(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра безпеки інформаційних технологій

УЗГОДЖЕНО
Декан ФККПІ
_____ К. Нестеренко
«___»_____2022 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ А. Полухін
«31» _____ 2022 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Технології захисту інформації»

Освітньо-професійна програма: «Інформаційні управляючі системи та технології»
«Інформаційні технології проектування»
Галузь знань 12 Інформаційні технології
Спеціальність: 122 Комп'ютерні науки

Форма навчання	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна:	7	105/3,5	17	-	34	54			Екз. 7 с
Заочна	8	120/4,0	4	-	8	93	1 к - 8 с		Екз. 8 с

Індекс: РБ-4-122-1/21-2.1.18
Індекс: РБ-4-122-1з/21-2.1.18
Індекс: РБ-4-122-2/21-2.1.18

СМЯ НАУ РП 09.01.08-01-2022

Робочу програму навчальної дисципліни «Технології захисту інформації» розроблено на основі освітньо-професійних програм «Інформаційні управляючі системи та технології» та «Інформаційні технології проектування» навчальних та робочих навчальних планів № РБ-4-122-1/21, № РБ-4-122-1з/21, № РБ-4-122-2/21 підготовки здобувачів вищої освіти освітнього ступеня «Бакалавр» за спеціальністю 122 «Комп'ютерні науки» та відповідних нормативних документів.

Робочу програму розробили:
професор кафедри безпеки інформаційних технологій _____ В. ХОРОШКО
доцент кафедри безпеки інформаційних технологій _____ Ю. ХОХЛАЧОВА

Робочу програму обговорено та схвалено на засіданні кафедри безпеки інформаційних технологій, протокол №7 від 27.08.2021 р.

Завідувач кафедри _____ О. КОРЧЕНКО

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 122 «Комп'ютерні науки» (освітньо-професійні програми «Інформаційні управляючі системи та технології» та «Інформаційні технології проектування») – кафедри комп'ютерних інформаційних технологій, протокол №__ від _____ р.

Гаранти освітніх програм: _____ І. РАЙЧЕВ
_____ Ю. СІНЬКО

Завідувач кафедри _____ А. САВЧЕНКО

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол № 10 від «27» 10 2022 р.

Голова НМРР _____ С. ГНАТЮК

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Врахований примірник____

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Технології захисту інформації» розроблена на основі «Методичних рекомендацій до розроблення і 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 даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця з комп'ютерних наук та інформаційних технологій та дозволяють вирішувати професійні задачі, що базуються на організації дій в кризових ситуаціях пов'язаних з інформаційною безпекою.

Мета та завдання вивчення навчальної дисципліни є підготовка фахівців з інформаційних технологій для виконання обов'язків посадових осіб служби захисту інформації.

Завданнями вивчення навчальної дисципліни є:

- оволодіння сучасними технологіями несанкціонованого отримання
- інформації;
- оволодіння технологіями захисту територій та об'єктів;
- отримання інформації по технічним каналам;
- оволодіння сучасними технологіями захисту мереж зв'язку;
- оволодіння сучасними технологіями програмного захисту;
- оволодіння сучасними технологіями криптографічного захисту;
- оволодіння сучасними технологіями стеганографії.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна:

ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки.

ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

Компетентності набуті студентом в результаті вивчення дисципліни:

ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

ФК3. Здатність та уміння проводити дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

ФК4. Здатність та уміння проводити дослідження проблеми забезпечення інформаційної безпеки національних інтересів України, вивчати і обґрунтовувати форми та методи захисту людини, суспільства й держави від зовнішніх і внутрішніх загроз в інформаційній сфері, а також шляхи підвищення ефективності функціонування інформаційних систем держави в сучасних умовах.

ФК5. Уміння застосовувати та розробляти сучасні технології, системи, технічні засоби, методи та моделі, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій, освітній та професійній діяльності;

ФК7. Здатність та уміння проводити дослідження проблеми забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів, інформаційні ресурси різних класів на об’єктах інформаційної діяльності та критичної інфраструктури, системи управління, на основі технології, методів, моделей та засобів у сфері інформаційної безпеки та/або кібербезпеки;

ФК9. Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення.

1.4. Міждисциплінарні зв’язки.

Навчальна дисципліна «Технології захисту інформації» базується на знаннях таких дисциплін, як: «Теорія прийняття рішень», «Системний аналіз» та доповнює такі дисципліни, як: «Управління ІТ-проетами» та інших.

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля, а саме:

2.2. Модульне структурування та інтегровані вимоги до кожного модуля

Модуль №1 "Технології захисту".

Інтегровані вимоги модуля №1:

Знати:

- види загроз інформації;
- канали витоку інформації;
- технології несанкціонованого витоку інформації;
- методи та засоби захисту інформації;
- технології захисту об’єктів;
- технології захисту мереж зв’язку;
- технології захисту інформації щодо технічних каналів;
- технології програмного захисту;
- технології криптографічного захисту;
- технології стеганографії.
- канали витоку інформації;
- методи та засоби захисту інформації;
- необхідні технології захисту;
- вимоги до технології захисту з урахуванням особливостей об’єктів та самої інформації.

Вміти:

– самостійно системно творчо мислити у досягненні мети професійної та науково-дослідницької діяльності при створенні технології клієнт-серверного програмного забезпечення надійного збереження даних;

– самостійно презентувати власні і колективні результати аналізу проблем кібербезпеки;

– самостійно вирішувати проблеми інноваційного характеру;

– самостійно шукати альтернативні рішення у професійній діяльності;

- самостійно креативно підходити до індивідуальної науково-дослідної діяльності;
- самостійно аналізувати, оцінювати та синтезувати нові ідеї;
- самостійно володіти навичками проведення експериментальних досліджень;

знання методології, методів та механізмів аналізу кіберресурсів із забезпеченням їх безпеки.

Модуль №1 "Моніторинг та тестування систем кібербезпеки".

Тема 1. Предмет дисципліни, визначення та історичні аспекти.

Предмет дисципліни, її цілі, структура та задачі. Визначення головних понять пов'язаних з технологією захисту інформації.

Історичні аспекти формування технології захисту інформації. Місце і роль захисту інформації в діяльності держави, організації та людини.

Тема 2. Канали витоку інформації. Технології несанкціонованого отримання інформації. Методи та засоби захисту інформації.

Канали витоку інформації: радіоканал, акустичний, електричний, візуально-оптичний та матеріально-речовий. Надається класифікація каналів витоку інформації та фізичні основи їх утворення. Особливості каналів витоку.

Технології несанкціонованого отримання інформації, відповідно до кожного каналу. Особливості роботи на різних об'єктах, з різними системами захисту та протидії. Обзір основних засобів несанкціонованого отримання інформації, як на українських, так і закордонних. Тактико-технічні характеристики засобів.

Тема 3. Класифікація методів захисту інформації. Технології захисту території та об'єктів.

Визначаються їх переваги, недоліки та особливості. Виконуємо функції. Ступені складності та показники оцінки захищеності інформації. Відзначаються підходи до вирішення проблеми захисту інформації та побудови комплексної системи.

Класифікація засобів захисту територій, об'єктів та приміщень. Побудова систем доступу на територію, об'єкти та приміщення. Зовнішній захист. Внутрішній захист. Вимоги до захисту територій, об'єктів, приміщень.

Тема 4. Технологія протидії несанкціонованому отриманню інформації по технічним каналам.

Технології фізичного захисту. Охоронна сигналізація. Інфракустичні, інфрачервоні, сейсмомагнітні, мікрохвильові, фотоелектричні, телевізійні та лазерні технології захисту.

Класифікація технологій. Технології створення акустичних та електромагнітних різного призначення. Технології захисту від радіо приборів та різних типів мікрофонів. Технології боротьби з витоком небезпечних сигналів. Технологія захисту від навмисного силового впливу.

Тема 5. Технології захисту мереж зв'язку. Технології програмного захисту.

Технології виявлення підключення до мереж зв'язку. Класифікація способів виявлення факту і місця підключення до мереж зв'язку. Технологія захисту волокно-оптичних мереж зв'язку. Технологія захисту телефонних мереж: пасивний захист, активний захист. Технології контролю мереж зв'язку. Маскування мови. Скреблювання.

Класифікація програмного захисту. Технології програм зовнішнього захисту. Технологія програм внутрішнього захисту. Технології програмного розпізнавання користувачів. Технології захисту від копіювання. Технології автентифікації та ідентифікації користувачів. Технології програмного захисту програм.

Тема 6. Технологія криптографічного захисту. Технології стеганографії.

Класифікація криптографічних технологій. Технології шифрування. Технології керування інформації. Технології комп'ютерної криптографії. Технології цифрового підпису. Технології цифрових водяних знаків.

Класифікація стеганосистем. Технологічні та інформаційні технології стеганографії. Технології комп'ютерної стеганографії. Технології використання інформаційного середовища (текстова, звукова, кадр (відео)). Технологія створення стеганоконтейнера. Синтаксичні технології. Сімантичні технології.

Тема 7. Шляхи розвитку технологій захисту інформації.

Шляхи та тенденції розвитку технологій захисту інформації. Державна політика в сфері інформаційної безпеки.

Тема 8. Розробка технологій захисту інформації.

Розробка технологій захисту інформації є складний і багатогранний процес, який потребує значних зусиль усіх гілок влади та вітчизняної науки.

2.3. Тематичний план.

№ п/п	Назва теми	Обсяг навчальних занять (год.)							
		Денна форма навчання				Заочна форма навчання			
		Усього	Лекції	Лабор. заняття	СРС	Усього	Лекції	Лабор. заняття	СРС
1	2	3	4	5	6	7	8	9	10
Модуль №1 «Технології захисту інформації»									
1.1	Предмет дисципліни, визначення та історичні аспекти.	**7 семестр**				**8 семестр**			
		13	2	2 2	7	11	-	-	11
1.2	Канали витоку інформації. Технології несанкціонованого отримання інформації. Методи та засоби захисту інформації.	13	2	2 2	7	15	2	2	11
1.3	Класифікація методів захисту інформації. Технології захисту території та об'єктів.	13	2	2 2	7	11	-	-	11
1.4	Технологія протидії несанкціонованому отриманню інформації по технічним каналам.	13	2	2 2	7	14	2	2	10
1.5	Технології захисту мереж зв'язку. Технології програмного захисту.	13	2	2 2	7	12		2	10
1.6	Технологія криптографічного захисту. Технології стеганографії.	12	2	2 2	6	10			10
1.7	Шляхи розвитку технологій захисту інформації.	12	2	2 2	6	10		-	10
1.8	Розробка технологій захисту інформації.	14	2	2 2 2	6	11		1	10
1.9	Контрольна робота	-	-	-	-	8	-	-	8
1.10	Модульна контрольна робота №1	2	1		1	-	-	-	-
1.11	Підсумкова семестрова контрольна робота	-	-	-	-	3	-	1	2
Усього за модулем №1		**105**	**17**	**34**	**54**	**105**	**4**	**8**	**93**
Усього за навчальною дисципліною		**105**	**17**	**34**	**54**	**105**	**4**	**8**	**93**

Виконання та оформлення домашнього завдання здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій.

Час, потрібний для виконання домашнього завдання – до 8 годин самостійної роботи.

2.4. Завдання на контрольну (домашню) роботу (ЗФН).

Контрольна (домашня) робота (ЗФН).

Домашнє завдання виконується в восьмому семестрі, відповідно до затверджених в установленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студентів і є важливим етапом у засвоєнні навчального матеріалу, що викладається у четвертому семестрі.

Домашнє завдання виконується на основі навчального матеріалу, винесеного на самостійне опрацювання студентами, і є складовою модулю №1 "Технології захисту інформації".

Конкретна мета домашнього завдання міститься, в залежності від варіанту завдання, та дозволяє вивчити застосування Мережевого монітора для аналізу мережевих пакетів, вивчити застосування програми "Диспетчер завдань" для оперативного аналізу продуктивності роботи системи, вивчити застосування консолі "Продуктивність" для аналізу продуктивності роботи системи.

Виконання та оформлення домашнього завдання здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій.

Час, потрібний для виконання домашнього завдання – до 8 годин самостійної роботи.

2.5. Перелік питань для підготовки до підсумкової контрольної роботи

Перелік питань та зміст завдань для підготовки до підсумкової контрольної роботи, розробляються провідними викладачами та затверджуються протоколом засідання кафедри та доводяться до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

При вивчення навчальної дисципліни використовуються наступні методи навчання:

– пояснювально-ілюстративний метод;

– метод проблемного викладу;

– репродуктивний метод;

– дослідницький метод.

Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному вирішенні задач, роботі з навчальною літературою, аналізі та побудови спеціального системного програмного забезпечення.

3.2. Рекомендована література

Базова література

3.2.1. Головань С.М. Загальне діловодство та ведення документів, що містять конфіденційну інформацію з грифом "Для службового користування". Навчально-методичний посібник. – К.: НАУ, 2003. – 92с.

3.2.2. Шевчук В.О., Корченко О.Г., Головань М.С., Душеба В.В., Пацира Є.В. Авіаційна безпека. Зберігання та обробка документів. Навчальний посібник. – К.: НАУ, 2004. – 92 с.

3.2.3. Ворожко В.П., Корченко А.Г. Захист інформації з обмеженим доступом. Збірник нормативних документів. - К.: Вид-во КМУЦА, 1999, - 283с.

3.2.4. О.В. Ботвінкін, В.П. Ворожко. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України: Аналітичний огляд. –К.: Видавництво НА СБ України, 2006. – 96 с.

3.2.5. Шлапаченко В.М., Ворожко В.П., Шамсутдінов О.В. Становлення та розвиток кримінально-правової охорони державної таємниці в Україні. – К.: Видавництво НА СБ України, 2006. – 55с.

3.2.6. Корченко А.Г. Англо-украинско-русский словарь с толкованиями по безопасности информации в компьютерных системах. - Киев: Издательство КМУГА. – 658с.

Допоміжна література

3.2.7. Корченко О.Г. Системи захисту інформації: монографія. – К.: НАУ, 2004. – 264с.

3.3. Інформаційні ресурси в інтернеті

3.3.1. www.rada.gov.ua – офіційний сайт Верховної Ради України.

3.3.2. www.dstszi.gov.ua/dstszi - офіційний сайт ДСТЗІ.

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ.

4.1. Оцінювання окремих видів виконаної студентом навчальної роботи здійснюється в балах відповідно до табл.4.1.

Таблиця 4.1

	Максимальна кількість балів	
	Денна форма навчання	**Заочна форма навчання**
Вид навчальної роботи	**Модуль №1**	
Виконання та захист лабораторних робіт	**4 семестр**	**5 семестр**
	8×10б = 80	2×20б = 40
Виконання та захист домашнього завдання (контрольної роботи)	-	30
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	*48 балів*	-
Виконання модульної контрольної роботи №1	20	-
Підсумкова семестрова контрольна робота	-	30
Усього за модулем №1	100	100
Усього за дисципліною	**100**	

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

Залікова рейтингова оцінка визначається (в балах та за національною шкалою) за результатами виконання всіх видів навчальної роботи протягом семестру.

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

4.4. Підсумкова семестрова рейтингова оцінка, перераховується в оцінку за національною шкалою та шкалою ECTS.

4.5. Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента, наприклад, так: 92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E тощо.

4.6. Підсумкова рейтингова оцінка з дисципліни дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена підсумкова рейтингова оцінка з дисципліни 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 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				