МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Технічні засоби захисту інформації»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	4	7	40	38	5	12	85	180	Екзамен (7)

30.08.2024

Тернопіль – 2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека, затвердженої Вченою радою ЗУНУ (протокол № 9 від 26.05.2021 р.).

Робочу програму склали: завідувач кафедри кібербезпеки, д.т.н., професор Василь ЯЦКІВ та старший викладач кафедри кібербезпеки, доктор філософії (спеціальність 125 - Кібербезпека та захист інформації) Сергій КУЛИНА.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №1 від 30 серпня 2024 р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Технічні засоби захисту інформації»

1. Опис дисципліни «Технічні засоби захисту інформації»

Дисципліна – «Технічні засоби захисту інформації»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 6	Галузь знань – 12 «Інформаційні технології»	Статус дисципліни – обов'язкова Мова навчання – українська
Кількість залікових модулів – 5	Спеціальність – 125 «Кібербезпека»	Рік підготовки: Денна – 4. Семестр: Денна – 7.
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції (год): Денна – 40. Лабораторні заняття (год): Денна – 38.
Загальна кількість годин – 180		Самостійна робота (год): 85. Тренінг (год): 12. Індивідуальна робота (год): 5.
Тижневих годин – 12, з них аудиторних – 6		Вид підсумкового контролю – екзамен.

2. Мета і завдання дисципліни «Технічні засоби захисту інформації»

2.1. Мета вивчення дисципліни

Мета дисципліни «Технічні засоби захисту інформації» полягає в систематизації інформації щодо розроблення, впровадження та експлуатації систем технічного захисту інформації на об'єктах інформаційної діяльності.

2.2. Завдання вивчення дисципліни

Завдання дисципліни полягає в отриманні студентами необхідних знань щодо проявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності.

2.3. Перелік компетентностей, формування котрих забезпечує вивчення дисципліни:

Здатність застосовувати знання у практичних ситуаціях.

Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

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

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

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Технічні засоби захисту інформації» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Фізика», «Комп'ютерні мережі», «Архітектура комп'ютерів та систем», «Кібернетична безпека», «Оцінка та управління ризиками»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.5. Результати навчання

Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень.

Використовувати сучасне програмно-апаратне забезпечення інформаційно комунікаційних технологій.

Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем.

Виявляти та вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.

3. Зміст дисципліни «Технічні засоби захисту інформації»

Змістовий модуль 1. Елементи інформаційної системи, що підлягають захисту

Тема 1. Види, джерела та носії інформації, що підлягають захисту

Властивості інформації як об’єкта захисту. Поняття цінності та ціни інформації. Складові ціни інформації. Види, джерела та носії інформації, що підлягає захисту. Класифікація демаскуючих ознак об’єктів захисту. Демаскуючі ознаки сигналів.

Тема 2. Небезпечні сигнали та їх джерела

Поняття небезпечного сигналу. Види побічних небезпечних електромагнітних випромінювань. Небезпечні сигнали, що утворюються в результаті акустоелектичних перетворень. Паразитні зв’язки та наведення. Низько- та високочастотні випромінювання

Тема 3. Технічна розвідка

Поняття та принципи технічної розвідки. Основні задачі та ограни технічної розвідки. Види технічної розвідки. Поняття промислового шпигунства. Законні та незаконні методи добування конфіденційної інформації про діяльність конкурентів. Контррозвідувальна діяльність. Комплексний захист конфіденційної інформації, його види. Пасивні та активні методи захисту конфіденційної інформації.

Тема 4. Концепція і методи технічного захисту інформації

Комплексне застосування методів захисту. Основні напрямки інженерно-технічного захисту інформації. Методи фізичного захисту інформації. Просторове та структурне приховування інформації. Часове та енергетичне приховування інформації. Поняття інформаційного портрету та інформаційного вузла об’єктів захисту. Дезінформація, як метод захисту інформації.

Змістовий модуль 2. Технічні канали витоку інформації

Тема 5. Технічні канали витоку інформації

Поняття витоку інформації та технічного каналу витоку інформації. Структура та характеристики технічного каналу витоку інформації. Класифікація технічних каналів витоку інформації. Характеристика та можливості оптичних, радіоелектичних, акустичних та матеріально-речових каналів витоку інформації.

Тема 6. Електричні канали витоку інформації

Канал побічних електромагнітних випромінювань ОТЗС. Канал побічних електромагнітних випромінювань ДТЗС. Канал «паразитної» модуляції сигналів ВЧ генераторів. Канал «паразитної» ВЧ генерації підсилювачів. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС. Канал побічних електромагнітних наведень на комунікації ДТЗС. Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).

Тема 7. Радіоелектронні канали витоку інформації

Особливості радіоелектронних каналів витоку інформації. Структура радіоелектронного каналу витоку інформації. Види витоку інформації через радіоелектронні канали. Класифікація перешкод.

Тема 8. Акустичні та віброакустичні канали витоку інформації

Фізичні основи акустичних каналів витоку інформації. Шляхи витоку акустичної інформації. Віброакустичні канали. Акустоелектричні канали. Оптико-електронний (лазерний) канал. Параметричні канали.

Тема 9. Технічні канали витоку інформації на основі закладних пристроїв

Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв). Загальні характеристики та особливості деяких типів закладних пристроїв. Заходи захисту інформації від витоку каналами на основі закладних пристроїв

Змістовий модуль 3. Запобігання витоку інформації

Тема 10. Методи та засоби захисту від спостереження та підслуховування

Засоби протидії спостереженню в оптичному діапазоні та радіолокаційному спостереженню. Енергетичне приховування акустичного сигналу. Засоби звукоізоляції та звукопоглинання. Класифікація засобів виявлення та локалізації закладних пристроїв. Методи та засоби виявлення випромінювання закладних пристроїв. Методи та засоби виявлення не випромінюючих закладних пристроїв.

Тема 11. Засоби запобігання витоку інформації через побічні електромагнітні випромінювання

Придушення небезпечних сигналів акустоелектричних перетворювачів. Екранування електромагнітних полів. Запобігання витоку інформації по ланцюгам електроживлення

Тема 12. Методи і засоби приховування інформації в каналах зв'язку

Структурне приховування мовної інформації в каналах зв'язку. Засоби контролю телефонних ліній. Перехват повідомлень в GSM каналах. Будова та основні технічні характеристиками аналізаторів телефонних ліній.

Тема 13. Методи і засоби технічної охорони об'єктів. системи сигналізації та відео спостереження

Системи телевізійного спостереження. Засоби телевізійної охорони. Основні характеристики відеокамер. Засоби запису та реєстрації зображення. Класифікація систем відеоспостереження.

4. Структура залікового кредиту

	Кількість годин					
	Лекції	Лабор. заняття	Інд. робота	Тренінг, КПІЗ	Самост. робота	Контр. заходи
Змістовий модуль 1. Елементи інформаційної системи, що підлягають захисту.						
Тема 1. Види, джерела та носії інформації, що підлягають захисту.	2	4	2	4	6	Поточне опитування
Тема 2. Небезпечні сигнали та їх джерела.	2				6	
Тема 3. Технічна розвідка.	4	2			6	
Тема 4. Концепція і методи технічного захисту інформації.	4	4			8	
Змістовий модуль 2. Технічні канали витоку інформації						
Тема 5. Технічні канали витоку інформації.	2	2	2	4	6	Поточне опитування
Тема 6. Електричні канали витоку інформації.	2	2			6	
Тема 7. Радіоелектронні канали витоку інформації.	4	4			6	
Тема 8. Акустичні канали витоку інформації.	4	4			6	
Тема 9. Технічні канали витоку інформації на основі закладних пристроїв.	4	4			8	
Змістовий модуль 3. Запобігання витоку інформації						
Тема 10. Методи та засоби захисту від спостереження та підслуховування.	2	2	1	4	6	Поточне опитування
Тема 11. Засоби запобігання витоку інформації через побічні електромагнітні випромінювання	2	2			6	
Тема 12. Методи і засоби приховування інформації в каналах зв’язку.	4	4			6	
Тема 13. Методи і засоби технічної охорони об’єктів. системи сигналізації та відео спостереження.	4	4			9	
Разом	40	38	5	12	85	

5. Тематика лабораторних робіт

Лабораторне заняття № 1

Тема: Дослідження структури об’єкту захисту

Мета роботи: Придбання теоретичних знань та практичних навичок з аналізу структури об’єкта захисту.

Лабораторне заняття № 2

Тема: Ідентифікація небезпечних чинників на об’єкт захисту

Мета роботи: Придбання опанування практичних навичок з визначення та ідентифікації загроз для заданого об’єкта захисту.

Лабораторне заняття № 3

Тема: Розробка політики інформаційної безпеки на основі технічних засобів захисту інформації

Мета роботи: Набуття досвіду зі створення політики інформаційної безпеки.

Лабораторне заняття № 4

Тема: Моделі загроз та їх класифікація для каналів витоку інформації.

Мета роботи: Розглянути питання оцінки дій загроз в інформаційних системах

Лабораторне заняття № 5

Тема: Створення просторового широкосмугового шумового сигналу для захисту комп'ютера від витоку інформації за рахунок побічних електромагнітних випромінювань

Мета роботи: освоєння навиків застосування апаратури просторового електромагнітного зашумлення для локалізації небезпечних сигналів, які розповсюджуються через канали побічних електромагнітних випромінювань

Лабораторне заняття № 6

Тема: Технічні канали витоку інформації.

Мета роботи: Вивчити та дослідити технічні канали витоку інформації

Лабораторне заняття № 7

Тема: Дослідження характеристик технічних засобів прослуховування інформації

Мета роботи: вивчити основні види засобів прослуховування інформації; виховувати прагнення захисту інформації, збереження її цілісності; розвивати знання, щодо особливостей засобів прослуховування інформації та алгоритмів їх роботи.

Лабораторне заняття № 8

Тема: Дослідження засобів відеоспостереження

Мета роботи: вивчити основні види засобів відеоспостереження; виховувати прагнення захисту інформації, збереження її цілісності; розвивати знання, щодо особливостей засобів відеоспостереження та алгоритмів їх роботи.

Лабораторне заняття № 9

Тема: Технічні канали витоку інформації на основі закладних пристроїв

Мета роботи: — навчитися класифікувати технічні канали витоку інформації на основі закладних пристроїв; ознайомитись з переліком основних груп закладних пристроїв зняття інформації; ознайомитись з основними способами виявлення закладних пристроїв; ознайомитись з основними засобами та методами блокування закладних пристроїв.

Лабораторне заняття № 10

Тема: Дослідження характеристик засобів блокування технічних каналів витоку інформації

Мета роботи: вивчити основні види засобів блокування технічних каналів витоку інформації; виховувати прагнення захисту інформації, збереження її цілісності; розвивати знання, щодо особливостей засобів блокування технічних каналів витоку інформації та алгоритмів їх роботи.

Лабораторне заняття № 11

Тема: Дослідження характеристик датчиків охоронної сигналізації»

Мета роботи: вивчити основні види датчиків охоронної сигналізації; виховувати прагнення захисту інформації, збереження її цілісності; розвивати знання, щодо особливостей датчиків охоронної сигналізації та алгоритмів їх роботи.

Лабораторне заняття № 12

Тема: Дослідження характеристик технічних засобів охорони периметру»

Мета роботи: вивчити основні види технічних засобів охорони периметру; виховувати прагнення захисту інформації, збереження її цілісності; розвивати знання, щодо особливостей технічних засобів охорони периметру та алгоритмів їх роботи.

Лабораторне заняття № 13

Тема: Вивчення функціональних характеристик комплексу засобів захисту «Лоза-1»

Мета роботи: вивчити основні функціональні можливості КЗЗ «Лоза-1»

6. Самостійна робота

Самостійне завдання студента полягає у виконанні обраного та підтвердженого викладачем наскрізного завдання. Студенти повинні обрати одну із запропонованих тематик:

Тематика

1. Активні способи захисту інформації.
2. Акустичні пристрої для прослуховування. Способи їх виявлення.
3. Види демаскуючих ознак
4. Види носіїв інформації та їх характеристика.
5. Вібраційні пристрої для прослуховування. Способи їх виявлення.
6. Вібро-акустичний канал просочування інформації.
7. Джерела загроз захисту інформації антропогенного характеру.
8. Джерела загроз інформації антропогенного характеру.
9. Джерела загроз інформації техногенного характеру.
10. Джерела сигналів.
11. Джерела функціональних сигналів.
12. Класифікація демаскуючих ознак.
13. Класифікація джерел інформації..
14. Класифікація джерел та носіїв інформації.
15. Класифікація і характеристика основних способів захисту інформації в сучасних інформаційних технологіях
16. Класифікація інформації у відповідності до Закону України «Про інформацію».
17. Класифікація розвідки.
18. Поняття «білого шуму».
19. Поняття та класифікація технічного каналу витоку інформації.
20. Призначення агентурної розвідки.
21. Призначення радіорозвідки.
22. Призначення та класифікація технічної розвідки.
23. Призначення технічної розвідки.
24. Пристрої пошуку технічних засобів пасивного типу.
25. Просторове і лінійне зашумлення.
26. Реалізація державної політики у галузі ТЗІ.
27. Сутність ознакового підходу до інформації.
28. Технічні канали витоку акустичної (мовної) інформації.
29. Фільтрація інформаційних сигналів.
30. Етапи побудови систем ЗІ.
31. Розроблення плану захисту інформації.
32. Побудова систем технічного захисту.
33. Технічне забезпечення безпеки інформації.
34. Захист машинних носіїв інформації.
35. Найпростіші апаратні пристрої, що використовуються для захисту інформації.
36. Складні технічні засоби, що використовуються для захисту інформації в комп'ютерних системах.
37. Звукоізоляція приміщень.
38. Віброакустичне маскування.
39. Розроблення плану захисту інформації.
40. Організація проведення обстеження об’єктів інформаційної діяльності підприємства
41. Реалізація первинних технічних заходів захисту
42. Реалізація основних технічних заходів захисту
43. Приймання, визначення повноти та якості робіт з ТЗІ.
44. Побудова моделі загроз інформації в інформаційних системах.
45. Канали витоку інформації в інформаційних системах.

Метою виконання самостійного завдання є оволодіння навиками оцінювання технічного захисту об’єктів та реалізація заходів захисту.

7. Організація і проведення тренінгу з дисципліни « Технічні засоби захисту інформації»

Тематика: застосування методів, засобів та алгоритмів для технічного захисту інформації.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.
2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.
3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Перелік завдань для тренінгу:

1 Апаратні засоби захисту інформації.
2 Екранування технічних засобів.
3 Електричні канали витоку інформації.
4 Електромагнітні канали витоку інформації.
5 Загрози інформації антропогенного характеру.
6 Загрози інформації природного характеру
7 Заземлення технічних засобів
8 Класифікація технічних каналів витоку інформації.
9 Конкурентна розвідка та промислове шпигунство.
10 Мета і завдання технічної розвідки.
11 Нормативні документи у сфері ТЗІ.
12 Організаційні заходи ТЗІ.
13 Організаційні та технічні засоби захисту інформації. Основні відмінності.
14 Основні об’єкти захисту інформації.
15 Основні принципи організації й ведення технічної розвідки.
16 Пасивні способи захисту інформації
17 Побічні електромагнітні випромінювання та наведення.
18 Речові демаскуючі ознаки.
19 Сигнальні демаскуючі ознаки.
20 Сутність запису і знімання інформації з носія.

8. Методи навчання

У навчальному процесі використовуються: лекції, практичні та індивідуальні заняття, групова робота, реферування, а також методи опитування, тестування, ділові ігри тощо.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Технічні засоби захисту інформації» використовуються наступні методи оцінювання навчальної роботи студентів:

- поточне тестування та поточне опитування;
- підсумкове модульне тестування та опитування за кожним заліковим модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання самостійної роботи;
- оцінювання завдань виконаних на тренінгу;
- ректорська контрольна робота;

- підсумковий екзамен.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Технічні засоби захисту інформації» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-8.	Підсумкове модульне тестування за темами № 1-9.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 9-13.	Підсумкове модульне тестування за темами № 10-13.	Визначається як середнє арифметичне з оцінок за завдання тренінгу (не менше двох).	Визначається як оцінка за наскрізне завдання самостійної роботи.	1. Теоретичні питання: 2 питання по 20 балів. 2. 15 тестів по 4 бали.

Шкала оцінювання:

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1-13
2	Методичні вказівки до виконання практичних робіт (електронний варіант)	1–13
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-13
4	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, Nod32, FoxitReader, AdobeReader, WinRAR, WinZip, MathCAD, MatLab, DjVu Viewer, Total Commander, C#, C++, MASM32, Java Server Pages, Servlets, EJB, Java Server Faces, JavaFX, BC3.0, .NET Framework, PHP, Visual C++, Symbian C++, ARIS, MS Project, IBM Rational, GPSS World, Visual Web Developer 2016 Express, SWI Prolog, Microsoft Project, Spider Project, Primavera Project Planner, SQL Server 2015 Enterprise, Visio Professional 2016, Project Professional 2016, Expression Studio 2, Visual Studio 2015, Visual Studio™ 2015, Visual Studio Team System 2015	1-13

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Аль-Амморі Алі. Елементи теорії надійності та інформаційної безпеки комп'ютеризованих систем: навч. посіб . Київ: Видавництво Ліра-К, 2024. - 282с.
2. Богуш В. М. Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В. М. Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. - 286с.
3. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. Посіб / Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П.. — К.: Видавництво Ліра-К, 2020. — 554 с.
4. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Київ: Видавництво Ліра-К, 2022. - 286с.
5. Голев Д.В., Кононович В.Г., Хомич С.В. Методики оцінки інформаційної захищеності телекомунікацій. Навчальний посібник. — Одеса : ОНАЗ ім. О. С. Попова, 2013. 217 с.
6. Гуз А.М. Організація захисту інформації з обмеженим доступом : навчальний посібник. Гуз А.М., Касперський І.П., Ткачук Т.Ю. Київ : НА СБУ, 2018. С. 33–58.
7. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник / Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
8. Євсеєв С.П. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури. Монографія / С.П. Євсеєв, О.Ю. Заковоротний, О.В. Мілов, Г.А. Кучук, О.А. Галуза, М.В. Коваль, О.В. Войтко, Р.В. Грищук – Харків: Вид. «Новий Світ-2000», 2024. 300 с. (Укр. мов.)
9. Козачок В.А. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів / Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. – Київ: ДУТ ННІЗІ, 2020. – 167 с.
10. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020. – 126 с.
11. Ластівка Г.І. Технічний захист інформації в інформаційних та телекомунікаційних системах: навчальний посібник / Г.І. Ластівка, П.М. Шпатар. Чернівці, Чернівецький національний університет, 2018. – 252 с.
12. Остапов С. Е. Технології захисту інформації: навчальний посібник (2-ге видання, стереотипне) / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2024 . – 678 с.

13. Полторак В.П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах. Навчальний посібник. – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
14. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект : навчально-методичний посібник / О. А. Самойленко. - Одеса, 2020. 133 с.
15. Чубенко А. Г.. Володілець інформації; Засоби захисту інформації. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. — Київ : Ваіте, 2018. — С. 175; 273.
16. CCTA Risk Analysis and Management Method [Електронний ресурс] – Режим доступу: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysismanagement-tool-cramm/103133 (дата звернення: 21.01.2022)
17. Jason Andress. Foundations of Information Security: A Straightforward Introduction. No Starch Press,US. 2019. – P. 380.