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

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних інформаційних технологій
Ігор ЯКИМЕНКО
_____
«___» _____ 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
_____
«___» _____ 2025 р.

ЗАТВЕРДЖУЮ:
Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
_____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Блокчейн: математичні проблеми та застосування»
ступінь вищої освіти – магістр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра спеціалізованих комп`ютерних систем

Форма навчання	Курс	Семестр	Лекції (год.)	Лабо. роботи (год.)	Інд. роб (год.)	Тренінг (год.)	Самост. робота (год.)	Разом (год.)	Залік/ екзамен. (семестр)
Денна	1	2	32	14	5	6	93	150	Екзамен (2)
Заочна	1	2	8	4	-	-	138	150	Екзамен (2)

Тернопіль – 2025

Робочу програму склала доцент кафедри спеціалізованих комп'ютерних систем, к.т.н., доцент Наталія ЯЦКІВ

Робоча програма затверджена на засіданні кафедри спеціалізованих комп'ютерних систем, протокол
№ 3 від 25.05.25 р.

Завідувач кафедри
спеціалізованих комп'ютерних систем Андрій СЕГІН

Гарант освітньо-професійної
програми Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Блокчейн: математичні проблеми та застосування»

Дисципліна «Блокчейн: математичні проблеми та застосування»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 5	Галузь знань – F Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 4	Спеціальність – F5 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна - 1* Семестр: *Денна – 2* *Заочна - 2,3*
Кількість змістових модулів – 2	Ступінь вищої освіти –магістр	Лекції (год): *Денна – 32* *Заочна - 8* Лабораторні заняття (год): *Денна – 14* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 93* *Тренінг 6* *Заочна – 138* Індивідуальна робота (год): *Денна – 5*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Блокчейн: математичні проблеми та застосування»

2.1. Мета вивчення дисципліни.

Метою дисципліни ««**Блокчейн: математичні проблеми та застосування**» є формування у студентів цілісного уявлення про суть технології блокчейн та переваги її використання в різних сферах діяльності людини.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни «Блокчейн: математичні проблеми та застосування» отримання студентами теоретичних знань, спеціальних умінь і практичних навичок з використання технології блокчейн.

2.3. В результаті вивчення дисципліни студент повинен знати:

− методи та переваги децентралізації;

− типи блокчейнів;

- методи, алгоритми та програмні засоби забезпечення цілісності та конфіденційності даних в технології блокчейн;
- криптографію на основі еліптичної кривої;
- криптографічні конструкції в технології блокчейн;
- структуру даних Дерева Merkle;
- алгоритми доказу виконаної роботи;
- принцип роботи та різновиди цифрових підписів;
- принципи роботи криптовалюти біткоін;
- формати ключів у Bitcoin.

2.4. В результаті вивчення дисципліни студент повинен уміти:

− використовувати технологію блокчейн у професійній діяльності, оцінювати її ефективність;

− розробляти та впроваджувати інформаційні системи на основі технології блокчейн та цифрових валют;

− застосовувати алгоритми консенсус у децентралізованих системах;

− застосовувати різні типи платформ для розробки додатків на основі технології блокчейн.

3. Програма навчальної дисципліни: «Блокчейн: математичні проблеми та застосування».

Змістовий модуль 1. Криптографія в блокчейн.

Тема 1. Вступ до блокчейн-технологій та розподілених реєстрів.

Основні поняття блокчейну та розподіленого реєстру**.** Історія виникнення блокчейну і еволюція технології. Основні характеристики блокчейну. Блокчейн та традиційна база даних. Основні сфери застосування з акцентом на кібербезпеку.

Тема 2. Криптографічні примітиви в блокчейні

Криптографічні хеш-функції: SHA-256, SHA-3, BLAKE2. Математичні властивості: односторонність, стійкість до колізій. Дерева Меркла: побудова та верифікація.

Тема 3. Асиметрична криптографія в блокчейні.

Асиметричні алгоритми шифрування . Основні алгоритми цифрового підпису в блокчейн. Алгоритм ECDSA. Підпис Шнорра. Цифровий підпис EdDSA. Осліплений підпис. Мультипідпис. . Порогові підписи. Агреговані підписи. Кільцеві підписи.

Тема 4. Алгоритми консенсусу в технології блокчейн

Алгоритм доказу виконання роботи. Алгоритми на основі підтвердження частки. Альтернативні алгоритми консенсусу.

Тема 5. Теорія складності та криптографічні задачі.

Роль теорії складності в безпеці блокчейну. Криптографічні пазли в Proof-of-Work. Односторонні функції та NP-складні задачі.

Тема 6. Архітектура блокчейн-мереж.

Структура блоків та транзакцій у блокчейні. Мережеві протоколи P2P. Методи масштабування блокчейнів.

Тема 7. Тріада блокчейн: масштабованість, безпека, децентралізація

Формальне визначення тріади. Неможливість одночасної оптимізації. Аналіз компромісів у різних блокчейн-системах. Теоретичні підходи до вирішення тріади. Практичні підходи до подолання обмежень.

Тема 8. Смарт-контракти та платформи**.**

Архітектура Ethereum та Ethereum Virtual Machine. Приклади мов програмування для смарт-контрактів: Solidity та Vyper. Сучасні платформи для розгортання смарт-контрактів.

Змістовий модуль 2. Конфіденційність та безпека блокчейн.

Тема 9. Аналіз вразливостей смарт-контрактів

Поширені типи вразливостей смарт-контрактів. Методи формальної верифікації смарт-контрактів. Інструменти безпеки для аналізу смарт-контрактів. Приклади використання інструментів на вразливому коді.

Тема 10. Методи захисту блокчейн-мереж.

Захист консенсусного рівня. Методи шифрування та забезпечення анонімності. Безпека мережевої інфраструктури вузлів. Порівняння методів захисту.

Тема 11. Zero-Knowledge Proofs у блокчейні

Математичні основи ZKP. Протоколи zk-SNARK, zk-STARK і Bulletproofs: пояснення та порівняння. Приклади використання ZKP у криптовалютах

Тема 12. Post-Quantum криптографія для блокчейну

Постквантові криптосистем: Kyber, Dilithium, NTRU, Classic McEliece, BIKE. Інтеграція в блокчейн-протоколи. Приклади блокчейн-платформ з постквантовою криптографією. Виклики масштабування та сумісності.

Тема 13. Блокчейн та IoT / кіберфізичні системи

Моделі застосування блокчейну для захисту IoT. Продуктивність блокчейн-рішень: пропускна здатність, затримка, енергоспоживання. Захист IoT-вузлів від фізичних атак. Порівняльна характеристика технологій (L1, L2, DAG, BFT, канали платежів). Приклади платформ та проектів.

Тема 14. Перспективні напрямки розвитку блокчейну

Проблема масштабованості та підхід Layer 2. Децентралізовані ідентифікатори. Конфіденційні обчислення. Гомоморфне шифрування. Багатосторонні обчислення: спільне обчислення без довіри. Приклади платформ конфіденційних обчислень.

Тема 15. Тенденції та майбутнє безпеки блокчейну

Аналіз сучасних досліджень у сфері безпеки блокчейну. Потенційні загрози в умовах постквантової епохи. Приклади потенційних атак. Перспективи розвитку технологій захисту.

4.1 Структура залікового кредиту з дисципліни «Блокчейн: математичні проблеми та застосування» (денна форма навчання)

	Кількість годин					
	Лекції	Лабор. роботи	Само	Індив. робота	Тренінг	Контро-льні заходи
Змістовий модуль 1. Криптографія в блокчейн						
Тема 1. Вступ до блокчейн-технологій та розподілених реєстрів	2		4	2	3	Поточне опитування
Тема 2. Криптографічні примітиви в блокчейні	2	2	4			
Тема 3. Асиметрична криптографія в блокчейні	2	2	4			
Тема 4. Алгоритми консенсусу в технології блокчейн	2	2	4			
Тема 5. Теорія складності та криптографічні задачі	2		8			
Тема 6. Архітектура блокчейн-мереж	2		8			
Тема 7. Тріада блокчейн: масштабованість, безпека, децентралізація	2		8			
Тема 8. Смарт-контракти та платформи	2	2	8			
Змістовий модуль 2. Конфіденційність та безпека блокчейн						
Тема 9. Аналіз вразливостей смарт-контрактів	2		7	3	3	Поточне опитування
Тема 10. Методи захисту блокчейн-мереж	2		8			
Тема 11 Zero-Knowledge Proofs у блокчейні	2	2	6			
Тема 12. Post-Quantum криптографія для блокчейну	2	2	6			
Тема 13. Блокчейн та IoT / кіберфізичні системи	2	2	8			
Тема 14. Перспективні напрямки розвитку блокчейну	2		4			
Тема 15. Тенденції та майбутнє безпеки блокчейну	2		6			
Разом	30	14	93	5	6	

4.2 Структура залікового кредиту

з дисципліни «Блокчейн: математичні проблеми та застосування» (заочна форма навчання)

	Кількість годин		
	Лекції	Прак-тичні заняття	Самостійна робота
Змістовий модуль 1. Криптографія в блокчейн			
Тема 1. Вступ до блокчейн-технологій та розподілених реєстрів	2	-	8
Тема 2. Криптографічні примітиви в блокчейні		-	8
Тема 3. Асиметрична криптографія в блокчейні		-	8
Тема 4. Алгоритми консенсусу в технології блокчейн		-	8
Тема 5. Теорія складності та криптографічні задачі	2	-	8
Тема 6. Архітектура блокчейн-мереж		-	10
Тема 7. Тріада блокчейн: масштабованість, безпека, децентралізація		-	10
Тема 8. Смарт-контракти та платформи		-	10
Змістовий модуль 2. Конфіденційність та безпека блокчейн			
Тема 9. Аналіз вразливостей смарт-контрактів	2	2	10
Тема 10. Методи захисту блокчейн-мереж		-	10
Тема 11. Zero-Knowledge Proofs у блокчейні		2	8
Тема 12. Post-Quantum криптографія для блокчейну		-	10
Тема 13. Блокчейн та IoT / кіберфізичні системи	2	-	10
Тема 14. Перспективні напрямки розвитку блокчейну			10
Тема 15. Тенденції та майбутнє безпеки блокчейну			10
Разом	8	4	138

5. Тематика лабораторних занять

Лабораторна робота №1.

Тема: Криптографічні примітиви в блокчейні

Мета: Зрозуміти, як базові криптографічні примітиви – зокрема, геш-функції та дерево Меркла – забезпечують цілісність даних у блокчейні, і набути практичних навичок їх реалізації засобами Python.

Завдання:

1. Реалізувати криптографічну геш-функцію (SHA-256) у Python та перевірити її роботу на різних вхідних даних.
2. Побудувати просте дерево Меркла для заданого набору транзакцій (даних) у Python і обчислити його кореневий хеш.
3. Продемонструвати, як зміна вхідних даних впливає на геш значення та Merkle root, підтверджуючи незмінність і цілісність даних в блокчейні.

Лабораторна робота №2.

Тема: Асиметрична криптографія в блокчейні

Мета: Засвоїти роль асиметричної криптографії (публічних та приватних ключів) у забезпеченні безпеки транзакцій блокчейну через цифрові підписи, що гарантують автентичність та незмінність транзакцій, та навчитися генерувати ключі і підписи в Python.

Завдання:

1. Згенерувати пару ключів (приватний та публічний) за допомогою алгоритму на еліптичних кривих (як у Bitcoin/Ethereum) у Python.
2. Виконати цифровий підпис заданого повідомлення або “транзакції” приватним ключем і перевірити підпис за допомогою відповідного публічного ключа.

3. Обчислити блокчейн-адресу на основі згенерованого публічного ключа (наприклад, як у Bitcoin: через подвійне гешування RIPEMD160(SHA-256)) та перевірити правильність отриманої адреси.

Лабораторна робота №3.

Тема: Алгоритми консенсусу в технології блокчейн

Мета: Дослідити основні алгоритми консенсусу, які лежать в основі блокчейну, та зрозуміти, як вони забезпечують узгодженість реєстру між усіма вузлами без центрального органу. Набути практичних навичок шляхом моделювання спрощених версій цих алгоритмів у Python.

Завдання:

1. Реалізувати спрощений механізм консенсусу **Proof-of-Work**: написати скрипт, що знаходить **nonce** для блоку з даними так, щоб SHA-256 хеш блоку відповідав заданій умові складності (наприклад, мав N початкових нулів).
2. Змоделювати узгодження ланцюга: створити два конкурентні "ланцюги" блоків і продемонструвати правило вибору найдовшого ланцюга як валідного (імітація ситуації форку та його вирішення).
3. Реалізувати спрощений механізм **Proof-of-Stake**: присвоїти "вузлам" мережі певні ваги (частки) і запропонувати алгоритм випадкового вибору вузла для генерації наступного блоку пропорційно до його частки, демонструючи принцип PoS.

Лабораторна робота №4.

Тема: Смарт-контракти та платформи

Мета: Ознайомитися з поняттям смарт-контрактів як самовиконуваних програм на блокчейні, що автоматично реалізують угоди між сторонами без посередників, та отримати навички розробки і взаємодії зі смарт-контрактами на популярних платформах (наприклад, Ethereum) засобами Python.

Завдання:

1. Розробити простий смарт-контракт (наприклад, контракт зберігання даних або токен) мовою Solidity (або аналогічною) та скомпілювати його.
2. Розгорнути (деплоїти) цей смарт-контракт у тестовій блокчейн-мережі Ethereum (наприклад, Ganache або тестнет) за допомогою Python-скрипта з використанням бібліотеки Web3.py.
3. Написати Python-скрипт для взаємодії з розгорнутим смарт-контрактом: викликати його функції (читання стану або запис даних, наприклад, змінити значення змінної або виконати передачу токенів) та вивести результати виконання.

Лабораторна робота №5. Тема: Zero-Knowledge Proofs у блокчейні

Мета: Зрозуміти принцип **Zero-Knowledge Proofs** (доказів з нульовим розголошенням) та їх застосування у блокчейні – коли можна довести істинність твердження, не розкриваючи саму інформацію. Отримати практичний досвід реалізації простих прикладів ZKP-протоколів засобами Python.

Завдання:

1. Реалізувати простий інтерактивний протокол **Zero-Knowledge** у Python (наприклад, ідентифікаційну схему Шнорра): продемонструвати, як доводити знання секрету (такого як пароль або числовий ключ) без розкриття цього секрету.
2. Використати Python-бібліотеку для генерації або перевірки zk-SNARK чи подібного доказу (наприклад, бібліотеку PySNARK або аналогічну) на простому прикладі: згенерувати доказ для деякого твердження та верифікувати його, не розкриваючи початкові дані.
3. Продемонструвати інтеграцію ZKP у блокчейн-сценарій: наприклад, змоделювати перевірку правильності транзакції або права доступу за допомогою доказу з

нульовим розголошенням (щоб валідатор міг переконатися в істинності транзакції, не знаючи її деталей).

Лабораторна робота №6.

Тема: Постквантова криптографія для блокчейну

Мета: Ознайомитися з принципами постквантової криптографії – алгоритмами шифрування та підпису, стійкими до атак квантових комп'ютерів – та дослідити їх значення для майбутнього блокчейнів. Набути навичок використання таких алгоритмів у Python, враховуючи, що квантові обчислення становлять загрозу для сучасних схем цифрового підпису (наприклад, ECDSA) у блокчейні.

Завдання:

1. Згенерувати криптографічну ключову пару з використанням **постквантового** алгоритму (наприклад, схема цифрового підпису Dilithium, Falcon або SPHINCS+) за допомогою доступної Python-бібліотеки.
2. Підписати тестове повідомлення (транзакцію) отриманим постквантовим приватним ключем і перевірити підпис відповідним публічним ключем. Порівняти цей процес із аналогічною процедурою для традиційного ECDSA (наприклад, переконатися, що верифікація проходить, та зіставити кроки).
3. Проаналізувати і порівняти розмір ключів та підписів, а також швидкодію обраного постквантового алгоритму зі стандартним ECDSA. Обговорити, як вплинуло б впровадження постквантових алгоритмів на масштабованість та продуктивність блокчейн-систем (зважаючи на більший розмір даних і потенційно повільнішу роботу).

Лабораторна робота №7.

Тема: Блокчейн та IoT / кіберфізичні системи

Мета: Дослідити можливості поєднання технології блокчейн з Інтернетом речей (IoT) та кіберфізичними системами. Розробити прототип, що демонструє використання блокчейну для захищеного збереження і обміну даними датчиків, зняттям центральних точок відмови та підвищенням довіри в IoT-мережі, реалізувавши все на Python.

Завдання:

1. Запрограмувати генерацію даних від декількох віртуальних IoT-пристроїв у Python (наприклад, імітувати показники датчика температури або вологості, що генеруються кожні N секунд).
2. Реалізувати спрощений блокчейн-реєстр у Python для запису цих даних: створити структуру блока, додати механізм хешування попереднього блока в кожен новий блок (ланцюг хешів) і забезпечити додавання нових "транзакцій" з даними датчиків у блоки.
3. Продемонструвати роботу прототипу: додати кілька блоків з даними від різних пристроїв, а потім спробувати змінити дані в одному з попередніх блоків. Написати перевірку цілісності ланцюга (перерахунок хешів), щоб виявити факт фальсифікації даних – таким чином підтвердити, що блокчейн захищає дані IoT від непомітного втручання.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання наскрізного проєкту на тему «Реалізація блокчейну на мові Python».

Мета завдання - створити блокчейн з використанням мови програмування Python. Це дозволить студентам краще зрозуміти концепцію блокчейну, його структуру та основні принципи роботи.

Вимоги до реалізації:

1. Блок повинен містити наступні поля:

Індекс блоку в ланцюжку.

Timestamp (час створення блоку).

Дані (довільні дані, які будуть зберігатися в блоці).

Хеш попереднього блоку.

Нонс (число, яке використовується для майнінгу).

2. Ланцюжок блоків повинен зберігатися в списку.

3. Реалізувати функцію створення нового блоку, яка:

Отримує дані для нового блоку.

Розраховує хеш попереднього блоку в ланцюжку.

Виконує майнінг блоку (знаходить нонс, при якому хеш блоку починається з певної кількості нулів).

Створює новий блок з усіма необхідними полями.

Додає новий блок до ланцюжка.

4. Реалізувати функцію перевірки цілісності ланцюжка, яка:

Перевіряє, чи хеш кожного блоку відповідає його даним.

Перевіряє, чи хеш кожного блоку збігається з хешем, записаним в наступному блоці.

5. Додатково можна реалізувати:

Консольний інтерфейс для взаємодії з блокчейном.

Можливість додавати транзакції в блоки.

Алгоритм консенсусу Proof-of-Work (PoW).

Завдання для студентів:

1. Реалізуйте структуру блоку з необхідними полями.
2. Напишіть функцію створення нового блоку, яка виконує майнінг.
3. Реалізуйте функцію перевірки цілісності ланцюжка блоків.
4. Створіть консольний інтерфейс для взаємодії з блокчейном (додатково).
5. Додайте можливість додавання транзакцій в блоки (додатково).
6. Реалізуйте алгоритм консенсусу Proof-of-Work (додатково).

Це завдання дозволить студентам на практиці застосувати знання з математики та програмування для реалізації простого блокчейну. Воно охоплює основні концепції блокчейну, такі як структура блоку, ланцюжок блоків, майнінг та перевірка цілісності. Виконуючи це завдання, студенти зможуть краще зрозуміти, як працює блокчейн та його математичні основи.

7. Організація та проведення тренінгу з дисципліни «Блокчейн: математичні проблеми та застосування»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Реалізація блокчейну	1. Створення прототипу 2. Реалізація алгоритмів консенсусу 3. Постійна пам'ять та інтерфейс командного рядка 4. Транзакції 5. Адреси 6. Мережа
2	Тестування роботи блокчейну	Дослідження області застосування та шляхи удосконалення блокчейну

8. Методи навчання.

У освітньому процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «**Блокчейн: математичні проблеми та застосування**» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;

- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;
- підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами 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 здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, 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 «Блокчейн: математичні проблеми та застосування» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40 %
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-7.	Підсумкове тестування за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Виконання лабораторних робіт:

90-100 балів: здобувач освіти самостійно, без помилок, виконав усі кроки лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами цифрової криміналістики.

75-89 балів: здобувач освіти виконав завдання лабораторної роботи, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи.

60-74 балів: здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у лабораторній роботі завдань є поверхневим.

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

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 20 запитань, кожна правильна відповідь дає 5 балів, максимум 100 балів.

Тренінг:

90-100 балів: здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами тестування на проникнення;

75-89 балів: здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи;

60-74 балів: здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених завдань є поверхневим;

1-59 балів: здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з наданим програмним забезпеченням.

Самостійна робота:

90–100 балів: звіт охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмета. Дослідження містить не лише опис, але й глибокий аналіз, порівняння різних підходів та методів, а також обґрунтовані висновки. Використані сучасні та актуальні джерела інформації, що свідчить про обізнаність здобувачів освіти з останніми тенденціями у цифровій криміналістиці. Здобувач освіти вільно володіє матеріалом, виступає впевнено та відповідає на всі запитання.

75–89 балів: звіт розкриває основні питання теми, але може бути менш деталізованим. В роботі присутні аналітичні елементи, але вони можуть бути не достатньо глибокими. Використані джерела інформації є релевантними, але можуть бути не найновішими. Здобувач освіти демонструє знання матеріалу, але може мати незначні труднощі з відповідями на додаткові питання.

60–74 балів: звіт охоплює лише основні аспекти теми. Можуть бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач освіти не завжди впевнено відповідає на запитання. Виступ може бути нечітким.

1–59 балів: зміст звіту 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. Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитань, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів. За відповідь на питання здобувач отримує 16–30 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 практичне завдання:

30 – 40 балів: доповідь охоплює всі основні аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Здобувач вільно володіє матеріалом, відповідає впевнено на всі запитання.

21–30 балів: доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

11–20 балів: відповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Здобувач не завжди впевнено відповідає на запитання.

1–10 балів: відповідь містить значні помилки або не зовсім відповідає завданню.

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)

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

№	Найменування	Номер теми
1.	Мультимедійний проектор	1 - 15
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Опорний конспект лекцій з курсу «Блокчейн: математичні проблеми та застосування» для студентів спеціальності F5 «Кібербезпека та захист інформації» /Укл.: Яцків Н.Г., Яцків В.В. – Тернопіль: Вектор, 2025. – 76 с.
2. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.
3. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
4. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security Internet of Things: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", Ternopil National Economic University, 2019. – 98 p.
5. Song, J. *Programming bitcoin: Learn how to program bitcoin from scratch*. O'Reilly Media, 2019, 321 p.
6. V.Yatskiv, N.Yatskiv, O. Bandrivskyi. "Proof of Video Integrity Based on Blockchain", **in *Proc.*** *Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on*, 2019, pp. 431-434.
7. Liu, X., Yang, H., Li, G., Dong, H., & Wang, Z. (2021). A blockchain-based auto insurance data sharing scheme. *Wireless Communications and Mobile Computing*, Volume 2021, Article ID 3707906 https://doi.org/10.1155/2021/3707906
8. Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T., & Zhao, C. (2021). Blockchain-based efficient device authentication protocol for medical cyber-physical systems. *Security and Communication Networks*, Volume 2021, *2021*, Article ID 5580939, 13 p. https://doi.org/10.1155/2021/5580939
9. S.Son,J.Lee,M.Kim,S.Yu,A.K.Das,andY.Park,"Designof secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, 2020. – pp. 192177–192191
10. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, *23*(2), 947. https://doi.org/10.3390/s23020947

11. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain – Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, *23*(2), 947. https://doi.org/10.3390/s23020947

12. Bashir, I. Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3. Packt Publishing Ltd. 2023, 819 p.

13. Antonopoulos, A. M., & Harding, D. A. Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.", 2023.

14. Blockchain/Cryptocurrency. Режим доступу: https://asecuritysite.com/blockchain/

15. Elliptic Curve Cryptography (ECC). Режим доступу: https://asecuritysite.com/ecc/

16. Blockchain Demo. Режим доступу: https://andersbrownworth.com/blockchain/

17. REMIX. Режим доступу: https://remix.ethereum.org

18. Блокчейн. Режим доступу: https://research.kr-labs.com.ua/category/blockchain/