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 «Комплексні системи 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	8	30	30	4	6	80	150	Екзамен (8)

29.08.2025 г.

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

1. Опис дисципліни «Комплексні системи захисту інформації»

Дисципліна «Комплексні системи захисту інформації»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 5	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 – 8.
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції (год): Денна – 30. Лабораторні заняття (год): Денна – 30.
Загальна кількість годин – 150		Самостійна робота (год): 78. Тренінг (год): 8. Індивідуальна робота (год): 4.
Тижневих годин – 15, з них аудиторних – 6		Вид підсумкового контролю – екзамен.

2. Мета й завдання вивчення дисципліни «Комплексні системи захисту інформації»

2.1. Мета завдання дисципліни

Метою викладання дисципліни «Комплексні системи захисту інформації» є навчання здобувачів освіти принципам проектування, впровадження та адміністрування сучасних систем кібербезпеки на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку сигналів технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки та державних нормативних документів з технології захисту інформації.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни: надати достатній рівень знань, умінь та компетентностей у галузі побудови комплексних систем захисту інформації; мати здатності до застосовування отриманих знань у практичних ситуаціях; знати та розуміти предметну область, розуміти професію; вміти виявляти, ставити та вирішувати проблеми у галузі кібербезпеки.

2.3.Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

- здатність до пошуку, оброблення та аналізу інформації;
- 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 «Комплексні системи захисту інформації» передбачає наявність систематичних та ґрунтовних знань із суміжних дисциплін («Оцінка та управління ризиками», «Безпека WEB ресурсів», «Технічні засоби захисту інформації», «Тестування на проникнення»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи здобувачів освіти.

2.5. Результати навчання

- Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
- Розробляти моделі загроз та порушника.
- Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
- Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.
- Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
- Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
- Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів.
- Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно телекомунікаційних системах.

3. Програма навчальної дисципліни «Комплексні системи захисту інформації»

Змістовний модуль 1. Завдання та методологічні основи КСЗІ

Тема 1. Сутність і завдання комплексної системи захисту інформації

1.1. Поняття комплексної системи захисту інформації
1.2. Сутність комплексної системи захисту інформації
1.3. Призначення комплексної системи захисту інформації
1.4. Принципи побудови комплексної системи захисту інформації
1.5. Цілі системного підходу до захисту інформації
1.6. Стратегії захисту інформації
1.7. Розробка політики безпеки підприємства
1.8. Основні вимоги, що пред'являються до комплексної системи захисту інформації

Тема 2. Методологічні основи комплексної системи захисту інформації

2.1. Основні поняття теорії захисту інформації

2.2. Методологія захисту інформації як теоретичний базис комплексної системи захисту інформації

2.3. Основні поняття теорії систем

2.4. Системний аналіз і системний підхід

2.5. Основні системні уявлення

Тема 3. Визначення складу інформації, що захищається

3.1. Методика визначення складу інформації, що захищається

3.2. Класифікація інформації за видами таємниці і ступенями конфіденційності

3.3. Визначення об'єктів захисту

3.4. Сховища носіїв інформації як об'єкт захисту

3.5. Методи оцінки захищеності підприємства

Тема 4. Джерела, способи і результати дестабілізуючого впливу на інформацію

4.1. Оцінка загроз безпеки інформації

4.2. Явища, фактори і умови дестабілізуючого впливу на захищає інформацію

4.3. Джерела дестабілізуючого впливу на інформацію

4.4. Види і способи дестабілізуючого впливу на інформацію з боку людей

4.5. Види і способи дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ

4.6. Визначення причин, обставин і умов дестабілізуючого впливу на інформацію з боку людей

4.7. Причини, обставини і умови дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ

Змістовний модуль 2. Моделювання, технологічна побудова, кадрове забезпечення КСЗІ

Тема 5. Канали і методи несанкціонованого доступу до інформації

5.1. Методика виявлення каналів несанкціонованого доступу до інформації

5.2. Визначення можливих методів несанкціонованого доступу до інформації, що захищається

5.3. Ділова розвідка як канал несанкціонованого доступу для отримання інформації

5.4. Інформаційний продукт як наслідок реалізації несанкціонованих дій

5.5. Модель потенційного порушника

Тема 6. Моделювання процесів комплексної системи захисту інформації

6.1. Поняття моделі об'єкта. Моделювання як інструмент аналізу об'єкта КСЗІ

6.2. Значення моделювання процесів КСЗІ

6.3. Архітектурне побудова комплексної системи захисту інформації

Тема 7. Технологічна побудова комплексної системи захисту інформації

7.1. Технологічне побудова організаційної системи КСЗІ

7.2. Структура організаційної системи підприємства

7.3. Загальний вміст робіт з проектування КСЗІ

7.4. Основні стадії проектування КСЗІ

7.5. Фактори, що впливають на вибір складу КСЗІ

7.6. Модель системи автоматизованого проектування захисту інформації

Тема 8. Кадрове забезпечення комплексної системи захисту інформації

8.1. Кадрова політика підприємства при створенні КСЗІ

8.2. Етапи роботи з персоналом

8.3. Комплексний захист інформації та персонал

8.4. Мотивація

8.5. Розробка кодексу корпоративної поведінки

Змістовний модуль 3. Нормативно-методичне забезпечення та планування діяльності КСЗІ

Тема 9. Нормативно-методичне забезпечення КСЗІ

9.1. Значення нормативно-методичного забезпечення

9.2. Склад нормативно-методичного забезпечення

9.3. Порядок розробки і впровадження документів підприємства

Тема 10. Управління комплексною системою захисту інформації

10.1. Загальні закони кібернетики

10.2. Сутність організації процесів управління КСЗІ

10.3. Технологія організаційного управління КСЗІ

10.4. Структуризація процесів технології управління

10.5. Вимоги до системи управління як об'єкту дослідження

10.6. Основи методології прийняття управлінського рішення

10.7. Загальні вимоги до прийняття управлінського рішення

10.8. Роль психологічної теорії прийняття управлінського рішення

Тема 11. Планування діяльності комплексної системи захисту інформації

11.1. Цілі планування діяльності КСЗІ

11.2. Принципи планування

11.3. Способи планування

11.4. Основні положення розроблення плану

11.5. Стадії планування

11.6. Контроль діяльності

Тема 12. Управління комплексною системою захисту інформації в умовах надзвичайних ситуацій

12.1. Поняття і основні види надзвичайних ситуацій

12.2. Технологія прийняття рішення в умовах надзвичайної ситуації

12.3. Фактори, що впливають на прийняття рішення

12.4. Забезпечення управління КСЗІ в умовах надзвичайних ситуацій

12.5. Підготовка заходів на випадок виникнення надзвичайної ситуації

4. Структура залікового кредиту дисципліни «Комплексні системи захисту інформації»

	Кількість годин					
	Лекції	Лабор. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Завдання та методологічні основи КСЗІ						
Тема 1. Сутність і завдання комплексної системи захисту інформації	2	2	6	2	2	Поточне опитування

Тема 2. Методологічні основи комплексної системи захисту інформації	2	2	6			
Тема 3. Визначення складу інформації, що захищається	2	2	6			Поточне опитування
Тема 4. Джерела, способи і результати дестабілізуючого впливу на інформацію	4	4	6			
Змістовний модуль 3. Моделювання, технологічна побудова, кадрове забезпечення КСЗІ						
Тема 5. Канали і методи несанкціонованого доступу до інформації	2	2	6	-	2	Поточне опитування
Тема 6. Моделювання процесів комплексної системи захисту інформації.	2	2	6			
Тема 7. Технологічна побудова комплексної системи захисту інформації	2	2	7			
Тема 8. Кадрове забезпечення комплексної системи захисту інформації	4	4	7			
Змістовний модуль 4. Нормативно-методичне забезпечення та планування діяльності КСЗІ						
Тема 9. Нормативно-методичне забезпечення КСЗІ	2	2	7	2	4	Поточне опитування
Тема 10. Управління комплексною системою захисту інформації	2	2	7			
Тема 11. Планування діяльності комплексної системи захисту інформації	2	2	7			
Тема 12. Управління комплексною системою захисту інформації в умовах надзвичайних ситуацій.	4	2	7			
Разом	30	30	78	4	8	

5. Тематика лабораторних робіт

Лабораторна робота 1. Дослідження системи аналізу ризиків та перевірки політики інформаційної безпеки підприємства

Мета роботи: Проведення дослідження системи аналізу ризиків та перевірки політики інформаційної безпеки підприємства

1. Огляд програмних продуктів в області аналізу ризиків та перевірки організаційних заходів забезпечення інформаційної безпеки

2. Опис системи

3. Інтерфейс системи

Лабораторна робота 2. Дослідження захищеності бездротових мереж передачі даних

Мета роботи: Проведення дослідження захищеності бездротових мереж передачі даних

1. Короткі теоретичні відомості.

2. Порядок виконання роботи.

3. Відповіді на запитання та підготовка звіту.

Лабораторна робота 3. Дослідження і адміністрування коштів забезпечення інформаційної безпеки Web-сервера Microsoft IIS Server.

Мета роботи: Ознайомитися, дослідити і адмініструвати кошти забезпечення інформаційної безпеки Web-сервера Microsoft IIS Server

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота 4. Дослідження і адміністрування коштів забезпечення інформаційної безпеки Microsoft ISA Security Server. Встановлювати чи налаштовувати брандмауера ISA. Побудова VPN-мережі на базі ISA

Мета роботи: Забезпечення інформаційної безпеки Microsoft ISA Security Server. Встановлення чи налаштування брандмауера ISA. Побудова VPN-мережі на базі ISA

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота №5 Дослідження структури об’єкту захисту

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

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота №6. Ідентифікація небезпечних чинників на об’єкт захисту

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

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота №7. Оцінювання стану інформаційної безпеки об’єкту

Мета роботи: Освоєння практичних навичок з моделювання стану безпеки об’єкта та ранжування загроз.

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота №8. Розробка політики інформаційної безпеки

Мета роботи: Набуття досвіду зі створення політики інформаційної безпеки.

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота № 9. «Модель порушника»

Мета роботи: Ознайомитись з основними моделями порушників та їх класифікацією.

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота № 10. Моделі загроз. Класифікації моделі загроз.

Мета : Розглянути питання оцінки дій загроз в інформаційних системах

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.

3. Відповіді на запитання та підготовка звіту.

Лабораторна робота № 11. «Протокол випробувань комплексних систем захисту інформації»

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

Лабораторна робота 12. Дослідження та розгортання мережевої інфраструктури Microsoft Windows Exchange Server

1. Короткі теоретичні відомості.
2. Порядок виконання роботи.
3. Відповіді на запитання та підготовка звіту.

7. Організація і проведення тренінгу з дисципліни «Комплексні системи захисту інформації»

Тематика: Розробка системи виявлення та запобігання вторгнень на основі open source рішень.

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

- практичних навичок ключових професійних дій та операцій, які є невід'ємною частиною майбутньої роботи у сфері кіберзахисту;
- уміння використовувати теоретичні знання для вирішення реальних, практичних завдань у сфері кіберзахисту;
- навичок аналізу професійних ситуацій, пошуку ефективних рішень та оцінки їхніх результатів;
- усвідомлення важливості дотримання стандартів у сфері кіберзахисту.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення учасників з темою та основними завданнями тренінгу, ключовими поняттями та принципами, що будуть використані в процесі роботи.
2. Організаційна частина полягає у формуванні робочих груп та поясненні правил роботи. Учасники групою обирають тему із рекомендованого переліку.
3. Практична частина реалізується шляхом виконання завдань тренінгу з подальшим оформленням звіту про виконану роботу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Завдання тренінгу полягає в проведенні дослідження на одну із рекомендованих тем:

1 Основні принципи організації КСЗІ.
2 Відкритість алгоритмів і механізмів захисту.
3 Концептуальні підходи до проектування систем захисту.
4 Принцип простоти застосування засобів захисту.
5 Організація проведення обстеження об'єктів інформаційної діяльності.
6 Організація розроблення системи захисту інформації.
7 Реалізація основних технічних заходів захисту.
8 Реалізація первинних технічних заходів захисту.
9 Контроль функціонування та керування системою ЗІ.
10 Визначення на підприємстві інформаційних і технічних ресурсів, а також об'єктів інформаційної діяльності, що підлягають захисту.

11 Категорiювання об'єктiв iнформацiйної дiяльностi пiдприємства.
12 Засекречування та розсекречування матерiальних носiїв iнформацiї.
13 Рекомендацiї з захисту iнформацiї, що обробляється засобами КРТ класу Б.
14 Класифiкатор засобiв копiювально-розмножувальної технiки.
15 Вимоги до захисту iнформацiї.
16 Порядок створення, впровадження, супроводу та модернiзацiї засобiв технiчного захисту iнформацiї вiд несанкцiонованого доступу.

Пiдсумкова оцiнка за тренiнг визначається як оцiнка за доповiдь та представлений звiт згiдно iз обраною групою темою дослiдження.

7. Самостiйна робота

Здобувачi освiти мають самостiйно опрацьовувати вiдповiдний обсяг iнформацiї, оскiльки це є обов'язковим компонентом їхньої навчальної дiяльностi у вищiй школi. Самостiйна робота полягає у проведенні дослiдження та пiдготовцi звiту згiдно однiєї вибраної здобувачем освiти теми iз запропонованих орiєнтованих тематик:

1. Сучасний стан нормативно-правової бази України щодо побудови КСЗI в IКС.
2. Сучаснi методики та програмнi засоби налагодження параметрiв полiтики безпеки операцiйних систем в IКС.
3. Опис операцiйних систем, що мають позитивнi експертнi висновки в Українi, щодо побудови КСЗI в IКС.
4. Опис АВПЗ, що мають позитивнi експертнi висновки в Українi, як складової КСЗI в IКС.
5. Опис КЗЗ вiд НСД, що мають позитивнi експертнi висновки в Українi, як складової КСЗI в IКС.
6. Опис засобiв ТЗI, що мають позитивнi експертнi висновки в Українi, як складової КСЗI в IКС.
7. Опис засобiв КЗI (крiм ЕЦП), що мають позитивнi експертнi висновки в Українi, як складової КСЗI в IКС.
8. Опис засобiв ЕЦП, що мають позитивнi експертнi висновки в Українi, як складової КСЗI в IКС.
9. Сучаснi методики та програмнi засоби побудови моделей загроз для iнформацiї та порушникiв в IКС.
10. Опис сучасних загроз для iнформацiї та нормального функцiонування IКС.
11. Сучаснi методики та програмнi засоби формування ФПЗ iнформацiї вiд НСД в IКС.
12. Сучаснi методики та програмнi засоби оцiнки стану захищеностi iнформацiї Web-сайту вiд НСД.
13. Сучаснi методики та програмнi засоби оцiнки надiйностi та ефективностi КСЗI в IКС.
14. Опис стану оформлення та провадження господарської дiяльностi у галузi ТЗI в Українi.
15. Опис стану оформлення та провадження господарської дiяльностi у галузi КЗI в Українi.
16. Опис стану оформлення та надання послуг електронного цифрового пiдпису в Українi.
17. Розробка таблиць даних для визначення необхiдностi та рiвня кожної послуги безпеки iнформацiї.

Метою виконання самостiйного завдання є оволодiння навиками аналiзу та оцiнювання ефективностi комплексних систем захисту iнформацiї та пiдготовка звiту згiдно проведеного дослiдження.

Загальнi вимоги до оформлення результатiв виконаних завдань самостiйної роботи: шрифт − Times New Roman; розмiр шрифту − 14 кегель; iнтервал мiж 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 застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших технічних засобів, лабораторні роботи, індивідуальні заняття; робота в мережі Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Комплексні системи захисту інформації» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне оцінювання;
- залікове модульне тестування та опитування;
- завдання на лабораторному обладнанні, тощо;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;
- 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 №1-6.	Підсумкове модульне тестування за темами № 1-6.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 7-12.	Підсумкове модульне тестування за темами № 7-12.	Оцінка за доповідь та представлений звіт згідно із обраною групою темою дослідження.	Оцінка за звіт про виконаного завдання самостійної роботи.	1. Теоретичні питання: 2 питання по 30 балів. 2. 20 тестів по 2 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 30 балів, що в підсумку дає максимально 60 балів. За відповідь на питання здобувач освіти отримує 15–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–15 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить 20 тестових завдань. За кожну правильну відповідь тестування здобувач освіти отримує 2 бали, максимум 40 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	1-12
2	Методичні вказівки до виконання практичних робіт (електронний варіант)	1–12
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-12
4	Засіб захисту інформації від несанкціонованого доступу «Лоза-1» версія 3, Екрануюча настільна шкатулка Фарадея для телефонів, автобрелків, NFC карт LockerBox RF MAXI. Генератор електромагнітних завад «Базальт-5ГЕШ», Мережевий завадозаглушувальний фільтр «ФЗП 103-2», Генератор шумових сигналів – МАРС ТЗО-4-2, Вібровипромінювач ВИ-3,ВИ-4, Акустичний випромінювач МАРС-АК, МАРС-АКЗ. Пристрій захисту телефонних ліній «Базальт – 3».	1-12

Рекомендовані джерела інформації

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/ show/80
2. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2019 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya-20.html
3. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2019 - Режим доступу: http://www.cryptohistory.ru/for students/ 03-KSZI
4. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf
5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку / 2023 - Режимдоступу : https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
6. Закон України "Про національну безпеку (2019)
7. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
8. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e
9. "Комплексна безпека інформації та захист інформаційних ресурсів" автора Олександра С. Горбачова. Видавництво: Каравела. Рік видання: 2019. с. - 127.
10. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html 2024.
11. Комплексні системи захисту інформації в інформаційнотелекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.