

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП
ПП22

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
роботи, к.т.н., доцент

С.О. Слободян

2022 р.



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ
Comprehensive information security systems

Рівень вищої освіти перший (бакалаврський)
Тип дисципліни обов'язкова
Мова викладання українська

Миколаїв 2022 рік

Робоча програма навчальної дисципліни «Комплексні системи захисту інформації» є однією із складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»
«___» _____ 2022 р. – с.

Розробник: Нужний С.М., завідувач кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Комплексні системи захисту інформації» узгоджено з гарантом освітньої програми

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Нужний С.М., канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Комплексні системи захисту інформації» розглянуто на засіданні кафедри КТІБ.

Протокол від «18» 04 2022 р. № 9.

Завідувач кафедри КТІБ, к.т.н., доцент С.М. Нужний

Проект робочої програми навчальної дисципліни «Комплексні системи захисту інформації» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «21» 04 2022 р. № 9.

Голова, к.т.н., доц. В.А. Скороходов

Проект робочої програми навчальної дисципліни «Комплексні системи захисту інформації» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент А.В. Лабарткава

Робочу програму навчальної дисципліни «Комплексні системи захисту інформації» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «27» 04 2022 р. № 3.

Голова Навчально-методичної ради НУК ім. адм. Макарова,

д.т.н., професор Є.І. Трушляков

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета вивчення навчальної дисципліни.....	6
3. Передумови для вивчення навчальної дисципліни	6
4. Очікувані результати навчання.....	6
5. Програма навчальної дисципліни.....	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	14
7. Форми поточного та підсумкового контролю.....	15
8. Критерії оцінювання результатів навчання.....	17
9. Засоби навчання	20
10. Рекомендовані джерела інформації.....	21

ВСТУП

Анотація

Ефективний захист інформації, що циркулює на об'єкті інформаційної діяльності (ОІД) в сучасних умовах можливий тільки при комплексному підході. В інших випадках для злоумисників залишається можливість створення каналу витоку інформації. Результатом такого підходу є розробка комплексної системи захисту інформації (КСЗІ). Отримання слухачами курсу теоретичних знань та практичних навичок проектування КСЗІ є базовим програмним результатом навчання та фаховою компетентністю.

Ключові слова: комплексна система захисту інформації, модель загроз, модель каналу витоку інформації

Abstract

Effective protection of information circulating on the object of information activities (OID) in modern conditions is possible only with an integrated approach. In other cases, it remains possible for intruder to create a channel of information leakage. The result of this approach is the development of complex system for information protection (CSIP). Acquisition by students of a course of theoretical knowledge and practical skills of designing CSIP is a basic program learning outcome and professional competence.

Keywords: Complex System for Information Protection, threat model, information leakage channel model

1 Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 3	Галузь знань 12 Інформаційні технології Спеціальність: 125 Кібербезпека	Обов’язкова	
Модулів – 1	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 3		4-й	4-й
Загальна кількість годин – 90		Семестр	
		8-й	8-й
		Індивідуальне науково-дослідне завдання не передбачено	
Тижневих годин для денної форми навчання: Аудиторних – 3; Самостійної роботи: – 3.	Рівень вищої освіти: перший (бакалаврський)	Лекції, год	
		15 год.	3 год.
		Лабораторні роботи, год	
		30 год.	6 год.
		Практичні роботи, год	
		-	-
		Самостійна робота, год	
		45	81
		Вид контролю: екзамен	
	Форма контролю: усна, письмова		

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Комплексні системи захисту інформації» є ознайомлення студентів із основами побудови, проектування, впровадження і супроводження захищених систем на об'єктах інформаційної діяльності та формування у студентів відповідно до освітньої програми таких компетентностей:

- (ЗК2) Знання та розуміння предметної області та розуміння професії;
- (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 до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- (ФК7) Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- (ФК12) Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

3. Передумови для вивчення навчальної дисципліни

Для ефективного вивчення дисципліни «Комплексні системи захисту інформації», студенти повинні засвоїти матеріал з дисциплін:

- Методи та засоби захисту інформації;
- Поля і хвилі в системах технічного захисту інформації;
- Безпека інформаційних та комунікаційних систем;
- Управління інформаційною безпекою;
- Системи і мережі передачі даних.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Комплексні системи захисту інформації» є:

- (РН2) Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

- (РН4) 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;
- (РН9) Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- (РН12) Розробляти моделі загроз та порушника;
- (РН16) Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів
- (РН34) Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
- (РН35) Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки
- (РН39) Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи.

Тема 1. Комплексний підхід до забезпечення інформаційної безпеки. Категорії інформаційної безпеки. (нормативно-законодавче, адміністративне, процедурне і програмно-технічне). Типи об'єктів інформаційної безпеки (державні організації; комерційні структури; окремі громадяни). [1], с. 11-16, с. 25-30; [2], с. 7-34; [3], с. 7-11.

Тема 2. Побудова комплексної системи інформаційної безпеки. Об'єктний простір інформаційної безпеки. Архітектура комплексної системи інформаційної безпеки. Принципи комплексної системи інформаційної безпеки. Функції комплексної системи інформаційної безпеки. Етапи створення комплексної системи. [1], с. 17-24; [2], с. 35-58

Тема 3. Обстеження об'єкта інформаційної безпеки. Зміст робіт при проведенні обстеження об'єкта інформаційної безпеки. Обстеження інформаційного, фізичного середовища та персоналу. Формування завдання на створення комплексної системи інформаційної безпеки [2], с. 59-83; [3], с. 18-187

Змістовий модуль 2. Забезпечення інформаційної безпеки

Тема 4. Нормативно-законодавче забезпечення. Адміністративна та кримінальна відповідальність за порушення інформаційної безпеки. Види державної та конфіденційної комерційної інформації. Економічні передумови захисту конфіденційної інформації. Суть державної та комерційної таємниць та необхідність їх захисту. Нормативне забезпечення та механізм захисту державної та комерційної таємниці. [1], с. 25-36; [2], с.35-58; [3], с. 7-11

Тема 5. Адміністративне забезпечення інформаційної безпеки. Зміст адміністративного забезпечення. Концепція політики інформаційної безпеки: суть, призначення і структура. [1], с. 37-46

Тема 6. Процедурне та програмно-технічне забезпечення інформаційної безпеки. Фізичний захист об'єктів. Захист інформації в комп'ютерних системах. Підтримка безперебійності роботи організації. Реагування на порушення режиму безпеки. Планування відновлювальних робіт. [1], с. 52-59

Змістовий модуль 3. Аналітично-організаційні аспекти забезпечення захисту інформації

Тема 7. Види моделей інформаційної безпеки: моделі об'єктів і суб'єктів інформаційної безпеки та моделі доступу, матриці конфіденційності, моделі загроз, моделі порушника [3], с. 189-249

Тема 8. Організаційне забезпечення інформаційної безпеки. Зміст та задачі організаційного забезпечення. Розробка порядку інформаційної діяльності об'єкта інформаційної безпеки. Організація конфіденційного документообігу. Організація режиму інформаційної безпеки. Зони режимності об'єкта безпеки. Організація служби інформаційної безпеки [1], с. 46-51

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Модуль 1 (М1)								
Змістовий модуль 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи.								
Тема 1. Комплексний підхід до забезпечення захисту інформації. Категорії інформаційної безпеки. (нормативно-законодавче, адміністративне, процедурне і програмно-технічне). Типи об'єктів інформаційної безпеки (державні організації; комерційні структури; окремі громадяни).	15	2	4	9	45	1	2	12
Тема 2. Побудова комплексної системи захисту інформації. Об'єктний простір інформаційної безпеки. Архітектура комплексної системи захисту інформації. Принципи комплексної системи захисту інформації. Функції комплексної системи інформаційної безпеки. Етапи створення комплексної системи захисту інформації.	15	2	4	9				15
Тема 3. Обстеження об'єкта інформаційної діяльності. Зміст робіт при проведенні обстеження. Обстеження інформаційного, фізичного середовища та персоналу. Формування завдання на створення комплексної системи захисту інформації	15	2	4	9				15
Разом за змістовим модулем 1	45	6	12	27	45	1	2	42
Змістовий модуль 2. Забезпечення інформаційної безпеки								
Тема 4. Нормативно-законодавче забезпечення. Адміністративна та кримінальна відповідальність за порушення інформаційної безпеки. Види державної та конфіденційної комерційної інформації. Економічні передумови захисту конфіденційної інформації. Суть державної та комерційної таємниць та необхідність їх захисту. Нормативне забезпечення та механізм захисту державної та комерційної таємниці.	15	2	4	4	30	1	2	9
Тема 5. Адміністративне забезпечення інформаційної безпеки. Зміст адміністративного забезпечення. Концепція політики інформаційної безпеки: суть, призначення і структура.	15	2	4	4				9

Назви змістових модулів і тем	Кількість годин							
	денна форма				заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р.		л	лаб	с.р.
Тема 6. Процедурне та програмно-технічне забезпечення інформаційної безпеки. Фізичний захист об'єктів. Захист інформації в комп'ютерних системах. Підтримка безперебійності роботи організації. Реагування на порушення режиму безпеки. Планування відновлювальних робіт.	15	2	4	4				9
Разом за змістовим модулем 2	30	6	12	12	30	1	2	27
Змістовий модуль 3. Аналітично-організаційні аспекти забезпечення захисту інформації								
Тема 7. Види моделей інформаційної безпеки: моделі об'єктів і суб'єктів інформаційної безпеки та моделі доступу, матриці конфіденційності, моделі загроз, моделі порушника.	9	2	4	3				6
Тема 8. Організаційне забезпечення інформаційної безпеки. Зміст та задачі організаційного забезпечення. Розробка порядку інформаційної діяльності об'єкта інформаційної безпеки. Організація конфіденційного документообігу. Організація режиму інформаційної безпеки. Зони режимності об'єкта безпеки. Організація служби інформаційної безпеки	6	1	2	3	15	1	2	6
Разом за змістовим модулем 3	15	3	6	6	15	1	2	12
Разом за модулем 1	90	15	30	45	90	3	6	81

Теми практичних занять

Практичні роботи програмою не передбачені

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Класифікація та категорювання інформації на ОІД в відповідності до СБУ № 440 12.08.05 «Звід відомостей, що становлять державну таємницю»	2
2	Етапи створення комплексної системи захисту інформації в відповідності до НД ТЗІ та Наказів Адміністрації Держспецзв'язку	2
3	Обстеження об'єкта інформаційної діяльності. Вимоги НД ТЗІ та Наказів Адміністрації Держспецзв'язку	2
4	Нормативно-законодавче та організаційне забезпечення інформаційної безпеки. Розробка порядку інформаційної діяльності об'єкта. Зони режимності об'єкта безпеки. Організація служби інформаційної безпеки	2
5	Концепція політики інформаційної безпеки: суть, призначення і структура	2
6	Процедурне та програмно-технічне забезпечення інформаційної безпеки. Захист інформації в комп'ютерних системах.	2
7	Модель інформаційної безпеки: моделі об'єктів і суб'єктів інформаційної безпеки та моделі доступу, матриці конфіденційності, моделі загроз, моделі порушника	2
8	Організація конфіденційного документообігу	1
Разом		30

Лабораторні роботи проводяться в режимі лабораторно-практичних занять з виконанням студентами елементів індивідуального науково-дослідного завдання за темою лабораторного заняття.

Студенти заочної форми виконують роботи № 1 – 4 та 7, 8 з урахуванням 1 год./ 1 лаб. роботу.

Самостійна робота

Метою самостійної робота є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних, практичних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК,

читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н.	З.Ф.Н.
1	До теми 1. Комплексний підхід до забезпечення захисту інформації. Категорії інформаційної безпеки. Типи об'єктів інформаційної безпеки.	9	12
2	До теми 2. Побудова комплексної системи захисту інформації. Архітектура комплексної системи захисту інформації. Принципи комплексної системи захисту інформації. Етапи створення комплексної системи захисту інформації.	9	14
3	До теми 3. Обстеження об'єкта інформаційної діяльності. Зміст робіт при проведенні обстеження. Обстеження інформаційного, фізичного середовища та персоналу.	9	15
4	До теми 4. Нормативно-законодавче забезпечення. Суть державної та комерційної таємниць та необхідність їх захисту. Нормативне забезпечення та механізм захисту державної та комерційної таємниці.	4	9
5	До теми 5. Адміністративне забезпечення інформаційної безпеки. Концепція політики інформаційної безпеки	4	9
6	До теми 6. Процедурне та програмно-технічне забезпечення інформаційної безпеки. Реагування на порушення режиму безпеки. Планування відновлювальних робіт.	4	9
7	До теми 7. Види моделей інформаційної безпеки: моделі об'єктів і суб'єктів інформаційної безпеки та моделі доступу, матриці конфіденційності, моделі загроз, моделі порушника	3	6
8	До теми 8. Організаційне забезпечення інформаційної безпеки. Розробка порядку інформаційної діяльності об'єкта інформаційної безпеки. Організація конфіденційного документообігу. Організація режиму інформаційної безпеки. Зони режимності об'єкта безпеки.	3	7
Разом		45	81

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, включається в завдання поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	7	7
2	Самостійне опрацювання окремих тем навчальної дисципліни	8	19
3	Підготовка до лабораторних робіт	10	15
4	Підготовка до модульних контрольних робіт	5	10
5	Індивідуальне науково-дослідне завдання	15	30
Усього годин за модуль 1 (разом за курсом)		45	81

Індивідуальне науково-дослідне завдання

Індивідуальне науково-дослідне завдання передбачає розробку комплексу документів на систему технічного захисту об'єкту для умовного об'єкту інформаційної та/або комерційної діяльності. Основними типами об'єктів захисту є:

- банківське відділення;
- ювелірний магазин;
- конструкторське бюро;
- магазин стрілецької зброї;
- аптека;
- музей.

Розробка документів виконується в відповідності до вимог нормативних документів поліції охорони МВД України та відповідних профільних міністерств і відомств.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- лабораторна робота, інструктаж;
- репродуктивний метод;
- проблемного викладу.

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;

- звіти з лабораторних робіт;
- командні проекти; індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контроль виконання розділів індивідуального науково-дослідного завдання;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації

для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання має ті ж вимоги, виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Процедура захисту звіту з індивідуального науково-дослідного завдання включає наступні елементи:

- надання пояснювальної записки звіту з індивідуального науково-дослідного завдання в електронному вигляді;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзамену** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову залікову роботу (проводиться у письмовій формі), до якої він допускається, якщо має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за підсумкову залікову роботу становить 30 балів. Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу – 5 балів. На заочній формі навчання – 5 балів.

Максимальна сумарна кількість балів за лабораторні роботи – $8 \times 5 = 40$ балів. На заочній формі навчання – $6 \times 5 = 30$ балів

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для заоч. Форми)	Критерії оцінювання
5	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
4	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
3	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми – 40 балів (8 робіт по 5 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>

Для поточного модульного контролю студентами виконуються 3 (три) модульних контрольних роботи за матеріалами змістовних модулів. Максимальний бал за кожну МКР – 5 балів. Загальна сума балів за модульні контрольні роботи – $5 \times 3 = 15$ балів.

За заочною формою навчання в кінці семестру виконується підсумкова залікова робота. Максимальна оцінка за підсумкову залікову роботу – 15 балів.

Критерії оцінювання задач та практичних завдань в МКР

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
бал	5	4,5	4	3,5	3	2,5	2	1,5	1	0,5

Критерії оцінювання задач та практичних завдань в індивідуальній науково-дослідній роботі

виконання роботи, %	критерії оцінювання	бал
100	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.	25
70 - 99	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).	20
59 - 69	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.	15
40 - 58	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.	10
20 - 39	Завдання виконано не у повному об'ємі. Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.	5
1 - 20	Робота не виконана.	

Розподіл оцінки за змістовними модулями та видами контролю

	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 1	Лабораторні роботи	15	Лабораторні роботи	10
	МКР 1	5	–	–
ЗМ 2	Лабораторні роботи	15	Лабораторні роботи	10
	МКР 2	5	–	–
ЗМ 3	Лабораторні роботи	10	Лабораторні роботи	10
	МКР 3	5	–	–
КР	–	–	Контрольна робота	30
ІНДЗ	Звіт	25	Звіт	25
Екзамен	Екзамен	15	Екзамен	15
Сума		100		100

Рівні підсумкової оцінки екзамену з дисципліни (перерахунковий коефіцієнт – 0,4)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) та спеціалізовані лабораторні стенди.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційну систему, спеціалізоване програмне забезпечення для інженерних розрахунків та моделювання технічних засобів, текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному виді).

10. Рекомендовані джерела інформації

Базові

Навчально-методична література

[1] Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с

[2] Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

[3] Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.

Закони України:

– Закон України „Про Державну службу спеціального зв'язку та захисту інформації України”.

– Закон України „Про інформацію”.

– Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”.

– Закон України „Про державну таємницю”.

– Закон України „Про захист персональних даних”.

– Закон України „Про доступ до публічної інформації”.

– Закон України „Про основи національної безпеки України”.

– Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”.

Нормативні документи системи ТЗІ:

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

– НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22

– НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення, наказ ДСТСЗІ СБУ від 28.05.99 №26

- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)
- НД ТЗІ 1.4-002-2008 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань, наказ Адміністрації Держспецзв'язку від 14.02.2008 №32
- НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, наказ ДСТСЗІ СБУ від 13.06.2000 № 29 (Зміна № 1 наказ ДСТСЗІ СБУ від 27.02.2001 №5)
- НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, наказ Адміністрації Держспецзв'язку від 29.08.2012 № 472
- НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, наказ ДСТСЗІ СБУ від 24.04.2003 № 41 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск., зміна № 2, наказ Адміністрації Держспецзв'язку від 17.08.2013 № 451)
- НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, наказ Адміністрації Держспецзв'язку від 15.04.2013 № 215
- НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 27.02.2001 № 5
- НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11
- НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11
- НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 09.04.2001 № 12
- НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 11.09.2001 № 54
- НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізу вальні. Методи та засоби випробувань, наказ ДСТСЗІ СБУ від 06.11.2001 № 64

- Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації, наказ ДСТСЗІ СБУ від 04.09.2000 № 41
- ТР ЕОТ -95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витoku каналами побічних електромагнітних випромінювань і наводок, наказ Державної служби України з питань ТЗІ від 09.06.95 № 25 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск)
- НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, наказ ДСТСЗІ СБУ від 28.05.99 № 26
- НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, наказ ДСТСЗІ СБУ від 28.05.99 № 26
- НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту, наказ ДСТСЗІ СБУ від 28.05.99 № 26
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806)
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172)
- НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки, наказ ДСТСЗІ СБУ від 26.07.99 № 34
- НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, наказ ДСТСЗІ СБУ від 13.12.2002 № 84 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)
- НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 02.04.2003 № 33 (Зміна № 1 наказ від 28.12.2012 № 806)
- НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-

телекомунікаційних системах, наказ Адміністрації Держспецзв'язку від 25.03.2011 № 65

– НД ТЗІ 2.7-001-99 Технічний захист інформації в програмно-керованих АТС загального користування. Порядок виконання робіт, наказ ДСТСЗІ СБУ від 28.05.99 №26 (Зміна № 1 наказ від 28.12.2012 № 806)

– НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки, наказ ДСТСЗІ СБУ від 26.07.99 № 34

– НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172 (Зміна № 1 наказ від 28.12.2012 № 806)

– НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172

– НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, наказ Адміністрації Держспецзв'язку від 23.07.2012 №389

– НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, наказ ДСТСЗІ СБ України від 20.12.2000 № 60 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

– НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ ДСТСЗІ СБУ від 18.06.2002 № 37, зміна № 2 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

– НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова), наказ ДСТСЗІ СБУ від 28.05.99 № 26

– НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, наказ ДСТСЗІ СБ України від 08.11.2005 № 125 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

– НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення

наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11

Допоміжні

Державна експертиза у сфері ТЗІ

Закони України:

- Закон України “Про наукову і науково-технічну експертизу”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України "Про Державну службу спеціального зв'язку та захисту інформації України”;

Положення Держспецзв'язку:

- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року № 1229;
- Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затверджене постановою Кабінету Міністрів України від 03.09.2014 № 411;
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373;
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087”.
- Положенням про державну експертизу в сфері технічного захисту інформації визначено об'єкти та суб'єкти експертизи, встановлено основні функції і права суб'єктів експертизи, порядок їх взаємодії при проведенні експертизи. У додатках приведено форми заяв та документів щодо результатів експертних робіт, які має отримати замовник експертизи.

Стандарти та нормативні документи колишнього СРСР

- ГОСТ 15.005-86 Система разработки и постановки продукции на производство. Создание изделий единичного и мелкосерийного производства, собираемых на месте эксплуатации.
- ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения.

– ГОСТ 24555-81 Система государственных испытаний продукции. Порядок аттестации испытательного оборудования. Основные положения

Метрологічне забезпечення захисту інформації

Закони України

– Закон України „Про метрологію та метрологічну діяльність”.

Державні стандарти України, нормативні документи системи ТЗІ, стандарти та нормативні документи колишнього СРСР

ДСТУ 2681-94 Метрологія. Терміни та визначення.

ДСТУ 2708-2006 Повірка засобів вимірювальної техніки. Організація та порядок проведення.

ДСТУ 3215-95 Метрологія. Метрологічна атестація засобів вимірювальної техніки. Організація та порядок проведення.

ДСТУ 3400:2006 Метрологія. Державні випробування засобів вимірювальної техніки. Основні положення, організація, порядок проведення і розгляду результатів.

ДСТУ 3412-96 Вимоги до випробувальних лабораторій та порядок їх акредитації.

ДСТУ 3651.0-97 Метрологія. Одиниці фізичних величин. Основні одиниці фізичних величин. Міжнародної системи одиниць. Основні положення, назви та позначення.

ДСТУ 4134-2002 Метрологія. Канали вимірювальні вимірювальних інформаційних систем та автоматизованих систем керування технологічними процесами. Вимоги до структури та змісту методик виконання вимірювань.

ДСТУ-Н РМГ 51-2006 Метрологія. Документи до методик повірки засобів вимірювання. Основні положення (РМГ 51-2002, IDT).

ДСТУ ISO/IEC 17025-2006 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій.

Зміни та доповнення