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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«29» 08 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«29» 08 2025 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	46	44	5	12	73	180	Екзамен (7)

29.08.2025

Тернопіль – 2025

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 15.06.2022 р.).

Робочу програму склав доцент кафедри кібербезпеки, доктор філософії (Кібербезпека та захист інформації) Сергій КУЛИНА.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2025 р.

Завідувач кафедри _____ 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 – 46. Лабораторні заняття (год): Денна – 44.
Загальна кількість годин – 180		Самостійна робота (год): 73. 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 здобувачами освіти 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 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.).

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.

2.5. Результати навчання

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

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 огради 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	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	4	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			6	
Змістовий модуль 2. Технічні канали витоку інформації						
Тема 5. Технічні канали витоку інформації.	4	4	2	4	4	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			6	
Змістовий модуль 3. Запобігання витоку інформації						
Тема 10. Методи та засоби захисту від спостереження та підслуховування.	4	4	1	4	4	Поточне опитування
Тема 11. Засоби запобігання витоку інформації через побічні електромагнітні випромінювання	4	4			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			7	
Разом	46	44	5	12	73	

5. Тематика лабораторних робіт

Лабораторна робота № 1

Тема: Дослідження структури об’єкту захисту

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

Лабораторна робота № 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.

Лабораторна робота № 3

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

Мета роботи: Набуття досвіду зі створення політики інформаційної безпеки.

Лабораторна робота № 4

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

Мета роботи: Розглянути питання оцінки дій загроз в інформаційних системах

Лабораторна робота № 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

Лабораторна робота № 6

Тема: Технічні канали витоку інформації.

Мета роботи: Вивчити та дослідити технічні канали витоку інформації

Лабораторна робота № 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.

Лабораторна робота № 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.

Лабораторна робота № 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; способами виявлення та засобами і методами блокування закладних пристроїв.

Лабораторна робота № 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.

Лабораторна робота № 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.

Лабораторна робота № 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.

Лабораторна робота № 13

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

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

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

Тематика: Виявлення та аналіз електромагнітних випромінювань від комп'ютерної техніки, дослідження акустичних та вібраційних каналів витоку інформації, практичне застосування технічних засобів активного та пасивного захисту.

Мета тренінгу з дисципліни "«Технічні засоби захисту інформації" – поглиблення та закріплення теоретичних знань з дисципліни, отриманих на лекційних та лабораторних заняттях, а також формування у здобувачів освіти:

- практичних навичок з ідентифікації та класифікації технічних каналів витоку;
- вміння використовувати спеціалізоване вимірювальне обладнання;
- здатності аналізувати рівень загрози та розробляти заходи із захисту інформації;
- розуміння принципів роботи активних та пасивних засобів захисту.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення здобувачів освіти з коротким оглядом основних понять захисту даних, що відносяться до конкретної теми тренінгу, демонстрація приладів, генераторів шуму та інших засобів, які будуть використовуватися на практиці під час тренінгу.
2. Організаційна частина полягає у поділі учасників на робочі групи та імітації каналу витоку з подальшою демонстрацією необхідних навичок для його виявлення та аналізу.
3. Практична частина реалізується шляхом відпрацювання навичок виявлення та аналізу технічного каналу витоку даних у рамках вибраного групою завдання тренінгу.
4. Підведення підсумків. Аналіз результатів роботи груп. Обговорення типових помилок та складних ситуацій, які можуть виникнути в реальних умовах.

Орієнтований 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.

Підсумкова оцінка за тренінг визначається як середнє арифметичне з оцінок, отриманих за виконання трьох довільно вибраних завдань тренінгу.

7. Самостійна робота

Здобувачі освіти мають самостійно опрацьовувати відповідний обсяг інформації, оскільки це є обов'язковим компонентом їхньої навчальної діяльності у вищій школі. Самостійна робота полягає у проведенні дослідження та підготовці звіту згідно однієї вибраної здобувачем освіти теми із переліку 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, реалізація заходів захисту та підготовка звіту про стан захищеності об’єкту.

Загальні вимоги до оформлення результатів виконаних завдань самостійної роботи: шрифт − Times New Roman; розмір шрифту − 14 кегель; інтервал між рядками – 1,5; абзац – 1,25 см, поля: верхнє і нижнє – 20 мм, ліве – 25 мм, праве – 15 мм; нумерація сторінок − у правому нижньому куті; обсяг звіту – 10-12 сторінок друкованого тексту. Максимальна кількість балів за завдання самостійної роботи становить 100 балів.

8. Методи навчання

У процесі навчання використовуються: лекції, в тому числі із використання мультимедійного проектора, лабораторні та індивідуальні заняття, робота в групі, реферування, а також методи опитування, тестування тощо.

9. Засоби оцінювання та методи демонстрування результатів навчання

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

- 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;
- екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу учасник може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій

формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. 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 отриманих за виконання трьох довільно вибраних завдань.	Оцінка за звіт про виконаного завдання самостійної роботи.	1. Теоретичні питання: 2 питання по 20 балів. 2. 15 тестів по 4 бали.

Виконання лабораторних робіт:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі кроки в рамках лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами, що відносяться до теми дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання лабораторної роботи, проте в процесі виконання допустив кілька дрібних помилок, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу чи не до кінця. Розуміння поставлених у лабораторній роботі завдань є поверхневим та неповним.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з програмним забезпеченням.

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем освіти теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 40 запитань кожна правильна відповідь дає 2,5 бали, максимум 100 балів.

Тренінг:

90-100 балів (Відмінно) - здобувач освіти самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами дисципліни.

75-89 балів (Добре) - здобувач освіти виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат, в процесі роботи виникали додаткові запитання.

60-74 балів (Задовільно) - здобувач освіти виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у тренінгу завдань є поверхневим.

1-59 балів (Незадовільно) - здобувач освіти не зміг виконати завдання або результати були повністю невірними. Не продемонстрував достатній рівень навичок роботи з апаратним та програмним забезпеченням.

Самостійна робота:

90–100 балів (Відмінно) - доповідь охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Дослідження містить не лише опис, але й аналіз, порівняння різних методів та засобів, висновки обґрунтовані. У процесі написання звіту використані сучасні джерела інформації, що свідчить про обізнаність здобувача освіти з напрямом дослідження. Здобувач освіти вільно володіє матеріалом, доповідає впевнено та відповідає на всі запитання.

75–89 балів (Добре) - доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими; використані джерела інформації є релевантними, але не найновішими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

60–74 балів (Задовільно) - доповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач не завжди впевнено відповідає на запитання, а сам виступ може бути нечітким.

1–59 балів (Незадовільно) - зміст доповіді не відповідає темі або є компіляцією застарілих даних. Робота є прямим копіюванням без самостійного опрацювання.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу з дисципліни «Технічні засоби захисту інформації». Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитання, за кожне з яких можна отримати від 0 до 20 балів, що в підсумку дає максимально 40 балів. За відповідь на питання здобувач освіти отримує 11–20 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–10 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить 15 тестових завдань. За кожну правильну відповідь тестування здобувач освіти отримує 4 бали, максимум 60 балів.

Шкала оцінювання:

За шкалою ЗУНУ	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 лабораторних робіт (електронний варіант)	1–13
3	ПК Intel Core i3-540 або інший схожий за параметрами ПК чи ноутбук, стенд генерації шумоподібних сигналів.	1-13
4	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, FoxitReader, AdobeReader, WinRAR, WinZip, DjVu Viewer, Total Commander, Python 3.8.	1-13

Рекомендовані джерела інформації

1. Яцків, В. В., Кулина, С. В. (2023). Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека». – Тернопіль 2023. – 88 с.
2. Кулина, С. В. (2023). Виявлення та виправлення помилок у захищених системах зберігання даних на основі обчислення проекцій числа. *Informatics and Mathematical Methods in Simulation*. Vol. 12, 2022, No. 4, pp. 337-345.
3. Кулина, С. В. (2023). Система розподіленого захищеного зберігання даних. *Вісник Львівського державного університету безпеки життєдіяльності*, № 27, 2023. С.48-59.
4. Аль-Амморі, А. (2024). *Елементи теорії надійності та інформаційної безпеки комп'ютеризованих систем*: навч. посіб. Київ: Ліра-К. 282 с.
5. Богуш, В. М., Бровко, В. Д., Кобус, О. С., & Козюра, В. Д. (2022). *Технічний захист інформації*. Ч. 1: *Основи технічного захисту інформації*: навч. посіб. Київ: Ліра-К. 286 с.
6. Богуш, В. М., Богуш, В. В., Бровко, В. Д., & Настрадін, В. П. (2020). *Основи кіберпростору, кібербезпеки та кіберзахисту*: навч. посіб. Київ: Ліра-К. 554 с.
7. Богуш, В. М., Бровко, В. Д., Кобус, О. С., & Козюра, В. Д. (2022). *Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення*. Київ: Ліра. 286 с.
8. Сальник, В. В., Гуж, О. А., Закусіло, В. С., Сальник, С. В., & Бєляєв, П. В. (2021). Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. *Збірник наукових праць Харківського національного університету Повітряних Сил*, (4 (70)), 77-82.
9. Остапов, С. Е., Євсеєв, С. П., & Король, О. Г. (2023). *Технології захисту інформації*: навч. посіб. Львів: Новий світ-2000. 678 с.
10. Гулак, Г. М. (2020). *Методологія захисту інформації. Аспекти кібербезпеки*: підручник. Київ: НА СБ України. 256 с.
11. Євсеєв, С. П., Заковоротний, О. Ю., Мілов, О. В., Кучук, Г. А., Галуза, О. А., Коваль, М. В., Войтко, О. В., & Грищук, Р. В. (2024). *Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури*: монографія. Харків: Новий Світ-2000. 300 с.
12. Лаптєв, О. А., Савченко, В. А., & Шуклін, Г. В. (2020). *Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності*: навч. посіб. Київ: ДУТ. 126 с.
13. Полторак, В. П. (2020). *Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах*: навч. посіб. Київ: КПІ ім. Ігоря Сікорського. 78 с.
14. CCTA Risk Analysis and Management Method. (н.д.). URL: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysismanagement-tool-cramm/103133.