

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 ОПІ
ПІ19



ЗАТВЕРДЖУЮ

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

С.О. Слободян

_____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Methods and Devices of Information Security

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

Робоча програма навчальної дисципліни «Метода і засоби захисту інформації» є однією із складових комплексної підготовки фахівців галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»

«__» _____ 2023 р. – с.

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

Проект робочої програми навчальної дисципліни «Метода і засоби 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 «Метода і засоби захисту інформації» розглянуто на засіданні кафедри КТІБ.

Протокол від «23» 06 2023 р. № 12.

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

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

Протокол від «30» 08 2023 р. № 1.

Голова, к.т.н., доц. _____ Д.О.Жук

Проект робочої програми навчальної дисципліни «Метода і засоби захисту інформації» погоджено з навчальним відділом.

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

Робочу програму навчальної дисципліни «Метода і засоби захисту інформації» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «7» 09 2023 р. № 6.

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.....	6
5. Програма навчальної дисципліни.....	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	18
7. Форми поточного та підсумкового контролю.....	18
8. Критерії оцінювання результатів навчання.....	20
9. Засоби навчання.....	22
10.Рекомендовані джерела інформації.....	23
Зміни та доповнення.....	26

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 злоумисниками, каналів витоку інформації, так і таких, що можуть бути спеціально створеними злоумисниками та передумовами функціонування таких каналів. Вивчення методів та засобів проведення спеціальних заходів для протидії злоумисникам 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 захисту інформації. Дисципліна є підготовчою для таких дисциплін як «Комплексні системи захисту інформації», «Захист аудіо- та відеоінформації» та «Моделювання об'єктів і процесів технічного захисту інформації».

Ключові слова: системи технічного захисту інформації, модель загроз, технічні канали витоку інформації, протидії витоку інформації.

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 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 at state and commercial enterprises, departments that specialize in providing information protection services. The course is preparatory to such subjects as "Integrated Information Security Systems", "Protection of Audio and Video Information" and "Modeling of objects and processes of technical information security".

Keywords: information protection systems, threat model, technical channel of information leakage, prevent information from leaking

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 6	Галузь знань 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації	Обов’язкова	
Модулів – 2	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 6		3–й та 4–й	2–й
Загальна кількість годин – 180		Семестр	
		6 та 7–й	3–й та 4–й
		Кількість годин	
		180	180
		Аудиторні:	
Тижневих годин для денної форми навчання: Аудиторних – 3; Самостійної роботи: – 3.	Рівень вищої освіти: перший (бакалаврський)	Лекції, год	
		30	12
		Лабораторні роботи, год	
		60	24
		Практичні заняття, год	
		–	–
		Самостійна робота, год	
		90	144
		Вид контролю: екзамен (6-й та 7-й семестри)	
Форма контролю: усна, письмова			

2. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни є отримання студентами необхідних знань щодо проявлення 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), алгоритмів розробки та реалізації заходів захисту, у тому числі і заходів захисту відомостей з обмеженим доступом (ВзОД), та формування у студентів відповідно до освітньої програми таких компетентностей:

- (ЗК2) Знання та розуміння предметної області та розуміння професії;
- (ЗК4) Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- (ЗК5) Здатність до пошуку, оброблення та аналізу інформації.
- (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.
- (ФК5) Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки
- (ФК7) Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- (ФК10) Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

3. Передумови для вивчення навчальної дисципліни

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

- Поля і хвилі в системах технічного захисту інформації;
- Безпека інформаційних та комунікаційних систем;
- Управління інформаційною безпекою;
- Електроніка та схемотехніка пристроїв технічного захисту інформації.

4. Очікувані результати навчання

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

– (PH4) 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;

– (PH12) Розробляти моделі загроз та порушника;

– (PH36) Виявляти небезпечні сигнали технічних засобів;

– (PH37) Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

– (PH48) Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Види, джерела та носії інформації, що підлягає захисту

Тема 1 Види, джерела та носії інформації, що підлягає захисту. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту [1] с.13-24

Тема 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. [1] с.24-97

Змістовий модуль 2. Технічні канали витоку інформації

Тема 3 Технічні канали витоку інформації: визначення, класифікація і структура технічних каналів витоку інформації. Основні способи і принципи роботи засобів спостереження за об'єктами в оптичному діапазоні. [1] с. 98-136, 161-164

Тема 4 Основні способи і принципи роботи засобів підслуховування та перехоплення сигналів в радіодіапазоні. [1] с.137-160, 165-168

Змістовий модуль 3. Принципи роботи засобів захисту інформації

Тема 5 Методи та принципи роботи засобів захисту інформації від спостереження в оптичному та радіотеплолокаційному каналах. [1] с.48-120

Тема 6 Методи та принципи роботи засобів захисту інформації від підслуховування в акустичному, вібраційному та гідроакустичному каналах. [2] с. 121-149

Тема 7 Методи та принципи роботи засобів захисту інформації від перехоплення в радіодіапазоні, каналам ПЕМВН та радіолокаційному каналі. [2] с.236-273

Тема 8 Активна радіоелектронна протидія засобам радіо і радіотехнічної розвідки. [2] с.274-306

Модуль 2

Змістовий модуль 4. Захист інформації що передається по відкритим телекомунікаційним лініям

Тема 9 Методи та засоби захисту акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям.

[1] с. 255-426; [2] с. 203-208, 274-306

Тема 10 Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами та технічними засобами. Скремблери 1, 2, 3 та 4 родів. [1] с. 427-435

Тема 11 Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодери, напіввокодери та ліпредери. [1] с. 436-471

Змістовий модуль 5. Інженерно-технічний захист інформації

Тема 12 Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що занесені в контрольовану зону (запису на диктофони та інші малогабаритні пристрої). [1] с. 129-130

Тема 13 Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші) [1] с. 130-150

Тема 14 Методи та засоби захисту акустичної інформації від перехоплення засобами ВЧ-збудження акустoeлектричних перетворювачів, ВЧ-накачування та ПЕМВН. [1] с. 150-180

Змістовий модуль 6. Контроль ефективності технічного захисту інформації

Тема 15 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. [1] с. 320-381

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.
1	2	3	4	6	7	8	9	11
Модуль 1 (М1)								
Змістовий модуль 1. Види, джерела та носії інформації, що підлягає захисту								
Тема 1. Види, джерела та носії інформації, що підлягає захисту. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту.	7	2	0	5	15	2	0	6
Тема 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.	8	2	0	6				7
Разом за змістовим модулем 1	15	4	0	11	15	2	0	13
Змістовий модуль 2. Технічні канали витоку інформації								
Тема 3. Технічні канали витоку інформації: визначення, класифікація і структура технічних каналів витоку інформації. Основні способи і принципи роботи засобів спостереження за об'єктами в оптичному діапазоні	15	2	4	9	30	2	4	12

Тема 4. Основні способи і принципи роботи засобів підслуховування та перехоплення сигналів в радіодіапазоні	15	2	4	9				12
Разом за змістовим модулем 2	30	4	8	18	30	2	4	24
Змістовий модуль 3. Принципи роботи засобів захисту інформації								
Тема 5. Методи та принципи роботи засобів захисту інформації від спостереження в оптичному та радіотеплолокаційному каналах	12	2	6	4	45	2	8	9
Тема 6. Методи та принципи роботи засобів захисту інформації від підслуховування в акустичному, вібраційному та гідроакустичному каналах	12	2	6	4				9
Тема 7. Методи та принципи роботи засобів захисту інформації від перехоплення в радіодіапазоні, каналам ПЕМВН та радіолокаційному каналі	12	2	6	4				9
Тема 8. Активна радіоелектронна протидія засобам радіо і радіотехнічної розвідки	9	1	4	4				8
Разом за змістовим модулем 3	45	7	22	16	45	2	8	35
Разом за модулем 1	90	15	30	45	90	6	12	72

Модуль 2								
Змістовий модуль 4. Захист інформації що передається по відкритим телекомунікаційним лініям								
Тема 9. Методи та засоби захисту акустичної (мовної) конфіденційної інформації, що передається по відкритим телекомунікаційним лініям	10	2	0	8	30	2	2	9

Тема 10. 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				8
Тема 11. Методи та засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям технічними засобами. Вокодери, напіввокодери та ліпредери	10	2	0	8				9
Разом за змістовим модулем 4	30	6	4	20	30	2	2	26
Змістовий модуль 5. Інженерно-технічний захист інформації								
Тема 12. 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				11
Тема 13. Методи та засоби захисту акустичної інформації від перехоплення ТЗР, що знаходяться за межами контрольованої зони (стетоскопи, спрямовані та лазерні мікрофони та інші)	14	2	8	4	45	2	10	11
Тема 14. Методи та засоби захисту акустичної інформації від перехоплення засобами ВЧ-збудження акустоелектричних перетворювачів, ВЧ-накачування та ПЕМВН	21	2	14	5				11
Разом за змістовим модулем 5	45	6	26	13	45	2	10	33

Змістовий модуль 6. Контроль ефективності технічного захисту інформації								
Тема 15. 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	1	0	14	15	2	0	13
Разом за змістовим модулем 6	15	1	0	14	15	2	0	13
Разом за модулем 2	90	15	30	45	90	6	12	72
Усього годин	180	30	60	90	180	12	24	144

Примітка. Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до таблиці (розд. 4).

ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	Дослідження структури, способів і принципів роботи засобів спостереження за об'єктами в оптичному діапазоні (системи телеспостереження)	6
2	Дослідження способів і принципів роботи засобів спостереження (радіомоніторингу) за сигналами в радіоефірі з використанням ресивера ICR-1500	6
3	Дослідження способів і принципів роботи засобів підслуховування за допомогою направленої мікрофону органного типу	4
4	Дослідження способів і принципів роботи засобів контролю рівня ПЕМВН (компрометуючого випромінювання) елементів та блоків ПЕОМ та засобів оргтехніки	6
5	Активна радіоелектронна протидія засобам радіо і радіотехнічної розвідки	4
6	Дослідження лінгвістичних способів захисту конфіденційної інформації в відкритих телекомунікаційних мережах та принципів роботи скремблерів 1, 2, 3 та 4 родів	6
7	Дослідження способів і принципів роботи засобів захисту ліній зв'язку від витоку конфіденційної інформації	4
8	Дослідження способів і принципів роботи засобів захисту акустичної інформації від перехоплення дистанційними засобами та методами	6
9	Апаратура для пошуку пристроїв несанкціонованого доступу до конфіденційної аудіоінформації. Індикатори поля	4
10	Методи та засоби пошуку електронно-технічних пристроїв несанкціонованого доступу до конфіденційної інформації за допомогою металодетектору	4
11	Дослідження структури, способів і принципів роботи охоронно-пожежної системи спостереження на об'єкті	6
12	Дослідження способів і принципів роботи засобів захисту акустичної інформації від витоку за межі контрольованої зони по конструкційним елементам	4
	Разом	60

Теми практичних занять

Практичні 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	
		Денна форма навчання	Заочна форма навчання
1	Модуль 1 До теми 1. Види інформації, що захищається технічними засобами, її властивості. Демаскуючі ознаки об'єктів захисту.	5	6
2	До теми 2. Принципи запису і знімання інформації з носіїв. Принципи добування і обробки інформації технічними засобами.	6	7
3	До теми 3. Технічні канали витоку інформації: визначення, класифікація і структура технічних каналів витоку інформації	9	12
4	До теми 4. Основні способи і принципи роботи засобів спостереження за об'єктами в оптичному діапазоні	9	12
5	До теми 5. Основні способи і принципи роботи засобів підслуховування	4	9
6	До теми 6. Основні способи і принципи роботи засобів перехоплення сигналів в радіодіапазоні	4	9
7	До теми 7. Заходи і принципи роботи засобів захисту інформації від спостереження в оптичному каналі.	4	9
8	До теми 8. Способи і принципи роботи засобів захисту інформації від підслуховування	4	8

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
	Модуль 2		
9	До теми 9. Способи і принципи роботи засобів захисту інформації від перехоплення в радіодіапазоні та по каналах ПЕМВН	8	9
10	До теми 10. Способи і принципи роботи засобів захисту інформації від спостереження в радіолокаційному та гідроакустичному каналах	4	8
11	До теми 11. Активна радіоелектронна протидія засобам радіо і радіотехнічної розвідки	8	9
12	До теми 12. Способи і засоби захисту акустичної інформації, що передається по відкритим телекомунікаційним лініям інформаційними методами	4	11
13	До теми 13. Способи і засоби захисту інформації в лініях зв'язку. Скремблери 1, 2, 3 та 4 родів	4	11
14	До теми 14. Способи і засоби захисту інформації в лініях зв'язку. Вокодери, напіввокодери та ліпредери	5	11
15	До теми 15. Способи захисту ліній зв'язку установ і підприємств державних і комерційних структур від витоку конфіденційної інформації	14	13
Разом		90	144

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 – 0,4 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 0,4 год. / 1 год. занять;
- підготовка до лабораторних робіт – 1,0 год. / 1 год. занять;
- підготовка до контрольних заходів – 1,0 год. на 1 захід.

Заочна форма навчання

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 2,5 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 5 год. / 1 год. занять;
- підготовка до лабораторних робіт – 2 год. / 1 год. заняття;
- підготовка до контрольних заходів – 3 год. на 1 захід.

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	6	15
2	Самостійне опрацювання окремих тем навчальної дисципліни	6	30
3	Підготовка до лабораторних робіт	30	24
4	Підготовка до модульних контрольних робіт	3	3
<i>Усього годин за модуль 1</i>		45	72
1	Підготовка до лекцій	6	15
2	Самостійне опрацювання окремих тем навчальної дисципліни	6	30
3	Підготовка до лабораторних робіт	30	24
4	Підготовка до модульних контрольних робіт	3	3
<i>Усього годин за модулем 2</i>		45	72
<i>Разом за курсом</i>		90	144

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 проєкти; 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.

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 за Модуль - $6 \times 5 = 30$ 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 – 50 балів (10 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 по 3(три) модульні контрольні роботи за матеріалами змістовних модулів. Максимальний бал за кожну МКР – 10 балів. Загальна сума балів за модульні контрольні роботи для кожного модуля – $10 \times 3 = 30$ балів.

За заочною формою навчання в кінці кожного семестру виконується підсумкова залікова робота. Максимальна оцінка за підсумкову залікову роботу – 30 балів.

Критерії оцінювання задач та практичних завдань в МКР

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

Розподіл оцінки за змістовними модулями та видами контролю

Модуль 1	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 1	МКР 1	10		
ЗМ 2	Лабораторні роботи	10	Лабораторні роботи	5
	МКР 2	10	–	–
ЗМ 3	Лабораторні роботи	20	Лабораторні роботи	25
	МКР 3	10	–	–
КР	–	–	Контрольна робота	30
Конспект лекцій	Конспект	10	Конспект	10
Екзамен	-	30	-	30
Сума		100		100
Модуль 2	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 4	МКР 1	10		
	Лабораторні роботи	5	Лабораторні роботи	10
ЗМ 5	Лабораторні роботи	25	Лабораторні роботи	20
	МКР 2	10	–	–
ЗМ 6	МКР 3	10		
КР	–	–	Контрольна робота	30
Конспект лекцій	Конспект	10	Конспект	10
Екзамен	-	30	-	30
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

1. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Юниор. – 2003. – 504 с
2. *Хорошко, В.О.* Пошук та локалізація радіо закладних пристроїв. Навчальний посібник / В.О. Хорошко, О.Д. Азаров, Г.О. Максименко, Ю.Є. Яремчук, Під ред. В.О. Хорошко. – Вінниця: ВНТУ, 2007. – 333 с.
3. *Ленков, С.В.* Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов., Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с.
4. 3. *Ленков, С.В.* Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов., Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. – 344 с.
5. *Андреев 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.
6. *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.
7. *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.)
8. *Антонюк А.О.* Основи захисту інформації в автоматизованих системах: Навч. посібн. – К.: Видавн. дім. «КМ Академія», 2003. — 244 с.

Допоміжні

1. *Нужний, С.М.* Захист інформації від витоку по технічним каналам. Частина I: Метод. вказівки до лабор. робіт. / С.М. Нужний, Під ред. проф. В.С. Блінцова. – Миколаїв: НУК, 2008. – 33 с.

2. *Нужний, С.М.* Техніка захисту аудіоінформації. Частина 1. Пристрої аналогового шифрування. Скремблери: Метод. вказівки до лабор. робіт. / С.М. Нужний, Д.В. Портний, Під ред. проф. В.С. Блінцова. – Миколаїв: НУК, 2008. – 33 с.
3. DigiScan EX 2.4. Руководство пользователя. – Copyright DigiScan-Labs, 2009. – 96 с.
4. Приемо-контрольный прибор СА-6. Руководство пользователя. – Satel, 2010. – 20 с.
5. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
6. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.4-002-08 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань.
9. НД ТЗІ 1.5-001-00 Радіовиявлювачі. Класифікація. Загальні положення.
10. НД ТЗІ 1.5-002-12 Класифікатор засобів технічного захисту інформації.
11. 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.
12. 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”
13. НД ТЗІ 2.3-001-01 Радіовиявлювачі вимірювальні. Методи та засоби випробувань.

14. 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.

15. 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.

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

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

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

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

20. 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

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

22. 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