

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 ОК 26	ЗАТВЕРДЖУЮ Проректор з науково-педагогічної роботи, к.т.н., доцент  С.О. Слободян 2023 р.
---------------------	---

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

**ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
ТА ПРОТИДІЇ ТЕХНІЧНИМ РОЗВІДКАМ**

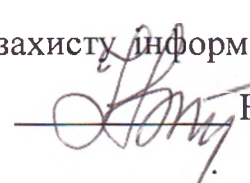
**BASICS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION
AND COUNTERING TECHNICAL INTELLIGENCE**

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

Робоча програма навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» є однією із складових комплексної підготовки фахівців галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону», спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)», освітня програма «Внутрішньополітична безпека»
«25» 08 2023 р. – 27с.

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

Проект робочої програми навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» узгоджено з гарантом освітньої програми

Гарант ОПП «Основи криптографічного захисту інформації та протидії технічним розвідкам», д.політ.н., професор  Н.О. Ніколаєнко

Проект робочої програми навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» розглянуто на засіданні кафедри КТІБ.

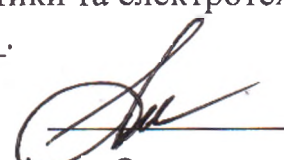
Протокол від «28» 08 2023 р. № 1.

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

Проект робочої програми навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «21» 09 2023 р. № 2.

Голова, к.т.н., доц.

 Д.О. Жук

Проект робочої програми навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» погоджено з навчальним відділом.

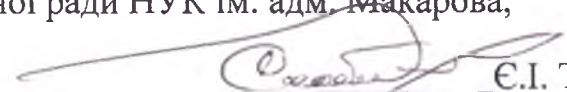
Начальник навчального відділу, к.т.н., доцент  А.В. Лабарткава

Робочу програму навчальної дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «27» 09 2023 р. № 7.

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 та завдання навчальної дисципліни	6
3. Передумови для вивчення навчальної дисципліни	6
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	18
7. Форми поточного та підсумкового контролю	19
8. Критерії оцінювання результатів навчання	21
9. Засоби навчання	23
10. Рекомендовані джерела інформації	24
Зміни та доповнення	27

ВСТУП

Анотація

Постійне зростання рівня загроз для інформаційних та матеріальних ресурсів вимагає створення нових та модифікації існуючих систем безпеки об'єктів інформаційної діяльності та критичних об'єктів інфраструктури. Вирішення задач можливе тільки за умови глибокого та всебічного аналізу як існуючих, можливих для використання зловмисниками, каналів витоку інформації, так і таких, що можуть бути спеціально створеними зловмисниками та передумовами функціонування таких каналів. Вивчення методів та засобів проведення спеціальних заходів для протидії зловмисникам, криптографічного захисту інформації та технологій побудови систем протидії витоку інформації. Такий підхід встановлено на законодавчому рівні та нормативними документами в сфері захисту інформації. Вивчення даної дисципліни забезпечує отримання студентами компетенцій, що необхідні для роботи в державних та комерційних підприємствах, в підрозділах, які спеціалізуються на наданні послуг з національної безпеки та безпека державного кордону.

Ключові слова: системи технічного захисту інформації, модель загроз, технічні канали витоку інформації, протидія витоку інформації, криптографічний захист, базові алгоритми криптографії та криптоаналізу, стеганографія та стеганоаналіз.

Abstract

The constant increase in the level of threats to information and material resources requires the creation of new and modification of existing security systems for information facilities and critical infrastructure. Problems can be solved only with a deep and comprehensive analysis of both existing, possible for use by attackers, information leakage channels, and those that can be specifically created by intruders and the prerequisites for the functioning of such channels. Study of methods and means of conducting special measures to prevention and response intruder, cryptographic protection of information and technologies for building systems to combat information leakage. This approach is enshrined in legislation and regulations in the field of information protection. The study of this subject provides students with the competencies necessary to work in state and commercial enterprises, in units that specialize in providing services for national security and the security of the state border.

Keywords: technical information protection systems, threat model, technical channels of information leakage, countermeasures against information leakage, basic algorithms of cryptography and cryptanalysis, steganography and steganoanalysis.

Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 8	Галузь знань 25 «Воєнні науки, національна безпека, безпека державного кордону» Спеціальність: 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) Освітня програма «Внутрішньополітична безпека»	Обов’язкова	
Модулів – 2		Рік підготовки	
Змістових модулів – 6		3-й та 4-й	–
		Семестр	
Загальна кількість годин – 240		6-й та 7-й	–
		Кількість годин	
		240	–
Тижневих годин для денної форми навчання: <u>6-й семестри:</u> Аудиторних – 2; Сам. роботи – 4. <u>7-й семестри:</u> Аудиторних – 5; Сам. роботи – 5.		Рівень вищої освіти: перший (бакалаврський)	Аудиторні:
	Лекції, год		
	45		–
	Лабораторні роботи, год		
	–		–
	Практичні заняття, год		
	60		–
	Самостійна робота, год		
	135		–
	Вид контролю: 6-й семестри – залік 7-й семестри – екзамен		
Форма контролю: усна, письмова			

1. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни є отримання студентами необхідних знань щодо виявлення технічних каналів витоку інформації (ТКВІ), шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації (ТЗІ) на об'єктах інформаційної діяльності (ОІД), засобам криптографічного і стеганографічного захисту інформації, основам криптоаналізу та стеганографії та формування у студентів відповідно до освітньої програми таких компетентностей:

- (ЗК-06) Здатність до адаптації та дії в новій ситуації;
- (ЗК-09) Здатність використовувати інформаційні та комунікаційні технології;
- (ФК-07) Здатність визначати необхідні технічні заходи врегулювання конфліктів і підтримання миру;
- (ФК-12) Здатність використовувати знання з загальновійськової та спеціальної підготовки;
- (ФК-13) Здатність організовувати та забезпечувати режим секретності, а також ведення, облік, зберігання, використання та знищення інших матеріальних носіїв інформації з обмеженим доступом, у тому числі – порядок захисту такої інформації в інформаційно-телекомунікаційних системах
- (ФК-14) Володіти основами криптографічного захисту інформації та протидії технічним розвідкам.

2. Передумови для вивчення навчальної дисципліни

Для ефективного вивчення дисципліни «Основи криптографічного захисту інформації та протидії технічним розвідкам», студенти повинні засвоїти матеріал з дисциплін:

- Історія військово-політичних стратегій держав світу;
- Національна безпека України;
- Політичний аналіз та прогнозування;
- Криміналістична експертиза документів.

3. Очікувані результати навчання

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

- (ПР-16) Вміти визначати необхідні технічні заходи врегулювання конфліктів і підтримання миру;
- (ПР-22) Вміти організовувати та забезпечувати режим секретності, а також ведення, облік, зберігання, використання та знищення інших матеріальних носіїв інформації з обмеженим доступом, у тому числі – порядок захисту такої інформації в інформаційно-телекомунікаційних системах;
- (ПР-23) Демонструвати вміння з основ криптографічного захисту інформації та протидії технічним розвідкам.

4. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. Криптографічні шифри

Тема 1. Історія криптографії та стеганографії. [1], С. 3-18; [2], С. 6-9.

Тема 2. Класифікація шифрів. Принципи їх роботи. [2], С. 10-15; [3], С. 3-13; 40-45.

Змістовний модуль 2. Криптографічні алгоритми

Тема 3. Алгоритми симетричного та асиметричного шифрування. [3], С. 14-39; 56-71.

Тема 4. Алгоритми потокового шифрування. [3], С. 51-55.

Змістовний модуль 3. Основи стеганографії

Тема 5. Термінологія та класифікація стеганографії. Динамічна стеганографія. [2], С. 9-39.

Тема 6. Цифрові стегоконтейнери. [2], С. 39-44.

Змістовний модуль 4. Основи криптоаналізу та стеганоаналізу

Тема 7. Основні алгоритми криптоаналізу та стеганоаналізу. [2], С. 45-61.

Тема 8. Перспективні напрями криптографії та стеганографії. [2], С. 62-64.

Модуль 2

Змістовий модуль 5. Види, джерела та носії інформації, що підлягає захисту

Тема 9. Види, джерела та носії інформації, що підлягає захисту. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту. [6], С. 13-23.

Тема 10. Джерела і носії інформації, що захищається технічними засобами. Принципи запису і знімання інформації з носіїв. Види загроз безпеці інформації, що захищається технічними засобами. Принципи добування і обробки інформації технічними засобами. [6], С. 24-97.

Змістовий модуль 6. Технічні канали отримання інформації

Тема 11 Технічні канали отримання інформації: визначення, класифікація і структура технічних каналів витоку інформації. [6], С. 98-136.

Тема 12 Методи та принципи роботи засобів отримання інформації при спостереженні в оптичному та радіотеплолокаційному каналах. [6], С. 98-136; 161-164, [7], С. 48-120.

Тема 13 Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному каналі (технології «з проникненням в приміщення»). [7], С. 121-149.

Тема 14 Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному та вібраційному каналах (технології «без проникнення в приміщення»). [7], С. 121-149.

Тема 15 Методи та принципи роботи засобів прослуховування та перехоплення сигналів в радіодіапазоні. [6], С. 137-160, 165-168.

Тема 16 Методи та принципи роботи засобів отримання інформації в радіочастотному каналі, радіолокаційному каналі та каналам ПЕМВН. [7], С. 236-273.

Змістовий модуль 7. Захист інформації що передається по відкритим телекомунікаційним лініям

Тема 17 Методи та засоби захисту акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям. [6], С. 255-426; [7] С.203-208; 274-306

Тема 18 Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами та технічними засобами. Скремблери 1, 2, 3 та 4 родів. [6], С. 427-435

Тема 19 Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодери, напіввокодери та ліпредери. [6], С. 436-471

Змістовий модуль 8. Інженерно-технічний захист інформації

Тема 20 Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що занесені в контрольовану зону (запису на диктофони та інші малогабаритні пристрої). [7], С. 129-130

Тема 21 Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші). [7], С. 130-150

Тема 22 Методи та засоби захисту акустичної інформації від перехоплення засобами ВЧ-збудження акустoeлектричних перетворювачів, ВЧ-накачування та ПЕМВН. [6], С. 150-180

Змістовий модуль 9. Контроль ефективності технічного захисту інформації

Тема 23 Основні етапи проектування системи захисту інформації технічними засобами. Заходи по утаєнню об'єктів від ТЗР (акустичної, гідроакустичної, сейсмічної та аерокосмічної розвідки). Способи оцінки загроз безпеці інформації і витрат на технічний захист. [6], С. 320-381

ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин			
	усього	у тому числі		
		л	пр.р	с.р.
Модуль 1 (М1)				
Змістовий модуль 1. Криптографічні шифри				
Тема 1. Історія криптографії та стеганографії	7	2	2	3
Тема 2. Класифікація шифрів. Принципи їх роботи	8	2	2	4
Разом за змістовим модулем 1	15	4	4	7

Назви змістових модулів і тем	Кількість годин			
	усього	у тому числі		
		л	пр.р	с.р.
Змістовий модуль 2. Криптографічні алгоритми				
Тема 3. Алгоритми симетричного та асиметричного шифрування	15	2	2	11
Тема 4. Алгоритми потокового шифрування	15	2	2	11
Разом за змістовим модулем 2	30	4	4	22
Змістовий модуль 3. Основи стеганографії				
Тема 5. Термінологія та класифікація стеганографії. Динамічна стеганографія	15	2	2	11
Тема 6. Цифрові стегоконтейнери	15	2	2	11
Разом за змістовим модулем 3	30	4	4	22
Змістовий модуль 4. Основи криптоаналізу та стеганоаналізу				
Тема 7. Основні алгоритми криптоаналізу та стеганоаналізу	8	2	2	4
Тема 8. Перспективні напрями криптографії та стеганографії	7	1	1	5
Разом за змістовим модулем 4	15	3	3	9
Разом за модулем 1	90	15	15	60
Модуль 2 (М2)				
Змістовий модуль 5. Види, джерела та носії інформації, що підлягає захисту				
Тема 9. Види, джерела та носії інформації, що підлягає захисту. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту	6	2	2	2
Тема 10. Джерела і носії інформації, що захищається технічними засобами. Принципи запису і знімання інформації з носіїв. Види загроз безпеці інформації, що захищається технічними засобами. Принципи добування і обробки інформації технічними засобами	9	2	4	3
Разом за змістовим модулем 5	15	4	6	5
Змістовий модуль 6. Технічні канали отримання інформації				
Тема 11. Технічні канали отримання інформації: визначення, класифікація і структура технічних каналів витоку інформації	10	2	2	6
Тема 12. Методи та принципи роботи засобів отримання інформації при спостереженні в оптичному та радіотеплолокаційному каналах	10	2	4	4
Тема 13. Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному каналі (технології «з проникненням в приміщення»)	10	2	4	4
Тема 14. Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному та вібраційному каналах (технології «без проникненням в приміщення»).	10	2	4	4

Назви змістових модулів і тем	Кількість годин			
	усього	у тому числі		
		л	пр.р	с.р.
Тема 15. Методи та принципи роботи засобів прослуховування та перехоплення сигналів в радіодіапазоні	10	2	2	6
Тема 16. Методи та принципи роботи засобів отримання інформації в радіочастотному каналі, радіолокаційному каналі та каналах ПЕМВН.	10	2	2	6
Разом за змістовим модулем 6	60	12	18	30
Змістовий модуль 7. Захист інформації що передається по відкритим телекомунікаційним лініям				
Тема 17. Методи та засоби захисту акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям	10	2	4	4
Тема 18. Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами та технічними засобами. Скремблери 1, 2, 3 та 4 родів	10	2	4	4
Тема 19. Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодері, напіввокодері та ліпредери	10	2	2	6
Разом за змістовим модулем 7	30	6	10	14
Змістовий модуль 8. Інженерно-технічний захист інформації				
Тема 20. Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що занесені в контрольовану зону (запису на диктофони та інші малогабаритні пристрої)	10	2	4	4
Тема 21. Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші)	10	2	2	6
Тема 22. Методи та засоби захисту акустичної інформації від перехоплення засобами ВЧ-збудження акусто-електричних перетворювачів, ВЧ-накачування та ПЕМВН	10	2	2	6
Разом за змістовим модулем 8	30	6	8	16
Змістовий модуль 9. Контроль ефективності технічного захисту інформації				
Тема 23. Основні етапи проектування системи захисту інформації технічними засобами. Заходи по утаєнню об'єктів від ТЗР (акустичної, гідроакустичної, сейсмічної та аерокосмічної розвідки). Способи оцінки загроз безпеці інформації і витрат на технічний захист	15	2	3	10
Разом за змістовим модулем 9	15	2	3	10
Разом за модулем 2	150	30	45	75
Усього годин	240	45	60	135

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
Модуль 1 (М1)		
1	Принципи шифрування. Переставні шифри. Шифр Playfair і шифр подвійного квадрата.	2
2	Розробка програмного коду для шифрування тексту шифром Цезаря. Шифрування методом Гронсфельда.	2
3	Алгоритми Віженера, Бофора і Евкліда та мережа Фейстеля.	2
4	Стандарт шифрування DES.	2
5	Криптосистема RSA.	2
6	Криптосистема Ель-Гамала.	2
7	Класифікація стегоалгоритму. Реалізація підсвідомого каналу. Реалізація динамічної стегосистеми.	2
8	Електронний цифровий підпис.	1
Разом за модулем 1		15
1	Види, джерела та носії інформації, що підлягає захисту. ЗВДТ. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту.	2
2	Джерела і носії інформації, що захищається технічними засобами. Принципи запису і знімання інформації з носіїв. Види загроз безпеці інформації, що захищається технічними засобами. Принципи добування і обробки інформації технічними засобами	4
3	Технічні канали отримання інформації: визначення, класифікація і структура технічних каналів витоку інформації	2
4	Засоби отримання інформації при спостереженні в оптичному та радіотеплолокаційному каналах (методи та принципи роботи)	4
5	Засоби отримання інформації при підслуховуванні в акустичному каналі (технології «з проникненням в приміщення»)	4
6	Засоби отримання інформації при підслуховуванні в акустичному та вібраційному каналах (технології «без проникненням в приміщення»).	4
7	Засоби прослуховування та перехоплення сигналів в радіодіапазоні	2

№ з/п	Назва теми	Кількість годин
8	Засоби отримання інформації в радіочастотному каналі, радіолокаційному каналі та каналам ПЕМВН.	2
9	Захист акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям	4
10	Захист акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами та технічними засобами. Скремблери 1, 2, 3 та 4 родів	4
11	Захист акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодери, напіввокодери та ліпредери	2
12	Захист акустичної інформації від перехоплення ТЗР, що занесені в контрольовану зону (запису на диктофони та інші малогабаритні пристрої)	4
13	Захист акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші)	2
14	Захист акустичної інформації від перехоплення засобами ВЧ-збудження акусто-електричних перетворювачів, ВЧ-накачування та ПЕМВН	2
15	Проектування системи захисту інформації технічними засобами (основні етапи). Наказ Держспецзв'язку №023 (ДСК) від 19.06.2015 р. зі змінами наказ № 01т від 23.01.2023 р.	3
Разом за модулем 1		45
Разом		60

ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторні роботи програмою не передбачені

САМОСТІЙНА РОБОТА

Метою самостійної роботи 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
Модуль 1		
1	До теми 1. Історія криптографії та стеганографії	3
2	До теми 2. Класифікація шифрів. Принципи їх роботи	4
3	До теми 3. Алгоритми симетричного та асиметричного шифрування	11
4	До теми 4. Алгоритми потокового шифрування	11
5	До теми 5. Термінологія та класифікація стеганографії. Динамічна стеганографія	11
6	До теми 6. Цифрові стегоконтейнери	11
7	До теми 7. Основні алгоритми криптоаналізу та стеганоаналізу	4
8	До теми 8. Перспективні напрями криптографії та стеганографії	5
Разом за модулем 1		60
Модуль 2		
9	До теми 9. Види, джерела та носії інформації, що підлягає захисту. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту.	2
10	До теми 10. Джерела і носії інформації, що захищається технічними засобами. Принципи запису і знімання інформації з носіїв. Види загроз безпеці інформації, що захищається технічними засобами. Принципи добування і обробки інформації технічними засобами	3
11	До теми 11. Технічні канали отримання інформації: визначення, класифікація і структура технічних каналів витоку інформації	6

№ з/п	Назва теми	Кількість годин
12	До теми 12. Методи та принципи роботи засобів отримання інформації при спостереженні в оптичному та радіотеплолокаційному каналах	4
13	До теми 13. Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному каналі (технології «з проникненням в приміщення»)	4
14	До теми 14. Методи та принципи роботи засобів отримання інформації при підслуховуванні в акустичному та вібраційному каналах (технології «без проникненням в приміщення»).	4
15	До теми 15. Методи та принципи роботи засобів прослуховування та перехоплення сигналів в радіодіапазоні	6
16	До теми 16. Методи та принципи роботи засобів отримання інформації в радіочастотному каналі, радіолокаційному каналі та каналам ПЕМВН.	6
17	До теми 17. Методи та засоби захисту акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям	4
18	До теми 18. Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами та технічними засобами. Скремблери 1, 2, 3 та 4 родів	4
19	До теми 19. Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодери, напіввокодери та ліпредери	6
20	До теми 20. Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що занесені в контрольовану зону (запису на диктофони та інші малогабаритні пристрої)	4
21	До теми 21. Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші)	6
22	До теми 22. Методи та засоби захисту акустичної інформації від перехоплення засобами ВЧ-збудження акусто-електричних перетворювачів, ВЧ-накачування та ПЕМВН	6

№ з/п	Назва теми	Кількість годин
23	До теми 23. Основні етапи проектування системи захисту інформації технічними засобами. Заходи по утаєнню об'єктів від ТЗР (акустичної, гідроакустичної, сейсмічної та аерокосмічної розвідки). Способи оцінки загроз безпеці інформації і витрат на технічний захист	10
Разом за модулем 2		75
Разом		135

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.

Денна форма навчання

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 1,0 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 1,0 год. / 1 год. занять;
- підготовка до практичних робіт – 2,0 год. / 1 год. занять;
- підготовка до контрольних заходів – 2,0 год. на 1 захід.

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин
1	Підготовка до лекцій	15
2	Самостійне опрацювання окремих тем навчальної дисципліни	15
3	Підготовка до практичних робіт	22
4	Підготовка до модульних контрольних робіт	8
Усього годин за модуль 1		60
1	Підготовка до лекцій	15
2	Самостійне опрацювання окремих тем навчальної дисципліни	15
3	Підготовка до практичних робіт	35
4	Підготовка до модульних контрольних робіт	10
Усього годин за модуль 2		75
Разом за курсом		135

5. 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.

6. 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 практичних робіт;
- проведення та перевірка модульних контрольних робіт;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

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

Процедура захисту звіту з практичної 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.

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.

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 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 **заліку** (Модуль 1) та **екзамену** (Модуль 2) 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 20 балів.

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.

7. Критерії оцінювання результатів навчання

При оцінюванні практичних робіт враховуються наступні критерії:

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

Максимальна оцінка за кожну практичну роботу – 5 балів (Модуль 1) та 3 бали (Модуль 2). Максимальна сумарна кількість балів за практичні роботи за:

- Модулем 1 – $8 \times 5 = 40$ балів;
- Модулем 2 – $15 \times 3 = 45$ балів.

Критерії оцінювання практичних робіт

Кількість балів	Критерії оцінювання
5 (3)	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 (2)	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 (2)	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 (1)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1 (0)	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 за модуль – 85 балів (8 робіт по 5 балів та 15 робіт по 3 бали). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 1 балу.</i>

Для поточного модульного контролю студентами виконуються по 9 (дев'ять) модульних контрольних роботи за матеріалами змістовних модулів за Модулями. Максимальний бал за кожну МКР

- Модулем 1 – $4 \times 10 = 40$ балів;
- Модулем 2 – $5 \times 5 = 25$ балів

Загальна сума балів за модульні контрольні роботи: 65 балів.

Критерії оцінювання задач та практичних завдань в МКР

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Модуль 1, бал	10	9	8	7	6	5	4	3	2	1
Модуль 2, бал	5	4,5	4	3,5	3	2,5	2	1,5	1	0,5

Розподіл оцінки за змістовними модулями та видами контролю

Модуль 1	Вид роботи	Кількість балів
ЗМ 1	Практичні роботи 1,2	10
	МКР 1	10
ЗМ 2	Практичні роботи 3,4	10
	МКР 2	10
ЗМ 3	Практичні роботи 5,6	10
	МКР 3	10
ЗМ 4	Практичні роботи 7,8	10
	МКР 4	10
Конспект лекцій	Конспект	10
Залік	—	10
Сума		100

Модуль 2	Вид роботи	Кількість балів
ЗМ 5	Практичні роботи 9,10	6
	МКР 5	5
ЗМ 6	Практичні роботи 11 - 16	18
	МКР 6	5
ЗМ 7	Практичні роботи 17 - 19	9
	МКР 7	5
ЗМ 8	Практичні роботи 20 - 22	9
	МКР 8	5
ЗМ 9	Практична роботи 23	3
	МКР 9	5
Конспект лекцій	Конспект	10
Екзамен	—	20
Сума		100

**Рівні підсумкової оцінки екзамену з дисципліни
(перерахунковий коефіцієнт – 0,2)**

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)

8. 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).

9. Рекомендовані джерела інформації

Базові

1. *Блінцов В. С., Гальчевський Ю. Л.* Математичні основи криптології. – Миколаїв: НУК, 2006. – 232 с
2. *Самойленко Д. М.* Динамічна текстова стеганографія. – Миколаїв: НУК, 2016. – 68 с.
3. *Блінцов В.С., Гальчевський Ю.Л.* Практикум з криптології // Навч. посібник. – Миколаїв: НУК, 2005. – 172 с.
4. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. [Текст] / Горбенко І.Д., Горбенко Ю.І. – Харків: Форт. – 2012, –867 с.
5. *Шнайер Б.* Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Си ++ Applied Cryptography. Protocols, Algorithms and Source Code in C. — Триумф, 2002. — 816 с.
6. *Хорошко В.А.* Методи і засоби захисту інформації / В.А. Хорошко, А.А. Чекатков. – Юніор. – 2003. – 504 с.
7. *Ленков, С.В.* Методи і засоби захисту інформації. В.2-х томах / Ленков С.В., Перегудов., Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.: Арії, 2008. – Том І. Несанкціоноване отримання інформації. – 464 с.
8. *Андрєєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є.* Основи інформаційної безпеки: Підручник /за ред. проф. В.О. Хорошко — К.: Вид. ДУІКТ, 2009. — 292 с.
9. *Рибальський О.В., Хахановський В.Г., Кудінов В.А.* Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.
10. *Остапов С. Е.* Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
11. *Антонюк А.О.* Основи захисту інформації в автоматизованих системах: Навч. посібн. – К.: Видавн. дім. «КМ Академія», 2003. — 244 с.

Допоміжні

1. Указ Президента України. Про Положення про порядок здійснення криптографічного захисту інформації в Україні. Указ від 22.05.1998 № 505/98
2. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.
3. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення.

4. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення.
5. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) "Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел".
6. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) "Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні".
7. ДСТУ ISO/IEC 15946-5 :2019 (ISO/IEC 15946-5:2017) "Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих".
8. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри".
9. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри.
10. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потоків шифри
11. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) "Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел".
12. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC 9796-3:2006, IDT) "Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі".
13. ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення.
14. DigiScan EX 2.4. Інструкція користувача. – Copyright DigiScan-Labs, 2009. – 96 с.
15. Прийомо-контрольний прилад СА-6. Інструкція користувача. – Satel, 2010. – 20 с.
16. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
17. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.

18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

19. НД ТЗІ 1.4-002-08 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань.

20. НД ТЗІ 1.5-001-00 Радіовиявлювачі. Класифікація. Загальні положення.

21. НД ТЗІ 1.5-002-12 Класифікатор засобів технічного захисту інформації.

22. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

23. НД ТЗІ 1.6-005-13 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”

24. НД ТЗІ 2.3-001-01 Радіовиявлювачі вимірювальні. Методи та засоби випробувань.

25. НД ТЗІ 2.3-002-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.

26. НД ТЗІ 2.3-003-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.

27. НД ТЗІ 2.3-004-01 Радіовиявлювачі індикаторні. Методи та засоби випробувань.

28. НД ТЗІ 2.3-005-01 Радіовиявлювачі панорамні. Методи та засоби випробувань.

29. НД ТЗІ 2.3-006-01 Радіовиявлювачі аналізувальні. Методи та засоби випробувань.

30. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки «Методики виявлення закладних пристроїв».

31. НД ТЗІ 2.7-013-16 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99

32. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

33. НД ТЗІ 4.7-001-01 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.

Зміни та доповнення