НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
02 червня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "Проектування, впровадження, супровід комплексних систем захисту інформації" (частина ІІ)

Галузь знань F – Інформаційні технології
Спеціальність F5 – «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека та захист інформаці»
Факультет (ННІ) Інформаційних технологій
Розробник: доцент, к.т.н., доцент Кулініч О.М.

Київ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій

_____ проф. І.М. Болбот
"____" _____ 2025 р.

"**СХВАЛЕНО**"
на засіданні кафедри комп'ютерних систем, мереж та кібербезпеки
Протокол № 9 від 26.05.2025 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

"**РОЗГЛЯНУТО** "
Гарант ОП «Кібербезпека та захист інформаці»
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Проектування, впровадження, супровід комплексних систем захисту інформації " (частина ІІ)

Галузь знань F – Інформаційні технології
Спеціальність F5 – «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека та захист інформаці»
Факультет (ННІ) Інформаційних технологій
Розробник: доцент, к.т.н., доцент Кулініч О.М.

Київ – 2025

1. Опис навчальної дисципліни

«Проектування, впровадження, супровід комплексних систем захисту інформації»

Навчальна дисципліна "Проектування, впровадження, супровід комплексних систем захисту інформації" спрямована на формування у студентів знань про теоретичні та практичні методи забезпечення захисту інформації. Вивчаються сучасні підходи до вибору методів захисту інформації. Курс є фундаментальною основою для підготовки здобувачів вищої освіти до самостійної практичної роботи.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Галузь знань	F – Інформаційні технології	
Спеціальність	F5 – Кібербезпека та захист інформації	
Освітня програма	«Кібербезпека та захист інформації»	
Характеристика навчальної дисципліни		
Вид	обов’язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	30	
Форма контролю	*екзамен*	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2025-2026	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	30	
Індивідуальні завдання	30	
Кількість тижневих аудиторних годин для денної форми навчання	4	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу, знайомство з базовими організаційними заходами для комплексних систем захисту інформації, а також інженерно-технічними заходами, засвоєння функціональних можливостей та методів побудови комплексних систем захисту інформації, опановування необхідними прийомами та практичними навичками при налаштуванні та конфігуруванні сучасного мережевого обладнання.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів до застосування методів побудови комплексних систем захисту інформації, навичок при налаштуванні та конфігуруванні сучасного мережевого обладнання.

В результаті вивчення навчальної дисципліни студент повинен

- **знати:** основні поняття та принципи побудови комплексної системи захисту інформації; нормативно – правову базу, що регулює етапи побудови, аудиту та впровадження КСЗІ; методики визначення об'єктів КСЗІ, їх класифікації та оцінки джерел дестабілізуючого впливу; принципи класифікації інформації, що підлягає захисту в КСЗІ підприємств та організацій різної форми власності; механізми та методи забезпечення організаційної, криптографічної, інженерно-технічної складових КСЗІ; методологію розробки та складанні моделей порушника та моделі загроз з врахуванням особливостей протікання бізнес-процесів на підприємстві чи організації; етапи проектування, розробки та підтримки КСЗІ та принципи сертифікації створюваних систем захисті інформації; принципи розробки політики безпека підприємства або організації різних форм власності.
- **вміти:** вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання; готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки; проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; вирішувати задачі захисту потоків даних в інформаційних, інформаційнотелекомунікаційних (автоматизованих) системах; визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах. **Набуття компетентностей:**

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями..

Спеціальні (фахові, предметні) компетентності (СК):

СК1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (ПРН), а саме

ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

ПРН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмноапаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

ПРН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

ПРН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу «Комплексні системи захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Комплексні системи захисту інформації» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю F5 «Кібербезпека та захист інформації»;
- навчальний план підготовки фахівців за спеціальністю F5 «Кібербезпека та захист інформації».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Комплексні системи захисту інформації» є курси «Організаційне забезпечення захисту інформації» та «Інформаційна безпека держави».

Курс «Проектування, впровадження, супровід комплексних системи захисту інформації» є базовим для вивчення наступної дисципліни: «Безпека інформації в інформаційно-комунікаційних системах».

2. Програма та структура навчальної дисципліни – повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Порядок проведення робіт із визначення можливих каналів витоку інформації.													
Тема 1. Нормативнометодичне забезпечення з питань побудови КТЗІ.	1	8	2		2		4						
Тема 2. Формування загальних вимог до КТЗІ.	2	8	2		2		4						
Тема 3. Поняття моделі загроз та моделі порушника. ..	3	8	2		2		4						
Тема 4. Технічні канали просочування інформації. Класифікація, причини і джерела утворення	4	8	2		2		4						
Тема 5. Акустичні канали витоку інформації	5	8	2		2		4						
Тема 6. Параметричні канали витоку інформації, їх класифікація.	6	8	2		2		4						
Тема 7. Оптичні, оптоелектронні та електромагнітні канали витоку інформації.	7	8	2		2		4						

Разом за змістовим модулем 1		**56**	**14**		**14**		**28**						
Змістовий модуль 2. Порядок проведення робіт зі створення комплексу технічного захисту інформації.													
Тема 1. Методи та засоби захисту акустичної інформації	8	8	2		2		4						
Тема 2. Активні методи і засоби захисту від витоку технічними каналами	9	8	2		2		4						
Тема 3. Пасивні методи і засоби захисту від витоку технічними каналами	10	8	2		2		4						
Тема 4. Закладні пристрої та методика їх виявлення	11	8	2		2		4						
Тема 5. Методи та засоби виявлення закладних пристроїв.	12	8	2		2		4						
Тема 6. Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації	13	8	2		2		4						
Тема 7. Порядок розробки ТЗ та паспорту на КТЗІ	14	8	2		2		4						
Тема 8. Експертиза комплексу технічного захисту інформації.	15	8	2		2		4						
Разом за змістовим модулем 2		**64**	**16**		**16**		**32**						
Всього годин		**120**	**30**		**30**		**60**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Нормативнометодичне забезпечення з питань побудови КТЗІ.	2
2	Формування загальних вимог до КТЗІ.	2
3	Поняття моделі загроз та моделі порушника.	2
4	Технічні канали просочування інформації. Класифікація, причини і джерела утворення	2
5	Акустичні канали витоку інформації	2
6	Параметричні канали витоку інформації, їх класифікація.	2
7	Оптичні, оптоелектронні та електромагнітні канали витоку інформації.	2
8	Методи та засоби захисту акустичної інформації	2
9	Активні методи і засоби захисту від витоку технічними каналами	2
10	Пасивні методи і засоби захисту від витоку технічними каналами	2
11	Закладні пристрої та методика їх виявлення	2
12	Методи та засоби виявлення закладних пристроїв	2
13	Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації	2
14	Порядок розробки ТЗ та паспорту на КТЗІ	2
15	Експертиза комплексу технічного захисту інформації.	2
	Разом	**30**

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Аналіз нормативно-методичного забезпечення з питань створення КТЗІ	2
2	Розроблення Акту обстеження ІТС	2
3	Розроблення моделі загроз інформації в ІТС	2
4	Розроблення моделі порушника властивостей інформації в ІТС	2
5	Розрахунок модель каналу витоку інформації	4
6	Розрахунок ослаблення радіохвиль на шляху розповсюдження у міських умовах	4
7	Дослідження комплектів для виявлення акустичних каналів витоку інформації	2
8	Дослідження багатофункціональних комплектів для виявлення віброакустичних каналів витоку інформації	2
9	Розрахунок акустичного каналу витоку інформації	4
10	Дослідження індикаторів електромагнітного поля, радіоприймачів сканування, аналізаторів спектру та частотомірів.	2
11	Розроблення вимог до КСЗІ в частині реалізації критеріїв гарантій	2
12	Розроблення програми та методики попередніх випробувань комплексу засобів захисту інформації	2
	Всього	**30**

Завдання на курсові роботи:

1. Принципи формування, характеристика, параметри та особливості розповсюдження електромагнітних хвиль.
2. Принципи формування, характеристика, параметри та особливості розповсюдження акустичних коливань.
3. Принцип високочастотного нав'язування та принципи формування відбитого сигналу.
4. Принципи та засоби пошуку та виявлення закладних пристроїв.
5. Методи захисту об'єктів інформаційної діяльності від витоку інформації різними каналами.
6. Принципи побудови та функціонування генераторів шуму в акустичному та високочастотному діапазонах.
7. Використання та налаштування систем IDS/IPS.
8. Описати порядок встановлення, використання та налаштування систем MARS Cisco.
9. Описати порядок встановлення та налаштування систем CSA.
10. Принципи виявлення мережевих атак на основі нечіткої логіки.
11. Принципи побудови та функціонування систем RBAC (Role-Based Access Control) і Okta.
12. Принципи побудови та функціонування експертних систем.
13. Принципи побудови, функціонування та налащтування систем RAID 10 і RAID 5.
14. Принципи побудови та використання Windows SCCM.

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

- систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;
- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;
- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Етапи створення КТЗІ.	3
2	Формування загальних вимог до КТЗІ.	3
3	Обґрунтування необхідності створення КТЗІ.	3
4	Порядок обстеження середовищ функціонування ОІД.	3
5	Формування завдання на створення КТЗІ.	3
6	Порядок розробки політики безпеки інформації.	3
7	Вибір варіанту КТЗІ.	3
8	Порядок розробки плану захисту інформації.	3
9	Порядок розробки технічного завдання на створення КТЗІ.	3
10	Порядок розробки проекту КТСЗІ.	3
	Разом	**30**

5. Засоби діагностики результатів навчання:
- екзамен;
- модульні тести;
- захист та лабораторних робіт.

6. Методи навчання:
- словесний метод (лекція, дискусія, співбесіда тощо);
- практичний метод;
- наочний метод (метод ілюстрацій, метод демонстрацій);
- робота з навчально-методичною літературою;
- відеометод (дистанційні, мультимедійні, веб-орієнтовані тощо);
- самостійна робота (виконання завдань).

7. Методи оцінювання.
- екзамен;
- захист практичних робіт;
- презентації та виступи на наукових заходах.

8. **Оцінювання результатів навчання.**

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Модуль 1. Порядок проведення робіт із створення комплексної системи захисту інформації.		
Лекція 1.	ПРН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	-
Лабораторна/практична робота 1.		**5**
Самостійна робота *(за наявності)* 1.		-
Лекція 2.		-
Лабораторна/практична робота 2.		**10**
Самостійна робота *(за наявності)* 2.		**5**

Лекція 3.	ПРН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. ПРН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	**-**
Лабораторна/практична робота 3.		**10**
Самостійна робота 3.		**5**
Лекція 4.		**-**
Лабораторна/практична робота 4.		**10**
Самостійна робота 4.		**5**
Лекція 5.		**-**
Лабораторна/практична робота 5.		**10**
Самостійна робота		**5**
Лекція 6.		**-**
Лабораторна/практична робота 6.		**10**
Самостійна робота		**5**
Лекція 7.		**-**
Самостійна робота		**5**
Модульна контрольна робота 1.		**20**
Всього за модулем 1		**100**
Модуль 2. Способи організації процесу моделювання.		
Лекція 8		**-**
Лабораторна/практична робота 7.	ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН14. Вирішувати задачі управляння процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. ПРН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	**5**
Самостійна робота 7.		**10**
Лекція 9.		**-**
Лабораторна/практична робота 8.		**5**
Самостійна робота 8.		**10**
Лекція 10.		**-**
Лабораторна/практична робота 9.		**5**
Самостійна робота 9.		**10**
Лекція 11.		**-**
Лабораторна/практична робота 10.		**5**
Самостійна робота 10.		**10**
Лекція 12.		**-**
Лабораторна/практична робота 11.		**-**
Самостійна робота 11.		**10**
Лекція 13.		**-**
Лабораторна/практична робота 12.		**-**
Самостійна робота 12.		**10**
Лекція 14.		**-**
Самостійна робота 13.		**10**
Модульна контрольна робота 2.		**10**
Всього за модулем 2		**100**
Навчальна робота		**(М1 + М2)/2*0,7 ≤ 70**

Екзамен/залік	**30**
Всього за курс	**(Навчальна робота + екзамен) ≤ 100**

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. Політика оцінювання

Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Реферати повинні мати коректні текстові посилання на використану літературу
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканом факультету)

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

9. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle https://elearn.nubip.edu.ua/course/view.php?id=4162 вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

10. Рекомендована література

Основна:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.
2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.
4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с

Допоміжна

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835