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 «Програмно-технічні засоби захисту інформації»

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – «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
" Програмно-технічні засоби захисту інформації "

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека та захист інформації»
Факультет (ННІ) Інформаційних технологій
Розробник: доцент, к.т.н., доцент Кулініч О.М.

Київ – 2025

1. Опис навчальної дисципліни

«Програмно-технічні засоби захисту інформації»

Навчальна дисципліна "Програмно-технічні засоби 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	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека та захист інформації	
Освітня програма	«Кібербезпека та захист інформації»	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	90	
Кількість кредитів ECTS	3	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
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	-	
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 системи захисту інформації; нормативно – правову базу, що регулює етапи побудови, систем захисту, їх класифікації та оцінки джерел дестабілізуючого впливу; принципи класифікації інформації, що підлягає захисту в організацій різної форми власності; механізми та методи забезпечення організаційної, криптографічної, інженерно-технічної складових; методологію розробки та складанні моделей порушника та моделі загроз з врахуванням особливостей протікання бізнес-процесів на підприємстві чи організації; етапи проектування, розробки та підтримки та принципи сертифікації створюваних систем захисті інформації; принципи розробки політики безпека підприємства або організації різних форм власності.
- **вміти:** вирішувати задачі супроводу та впровадження 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 F5 «Кібербезпека та захист інформації» 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.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.**Спеціальні (фахові, предметні) компетентності (СК):**

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.

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

СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

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

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.

ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

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.

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.

ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

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.

ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

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 «Програмно-технічні засоби захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Програмно-технічні засоби захисту інформації» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека та захист інформації»;
- навчальний план підготовки фахівців за спеціальністю 125 «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 «Програмно-технічні засоби 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. Сучасна елементна база для побудови засобів захисту													

Тема 1. Принципи побудови елементів послідовної та комбінаційної логіки.	1	6	2		2		2						
Тема 2. Структура та функціонування шифраторів та дешифраторів.	2	6	2		2		2						
Тема 3. Принципи створення мультиплексорів та де мультиплексорів.	3	6	2		2		2						
Тема 4. Основа для побудови ЗЗІ – програмуємі логічні матриці.	4	6	2		2		2						
Тема 5. Схемотехніка та функціонування ПМЛ	5	6	2		2		2						
Тема 6. Різновиди схемотехнічних рішень засобів захисту інформації.	6	6	2		2		2						
Тема 7. Принципи периферійного сканування та програмування ПЛМ.	7	6	2		2		2						
Разом за змістовим модулем 1		**42**	**14**		**14**		**14**						
Змістовий модуль 2. Принципи створення засобів захисту інформації.													
Тема 1. Методи та засоби побудови засобів інформації.	8	6	2		2		2						
Тема 2. Принципи побудови регістрових систем захисту інформації	9	6	2		2		2						
Тема 3. Ситеми захисту інформації побудовані на використанні методів гамування	10	6	2		2		2						

Тема 4. Принципи використання лічильнків та дільників частоти в схемах захисту інформації.	11	6	2		2		2						
Тема 5. Методи та засоби генерації імпульсів для систем ЗЗІ.	12	6	2		2		2						
Тема 6. Порядок проведення робіт зі створення та атестації засобів захисту інформації.	13	6	2		2		2						
Тема 7. Порядок розробки ТЗ на засіб захисту інформації.	14	6	2		2		2						
Тема 8. Експертиза та ліцензування засобів захисту інформації.	15	6	2		2		2						
Разом за змістовим модулем 2		**48**	**16**		**16**		**16**						
Всього годин		**90**	**30**		**30**		**30**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Принципи побудови елементів послідовної та комбінаційної логіки.	2
2	Принципи побудови елементів послідовної та комбінаційної логіки	2
3	Принципи створення мультиплексорів та де мультиплексорів.	2
4	Основа для побудови ЗЗІ – програмуємі логічні матриці.	2
5	Схемотехніка та функціонування ПМЛ	2
6	Різновиди схемотехнічних рішень засобів захисту інформації.	2
7	Принципи периферійного сканування та програмування ПЛМ.	2
8	Методи та засоби побудови засобів інформації.	2
9	Принципи побудови регістрових систем захисту інформації	2
10	Ситеми захисту інформації побудовані на використанні методів гамування	2

11	Принципи використання лічильнків та дільників часеоти в схемах захисту інформації.	2
12	Методи та засоби генерації імпульсів для систем ЗЗІ.	2
13	Порядок проведення робіт зі створення та атестації засобів захисту інформації.	2
14	Порядок розробки ТЗ на засіб захисту інформації.	2
15	Експертиза та ліцензування засобів 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 систем захисту інформації.	2
2	Дослідження принципу роботи шифраторів.	2
3	Дослідження принципу роботи дешифраторів.	2
4	Дослідження принципу роботи мультиплексорів.	2
5	Дослідження принципу роботи демультиплексорів.	4
6	Розрахунок схем роботи суматорів.	4
7	Принципи побудови схем компараторів.	2
8	Дослідження роботи тригерних пристроїв.	2
9	Принципи функціонування регістрових схем.	4
10	Принципи побудови та функціонування лічильників.	2
11	Принципи побудови та функціонування дільників частоти.	2
12	Принципи побудови та функціонування засобів захисту інформації.	2
	Всього	**30**

Курсова робота не передбачена.

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.

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Порядок розробки технічного завдання на створення ЗЗІ.	3
2	Порядок розробки проекту ЗЗІ.	3
3	Сутність технічного проекту ЗЗІ	3
4	Порядок проведення дослідної експлуатації ЗЗІ.	3
5	Порядок проведення державної експертизи ЗЗІ	3
6	Порядок розробки політики безпеки інформації в ІТС.	3
7	Принципи побудови та функціонування генераторів шуму.	4
8	Принципи побудови та функціонування генераторів гамуючих послідовностей.	4
9	Принципи побудови та функціонування систем синхронізації.	4
	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.	ПРН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	-
Лабораторна/практична робота 1.		**5**
Самостійна робота *(за наявності)* 1.		-
Лекція 2.		-
Лабораторна/практична робота 2.		**10**

Самостійна робота *(за наявності)* 2.	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. 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. ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	**5**
Лекція 3.		**-**
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. 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. ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. 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	**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**

	загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
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. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

- на лабораторних роботах шляхом перевірки підготовки до

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

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): $R_{дис}=R_{НР}+R_{АТ}$.

8.1. 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)

9. Навчально-методичне забезпечення

1. Електронний навчальний курс на платформі Moodle https://elearn.nubip.edu.ua/course/view.php?id=4943 вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

10. Рекомендована література

Основна:

1. Схемотехніка електронних систем: У 3 кн. Кн. 1. Аналогова схемотехніка та імпульсні пристроі: Підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та ін. — 2-ге вид., допов. і переробл. — К.: Вища шк., 2004. - 336 с.: іл.

2.Схемотехніка електронних систем: У 3 кн. Кн. 2. Цифрова схемотехніка: Підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та ін. — 2-ге вид., допов. і переробл. — К.: Вища шк., 2004. - 423 с.: іл.

3. Схемотехніка електронних систем: У 3 кн. Кн. 3. Мікропроцесори та мікроконтролери: Підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та ін. — 2-ге вид., допов. і переробл. — К.: Вища шк., 2004. - 399 с.: іл.

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

http://moodle.fit.knu.ua/ - Модульне об'єктно-орієнтоване динамічне навчальне середовище Moodle Київського національного університету імені Тараса Шевченка.

https://ru.coursera.org/ - проект в сфері масової онлайн-освіти.

prometheus.org.ua - український громадський проект масових відкритих онлайн-курсів.