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

ЗАТВЕРДЖУЮ

Декан ФКІТ
Ігор ЯКИМЕНКО
_____
«__» _____ 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ
_____
«__» _____ 2024 р.

ЗАТВЕРДЖУЮ:
Директор ННІНОТ
Святослав ПИТЕЛЬ
_____
04 _____ 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Блокчейн: математичні проблеми та застосування»
ступінь вищої освіти – магістр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра спеціалізованих комп'ютерних систем

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. роботи (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	2	30	14	4	6	96	150	2
Заочна	1	2	8	4	-	-	138	150	3

Тернопіль – 2024

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 16. 10. 2024 р.

Завідувач кафедри
спеціалізованих комп'ютерних систем _____ Андрій СЕГІН

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 2 від 16. 10. .2024 р.

Голова групи
забезпечення спеціальності _____ Василь ЯЦКІВ

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 – 12 Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 4	Спеціальність – 125 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 – 30* *Заочна - 8* Практичні заняття (год): *Денна – 14* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 96* *Тренінг 6.* *Заочна – 138* Індивідуальна робота (год): *Денна – 4*
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 «**Технологія блокчейн**» 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. Технологія блокчейн.

Зростання технології блокчейн. Прогрес до зрілості. Зростання інтересу до блокчейн. Розподілені системи. Історія блокчейна. Біткоін. Електронна готівка.

Література: 1, 2.

Тема 2. Архітектура блокчейн.

Блокчейн за рівнями. Блокчейн в бізнесі. Загальні елементи блокчейну. Функціональність блокчейну. Переваги та особливості блокчейну. Обмеження технології блокчейн.

Література: 1, 2.

Тема 3. Типи блокчейна.

Розподілені книги. Спільна книга. Публічні блокчейни. Приватні блокчейни. Напівприватні блокчейни. Дозволена бухгалтерська книга. Повністю приватні та власні блокчейни. Токенізовані блокчейни. Блокчейни без токенів. Блокчейни 1-го рівня. Монолітні та полілітні блокчейни. Блокчейни 2-го рівня.

Література: 1, 3, 5.

Тема 4. Децентралізація.

Методи децентралізації. Конкурсна децентралізація. Кількісна оцінка децентралізації. Переваги децентралізації. Вимоги до оцінювання. Повна децентралізація екосистеми. Зберігання. Обчислювальна потужність. Децентралізація на практиці. Розумні контракти. Автономні агенти. Децентралізовані організації. Децентралізовані програми. Децентралізований веб.

Література: 2, 3, 6

Тема 5. Симетрична криптографія в блокчейн.

Послуги, що надаються криптографією. Криптографічні примітиви. Безключові примітиви. Випадкові числа. Хеш-функції. Симетричні ключові примітиви. Коди аутентифікації повідомлень. Секретні ключові шифри. Розширений стандарт шифрування. Стандарт шифрування даних. Як працює AES. Шифрування та дешифрування за допомогою AES.

Література: 1, 2, 3.

Тема 6. Асиметрична криптографія в блокчейн.

Фундаментальна математика. Відкриті та закриті ключі. Алгоритми асиметричної криптографії. Розкладання цілих чисел. Дискретний логарифм. Еліптичні криві. Інтегрована схема шифрування. Шифрування та дешифрування за допомогою RSA.

Література: 1, 2, 4.

Тема 7. Цифрові підписи в блокчейн.

Алгоритми цифрового підпису RSA. Генерація цифрових підписів RSA. Алгоритм цифрового підпису еліптичної кривої. Створення цифрових підписів ECDSA. Різні типи цифрових підписів. Сліпі підписи. Мультипідписи. Порогові підписи. Сукупність підписів. Кільцеві підписи.

Література: 1, 2, 5.

Тема 8. Математика еліптичних кривих.

Додавання точки. Подвоєння точки. Множення точки. Задача дискретного логарифмування. Генерація ключів за допомогою ECC. Визначення кривої для біткоіна. Робота з кривою secp256kl.

Література: 1, 2, 5.

Змістовий модуль 2. Конфіденційність та безпека блокчейн.

Тема 9. Криптографічні конструкції та технологія блокчейн.

Гомоморфне шифрування. Обмін секретами. Схеми зобов'язань. Докази з нульовим знанням. zk-SNARKs. zk-STARKs. Докази діапазону нульових знань. Схеми кодування. Base 64. Base 58. Перевірні випадкові функції.

Література: 2, 3, 9.

Тема 10. Алгоритми консенсусу.

Введення у консенсус. Відмовостійкість. Аналіз і проектування алгоритмів консенсусу. Алгоритми CFT. Алгоритми BFT. Алгоритм Istanbul Byzantine Fault Tolerance. Стани консенсусу. Консенсус Накамото. Варіанти PoW. Proof of Storage. Proof of Stake. HotStuff. Вибір алгоритму.

Література: 2, 3, 10

Тема 11. Архітектура біткоіна.

Криптографічні ключі. Приватні ключі в Bitcoin. Відкриті ключі в Bitcoin. Адреси. Типові біткоін-адреси. Розширені біткоін-адреси. Транзакції Coinbase. Життєвий цикл транзакції. Перевірка транзакції. Плата за транзакцію Структура даних транзакції. Метадані.

Література: 2, 3, 4, 11.

Тема 12. Структура блокчейн.

Структура. Блок генезису. Застарілі та бездіяльні блоки. Вилки. Підтвердження роботи (PoW). Системи Майнінг. Пули для майнінгу. Мережа. Типи повідомлень. Клієнтське програмне забезпечення. Фільтри Блума. Гаманці.

Література: 1, 2, 4.

Тема 13. Конфіденційність блокчейну.

Конфіденційність. Методи досягнення конфіденційності. Обфускація. Гомоморфне шифрування. Протоколи змішування. Шифрування на основі атрибутів. Анонімні підписи. Конфіденційність за допомогою протоколів рівня 2. Конфіденційність з використанням нульового знання. Криптографічні зобов'язання. Докази з нульовим знанням. Створення ZK-SNARK.

Література: 1, 2, 5, 12.

Тема 14. Безпека блокчейну.

Рівні блокчейну та атаки. Атаки відтворення транзакцій. Атаки на консенсусні протоколи. Подвійне витрачання. Розгалуження та реорганізація ланцюга. Прикладний рівень блокчейну. Атаки на гаманці. Атаки на блокчейни рівня 2. Атака на криптографію з відкритим ключем. Атаки на хеш-функції. Інструменти та механізм аналізу безпеки. Моделювання загроз. Регулювання та відповідність.

Література: 1, 2, 5, 10.

Тема 15. Застосування блокчейну та перспективи

Приклади використання. Інтернет речей. Архітектура IoT. Переваги конвергенції IoT і блокчейну. Впровадження IoT на основі блокчейну на практиці. Налаштування Raspberry Pi. Налаштування першого вузла. Налаштування вузла Raspberry Pi.

Література: 1, 2, 5, 12.

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

	Кількість годин					
	Лекції	Практ. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Криптографія в блокчейн						
Тема 1. Технологія блокчейн	2		4	2	3	Поточне опитування
Тема 2. Архітектура блокчейн	2		4			
Тема 3. Типи блокчейна	2	2	4			
Тема 4. Децентралізація	2	2	4			
Тема 5. Симетрична криптографія в блокчейн	2	2	8			
Тема 6. Асиметрична криптографія в блокчейн	2	2	8			
Тема 7. Цифрові підписи в блокчейн	2	2	8			
Тема 8. Математика еліптичних кривих.	2		8			
Змістовий модуль 2. Конфіденційність та безпека блокчейн						
Тема 9. Криптографічні конструкції та технологія блокчейн	2		8	2	3	Поточне опитування
Тема 10. Алгоритми консенсусу	2	2	8			
Тема 11 Архітектура біткоіна	2		8			
Тема 12. Структура блокчейн	2	2	6			
Тема 13. Конфіденційність блокчейну	2		8			
Тема 14. Безпека блокчейну	2		4			
Тема 15. Застосування блокчейну та перспективи	2		6			
Разом	30	14	96	4	6	

4.2 Структура залікового кредиту

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

	Кількість годин		
	Лекції	Практичні заняття	Самостійна робота
Змістовий модуль 1. Криптографія в блокчейн			
Тема 1. Технологія блокчейн	2	-	8
Тема 2. Архітектура блокчейн		-	8
Тема 3. Типи блокчейна		-	8
Тема 4. Децентралізація		-	8
Тема 5. Симетрична криптографія в блокчейн	2	-	8
Тема 6. Асиметрична криптографія в блокчейн		-	10
Тема 7. Цифрові підписи в блокчейн		-	10
Тема 8. Математика еліптичних кривих.		-	10

Змістовий модуль 2. Конфіденційність та безпека блокчейн			
Тема 9. Криптографічні конструкції та технологія блокчейн	2	2	10
Тема 10. Алгоритми консенсусу		-	10
Тема 11. Архітектура біткоіна		2	8
Тема 12. Структура блокчейн		-	10
Тема 13. Конфіденційність блокчейну	2	-	10
Тема 14. Безпека блокчейну			10
Тема 15. Застосування блокчейну та перспективи			10
Разом	8	4	138

5. Тематика практичних (семінарських або лабораторних) занять

Практичне заняття №1

Тема: *Принципи роботи криптовалюти біткоін.*

Питання для обговорення:

1. Відправлення та отримання біткоінів
2. Звичайні форми транзакцій.
3. Конструкція транзакції.

Література: 2, 3, 11.

Практичне заняття №2

Тема: *Криптографія та криптовалюти.*

Питання для обговорення:

1. Поняття хеш – функції.
2. Алгоритми обчислення хеш – функції.
3. Дослідження хеш – функції.
4. Алгоритми шифрування з відкритими ключами.
5. Алгоритми шифрування із закритими ключами.

Література: 3, 12.

Практичне заняття №3

Тема: Принципи технології Blockchain

Питання для обговорення:

1. Структура блоку. Заголовок блоку. Блок генезису.
2. З'єднання блоків у Blockchain.
3. Дерево Меркле (Merkle).

Література: 1, 2, 5.

Практичне заняття №4

Тема: Алгоритми доказу виконаної роботи **ля обговорення**

Питання для обговорення:

1. PoS (Proof of Stake),
2. DPoS (delegated Proof of Stake),
3. Proof of Activity (PoW + PoS),
4. Proof of Burn, Proof of Capacity, Proof-of-Storage, PoSe (proof-of-service)

Література: 4, 5.

Практичне заняття №5

Тема: Мережа Bitcoin

1. Питання для обговорення:
2. Архітектура однорангової мережі.
3. Типи вузлів і їх задачі.
4. Розширена мережа Bitcoin.

Література: 2, 3.

Практичне заняття №6

Тема: Проект Ethereum

Питання для обговорення:

1. Середовище розробки.
2. Мови програмування для платформи Ethereum (Serpent; Mutan; Solidity; LLL).
3. Ethereum – акаунти.
4. Повідомлення і транзакції.
5. Виконання коду. Блокчейн і майнінг.
6. Децентралізоване зберігання файлів.

Література: 4, 5.

Практичне заняття №7

Тема: Платформи для проектування додатків на основі технології блокчейн

Питання для обговорення:

1. Azure Blockchain Service Microsoft,
2. IBM Watson IoT.
3. Amazon Blockchain IoT.

Література: 3, 4.

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 навчальному 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.

10. 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 лабора-торних робіт №1-7.	Підсумкова письмова робота за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	1. 15тестів по 4 бали - max 60 балів. 2.Практич-не завдання - max 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.	Мультимедійний проектор	1 - 15
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. 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.
2. 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.
3. 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.
4. Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 2. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 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