.5).

Таблиця 4.5

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

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

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./А, 88/Добре/В, 77/Добре/С, 67/Задов./D, 66/Задов./E* тощо.

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



(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	Анульованого			

(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				