(Ф 03.02 – 110)

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

ПОГОДЖЕНО
Проректор з наукової роботи
_____ Євген РОМАНЕНКО
«20» 10 2021 р.

ЗАТВЕРДЖЕНО
Проректор з навчальної роботи
_____ Анатолій ПОЛУХІН
«20» 10 2021 р.

УЗГОДЖЕНО
Декан Факультету аеронавігації,
електроніки та телекомунікацій
_____ Сергій ЗАВГОРОДНІЙ
«13» 10 2021 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА

навчальної дисципліни

«Методи захисту інформації для забезпечення адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості зв'язку»

Галузь знань: 17 «Електроніка та телекомунікації»
Спеціальність: 172 «Телекомунікації та радіотехніка»
Освітньо-наукова програма: «Телекомунікації та радіотехніка»

Форма навчання	Семестр	Усього (годин/кредитів ECTS)	Лекції	Практ. заняття	Лабораторні	Самост. робота	ДЗ / РГР / К.р	КР / КПр	Форма сем. контролю
Денна / вечірня	2	90/3,0	10	20	-	60	-	-	екзамен – 2 с
Заочна	2	90/3,0	6	4	-	80	-	-	екзамен – 2 с

Індекс: НДФ-2-172/21 – ОК 1.3.3
НДФ-2-172з/21 – ОК 1.3.3

СМЯ НАУ РП 22.06-01-2021

Робочу програму навчальної дисципліни «Методи захисту інформації для адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості зв'язку» розроблено на основі освітньо-наукової програми «Телекомунікації та радіотехніка», навчальних та робочих навчальних планів № НДФ-2-172/21, № РДФ-2-172/21, № НДФ-2-172з/21, № РДФ-2-172з/21 підготовки здобувачів вищої освіти освітнього-наукового ступеня «Доктор філософії» за спеціальністю 172 «Телекомунікації та радіотехніка» та відповідних нормативних документів.

Робочу програму розробив
професор кафедри телекомунікаційних та
радіоелектронних систем, д.т.н._____ Георгій КОНАХОВИЧ

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 172 «Телекомунікації та радіотехніка» (освітньо-наукової програми «Телекомунікації та радіотехніка») – кафедри телекомунікаційних та радіоелектронних систем, протокол №27 від «4» 10 2021 р.

Гарант освітньо-наукової програми
«Телекомунікації та радіотехніка»_____ Максим ЗАЛІСЬКИЙ

Завідувач кафедри _____ Роман ОДАРЧЕНКО

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету аеронавігації, електроніки та телекомунікацій, протокол №12 від «18» 10 2021 р.

Голова НМРР _____ Олександр КРИВОНОСЕНКО

УЗГОДЖЕНО
Завідувач відділу
аспірантури та докторантури
_____ Анжела ЛЕЛЕЧЕНКО
«19» 10 2021 р.

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

ЗМІСТ

сторінка

Вступ 4
1. Пояснювальна записка 4
1.1. Місце, мета, завдання навчальної дисципліни 4
1.2. Результати навчання, які дає можливість досягти навчальна дисципліна 4
1.3. Компетентності, які дає можливість здобути навчальна дисципліна 5
1.4. Передумови вивчення навчальної дисципліни 6
2. Зміст навчальної дисципліни 6
2.1. Програма навчальної дисципліни 6
2.2. Тематичний план навчальної дисципліни 7
2.3. Перелік питань для підготовки до екзамену 8
3. Навчально-методичні матеріали з дисципліни 8
3.1. Методи навчання 8
3.2. Рекомендована література (базова і допоміжна) 9
3.3. Інформаційні ресурси в Інтернеті 9
4. Система оцінювання результатів навчання 9
4.1. Засоби оцінювання результатів навчальної діяльності 9
4.2. Методи контролю та схема нарахування балів 9
4.3. Критерії оцінювання досягнень аспірантів 10

ВСТУП

Робоча програма (РП) навчальної дисципліни «Методи захисту інформації для забезпечення адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості зв'язку» розроблена на основі «Методичних рекомендацій до розроблення та оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора від 29.04.2021 № 249/од, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце, мета, завдання навчальної дисципліни

Місце дисципліни в системі професійної підготовки фахівця: ця навчальна дисципліна є дисципліною з оволодіння глибинними знаннями зі спеціальності 172 «Телекомунікації та радіотехніка» та спрямована на формування навичок щодо забезпечення інформаційної безпеки сучасних інформаційно- телекомунікаційних систем.

Метою викладання дисципліни є детальне розкриття методів боротьби з кібер загрозами для сучасних інформаційно- телекомунікаційних систем, технологій підвищення живучості цих систем, методів аналізування систем перехоплення інформації в мережевому та безпровідному обладнанні , серверах та обладнанні робочих місць операторів інформаційно-телекомунікаційних систем.

Завданнями вивчення навчальної дисципліни є:

- вивчення методів створення каналів витоку інформації в сучасних системах зв'язку ;
- вивчення програмно-апаратних засобів перехоплення інформації,яка циркулює в інформаційно-телекомунікаційних системах;
- вивчення принципів функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації;
- вивчення методів захисту інформаційно- телекомунікаційних мереж від загроз терiростичної діяльності та забезпечення безпеки авіаційного транспорту;
- дослідження шляхів вдосконалення стратегій інформаційної та кібербезпеки.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна

ПРН 14. Концептуальні поглибленні знання методологічних і теоретичних основ побудови сучасних телекомунікаційних, інформаційних, радіотехнічних та електронних систем, зокрема для авіаційно-космічної галузі.

ПРН 20. Профільовані знання й практичні навички з електроніки, електромагнетизму, оптики, квантової фізики для досліджень у сфері телекомунікацій та радіотехніки.

ПРН 22. Знання у галузі інформаційної безпеки з аналізу різного роду загроз, зокрема в інформаційному просторі, уміння розробляти та досліджувати моделі загроз безпеки.

ПРН 24. Знання про суб'єкти інформаційної безпеки та інформаційні аспекти кібербезпеки для удосконалення, розроблення та подальшого розвитку методів захисту інформаційно-телекомунікаційних мереж від загроз терористичної діяльності та гібридних війн, зокрема для відповідної складової авіаційної безпеки, уміння їх використовувати.

ПРН 26. Уміння використовувати принципи функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації для адаптації телекомунікаційних систем і мереж зв'язку до зовнішніх впливів, розроблення на цій основі методів підвищення живучості зв'язку.

ПРН 27. Уміння відслідковувати тенденції та напрямки розвитку інформаційно-телекомунікаційних та радіотехнічних систем, а також суміжних і прикладних областей, зокрема пов'язаних з авіаційно-космічною галуззю.

ПРН 31. Уміння підготувати самостійне розгорнуте дослідження (дисертацію), що пропонує розв'язання актуального наукового завдання в галузі телекомунікацій та/або радіотехніки або на межі кількох галузей, результати якого становлять оригінальний внесок у суму знань галузі телекомунікацій та/або радіотехніки та інших галузей.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна

У результаті вивчення навчальної дисципліни здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» повинен набути такі компетентності:

ФК 1. Здатність використовувати у науковій та науково-педагогічній діяльності концептуальні поглибленні знання методологічних і теоретичних основ побудови сучасних телекомунікаційних, інформаційних, радіотехнічних та електронних систем, зокрема для авіаційно-космічної галузі.

ФК 7. Здатність використовувати професійно профільовані знання й практичні навички з електроніки, електромагнетизму, оптики, квантової фізики для досліджень у сфері телекомунікацій та радіотехніки.

ФК 9. Здатність використовувати знання у галузі інформаційної безпеки для аналізу різного роду загроз, зокрема, в інформаційному просторі, а також вміння розробляти та досліджувати моделі загроз безпеки.

ФК 11. Здатність використовувати знання про суб'єкти інформаційної безпеки та інформаційні аспекти кібербезпеки для удосконалення, розроблення та подальшого розвитку методів захисту інформаційно-телекомунікаційних мереж від загроз терористичної діяльності та гібридних війн, зокрема для відповідної складової авіаційної безпеки.

ФК 13. Здатність використовувати принципи функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації для адаптації телекомунікаційних систем і мереж зв'язку до зовнішніх впливів, розроблення на цій основі методів підвищення живучості зв'язку.

ФК 14. Здатність відслідковувати тенденції та напрямки розвитку інформаційно-телекомунікаційних та радіотехнічних систем, а також суміжних і прикладних областей, зокрема пов'язаних з авіаційно-космічною галуззю.

1.4. Передумови вивчення навчальної дисципліни

Навчальна дисципліна «Методи захисту інформації для забезпечення адаптації інформаційно- телекомунікаційних систем до зовнішніх впливів та живучості зв'язку »

базується на таких дисциплінах, як: «Системно-синергетичне моделювання об'єктів досліджень та математичні методи обробки даних в телекомунікаціях та радіотехніці» та «Методи забезпечення надійності та ефективності експлуатації сучасних телекомунікаційних та радіотехнічних систем »;

є базою таких дисциплін як: «Оптимізація та синтез мережевих структур телекомунікацій», «Аналіз і синтез методів обробки інформації в системах CNS/ATM» та інших.

2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Програма навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля, а саме: навчального **модуля № 1 «Методи захисту інформації для забезпечення адаптації інформаційно- телекомунікаційних систем до зовнішніх впливів та живучості зв'язку»**, який є логічно завершеним, самостійним, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

Модуль № 1 «Методи захисту інформації для забезпечення адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості».

Інтегровані вимоги модуля № 1:

У результаті вивчення навчальної дисципліни здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» повинен **знати:**

- основні показники та критерії захищеності інформаційно – телекомунікаційних систем(ІТС) ;
- методи розробки та дослідження моделей загроз безпеки(ІТС);
- методи технічного захисту інформації ІТС;
- методи криптографічного та стеганографічного захисту інформації;
- методи виявлення шкідливих програм в структурних елементах телекомунікаційного та радіотехнічного обладнання;
- методи захисту від кібер загроз телекомунікаційних систем;
- методи забезпечення інформаційної безпеки на авіаційному транспорті;
- стратегії підвищення живучості авіаційного зв'язку.

У результаті вивчення навчальної дисципліни здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» повинен **уміти:**

- проводити оцінку загроз інформаційної безпеки ІТС;
- визначати план дій щодо виявлення каналів витоку інформації;
- оцінювати ефективність використання програмно-апаратних засобів захисту інформації в ІТС;
- аналізувати наслідки кіберзагроз, терористичної діяльності та гібридних війн на живучість авіаційного зв'язку ;
- вдосконалювати стратегії побудови комплексних систем захисту інформації в ІТС.

Навчальна дисципліна передбачає вивчення п'яти тем:

Тема 1. Моделі загроз в інформаційному просторі

Вступ. Предмет, мета та задачі курсу. Класифікація каналів витоку інформації в інформаційно-телекомунікаційних мережах. Класифікація програмно-апаратних засобів порушення конфіденційності, цілісності та доступності інформації.

Тема 2. Методи запровадження закладних пристроїв в мережеве обладнання ІТС

Класифікація шкідливих програм для перехоплення інформації в ІТС. Способи впровадження та активізації шкідливих програм в пристрої ІТС. Способи організації витоку інформації в безпровідних ІТС.

Тема 3. Системи протидії кіберзагрозам, терористичній діяльності та гібридним війнам

Історія протидії спецслужб та хакері у різних країнах. Основні технічні рішення із захисту телефонних переговорів у ІТС. Сучасні технології контролю безпеки в ІТС.

Тема 4. Основні сучасні засоби захисту інформації в ІТС

Сучасні методи технічного захисту інформації. Методи криптографічного та стеганографічного захисту інформації. Оцінювання методів підвищення живучості зв'язку.

Тема 5. Тенденції забезпечення інформаційної безпеки на авіаційному транспорті

Вимоги ІСАО до захисту інформації в авіаційній галузі. Шляхи побудови комплексних систем захисту інформації на авіаційному підприємстві.

2.2. Тематичний план навчальної дисципліни

№ п/п	Назва теми	Обсяг навчальних занять (год.)							
		Денна / вечірня форма навчання				Заочна форма навчання			
		Усього	Лекції	Практ. заняття	СРС	Усього	Лекції	Практ. заняття	СРС
1	2	3	4	5	6	7	8	9	10
Модуль №1 «Методи захисту інформації для забезпечення адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості»									
1.1	Моделі загроз в інформаційному просторі	2 семестр				2 семестр			
		18	2	2 2	12	20	2	2	16
1.2	Методи запровадження закладних пристроїв в мережеве обладнання	14	2	2	10	18	2	-	16
1.3	Системи протидії кіберзагрозам, терористичній діяльності та гібридним війнам	18	2	2 2	12	16	-	-	16
1.4	Основні сучасні засоби захисту інформації в ІТС	18	2	2 2	12	20	2	2	16
1.5	Тенденції забезпечення інформаційної безпеки на авіаційному транспорті	16	2	2 2	10	16	-	-	16
1.6	Модульна контрольна робота №1	6	-	2	4	-	-	-	-
Усього за модулем №1		**90**	**10**	**20**	**60**	**90**	**6**	**4**	**80**
Усього за навчальною дисципліною		**90**	**10**	**20**	**60**	**90**	**6**	**4**	**80**

2.3. Перелік питань для підготовки до екзамену

Перелік питань та зміст завдань для підготовки до екзамену розробляються провідними викладачами, затверджуються протоколом засідання кафедри та доводяться до відома здобувачів вищої освіти освітнього-наукового ступеня «Доктор філософії».

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

Основним методом навчання є комунікативний метод. Для успішного засвоєння матеріалу лекційні заняття рекомендується проводити з використанням мультимедійного обладнання. З метою активації навчально-пізнавальної діяльності здобувачів вищої освіти освітнього-наукового ступеня «Доктор філософії» під час вивчення дисципліни під час проведення практичних занять застосовуються такі методи та технології навчання: робота в малих групах, проблемна дискусія, мозкова атака, презентація, комп'ютерне моделювання.

3.2. Рекомендована література

Базова література

3.2.1. Конахович Г.Ф.,Прогонов Д.О., Пузиренко О.Ю. Компютерна стеганографічна обробка й аналіз мультимедійних даних: підручник.\ Київ: Центр учбової літератури, 2018.-558с.

3.2.2. Кузнецов О.О. Захист інформації в інформаційних системах. –Х.: Вид. ХНЕУ, 2017.-512с.

3.2.3. Konakhovich G., Symonychenko Y., Symonychenko A., Daradkeh Y.I. The research of realization of hidden channel for information transmission with the use of steganographic tools // CEUR Workshop Proceedings, 2020, Volume 2654, pp. 504-515.

Допоміжна література

3.2.4. National – Cyber- Strategy USA. New York: 2018.

3.2.5. ISO\ IES 9594-- 8.

3.3. Інформаційні ресурси в інтернеті

3.3.1 Методичні розробки кафедри (в електронному вигляді).

4. СИСТЕМА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

4.1. Засоби оцінювання результатів навчальної діяльності

Діагностика навчальних досягнень аспірантів здійснюється шляхом обов'язкового виконання аспірантами таких видів начальної діяльності: робота на практичному занятті, виконання модульної контрольної роботи.

4.2. Методи контролю та схема нарахування балів

4.2.1. Оцінювання окремих видів виконаної здобувачем вищої освіти освітнього-наукового ступеня «Доктор філософії» навчальної роботи здійснюється в балах відповідно до табл. 4.1.

Таблиця 4.1

Вид навчальної роботи	**Максимальна кількість балів**	
	Очна форма навчання	**Заочна форма навчання**
	Модуль №1 «Методи захисту інформації для забезпечення адаптації інформаційно-телекомунікаційних систем до зовнішніх впливів та живучості»	
Виконання та захист практичних робіт	12б×5 = 60	30б×2=60
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	*36 балів*	–
Виконання модульної контрольної роботи №1	20	–
Усього за модулем № 1	**80**	**60**
Семестровий екзамен	**20**	**40**
Усього за дисципліною	**100**	

4.2.2. Переведення підсумкової рейтингової оцінки в балах в оцінки за національною шкалою та шкалою ECTS здійснюється відповідно до табл. 4.2.

Таблиця 4.2

Відповідність підсумкової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	**Оцінка за національною 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** (в загальному 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)

4.2.3. Підсумкова рейтингова оцінка з дисципліни заноситься до заліково-екзаменаційної відомості, індивідуального навчального плану здобувача вищої освіти освітнього-наукового ступеня «Доктор філософії» та до академічної довідки про виконання освітньо-наукової програми.

4.3. Критерії оцінювання досягнень аспірантів

4.3.1. Критерієм успішного проходження здобувачем вищої освіти освітнього-наукового ступеня «Доктор філософії» оцінювання є досягнення ним мінімальних рівнів оцінок за кожним запланованим видом навчальної діяльності.

Виконані види навчальної роботи зараховуються здобувачу вищої освіти освітнього-наукового ступеня «Доктор філософії», якщо він отримав за них позитивну оцінку (за національною шкалою) відповідно до даних табл. 4.3.

Таблиця 4.3

Відповідність рейтингових оцінок за окремі види навчальної роботи в балах оцінкам за національною шкалою

Рейтингова оцінка в балах				**Оцінка за національною шкалою**
Виконання та захист практичної роботи (очна форма)	**Виконання та захист практичної роботи (заочна форма)**	**Поточна модульна оцінка**	**Контрольна модульна оцінка**	
11 – 12	27 – 30	54 – 60	18 – 20	Відмінно
9 – 10	23 – 26	45 – 53	15 – 17	Добре
7 – 8	18 – 22	36 – 44	12 – 14	Задовільно
менше 7	менше 18	менше 36	менше 12	Незадовільно

4.3.2. Здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» допускається до виконання модульної контрольної роботи за умови наявності у нього поточної модульної рейтингової оцінки величиною не менше 60% максимальної поточної модульної рейтингової оцінки.

Слід мати на увазі, що отримання аспірантом лише мінімальних оцінок за виконання окремих видів навчальної роботи з певного модуля може виявитися недостатнім для отримання допуску до виконання модульної контрольної роботи та потребуватиме виконання ним додаткового індивідуального завдання, захистити його з позитивною оцінкою в балах, яка буде додана до поточної модульної рейтингової оцінки.

4.3.3. Здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» допускається до екзамену за умови отримання позитивних (за національною шкалою) контрольних модульних рейтингових оцінок.

У разі отримання незадовільних контрольної модульної чи екзаменаційної рейтингових оцінок здобувач вищої освіти освітнього-наукового ступеня «Доктор філософії» повинен повторно пройти відповідний контроль в установленому порядку. При повторному його проходженні максимальна величина рейтингової оцінки в балах не повинна перевищувати максимальне значення оцінки «Добре» за національною шкалою.

(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 ознайом-леної особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата Введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				