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

ЗАТВЕРДЖУЮ

В.о. декана ФКІТ
Ігор ЯКИМЕНКО

«_____» 2023 р.

ЗАТВЕРДЖУЮ

В.о. проректора з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ

«_____» 2023 р.

РОБОЧА ПРОГРАМА

з дисципліни «Блокчейн та цифрові валюти»
ступінь вищої освіти – бакалавр
галузь знань - 15 Автоматизація та приладобудування
спеціальність – 151 Автоматизація та комп'ютерно-інтегровані технології
освітньо-професійна програма – Інформаційні системи та технології

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Зал. (сем.)
Денна	3	6	28	14	3	6	99	150	6

Тернопіль – 2023

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Автоматизація, комп'ютерно-інтегровані технології та робототехніка,
протокол № 1 від 31.08 2023 р.

Голова групи
забезпечення спеціальності Андрій СЕГІН

Гарант ОП Ігор ПІТУХ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Блокчейн та цифрові валюти»

Дисципліна «Блокчейн та цифрові валюти»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 5	Галузь знань 15 Автоматизація та приладобудування	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 3	Спеціальність – 151 Автоматизація та комп'ютерно-інтегровані технології	Рік підготовки: *Денна – 3* Семестр: *Денна – 6*
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год): *Денна – 28* Практичні заняття (год): *Денна – 14*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 99* *Тренінг (год).* *Денна – 6* *КПІЗ (год).* *Денна – 3* Індивідуальна робота (год): *Денна – 3*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни «Блокчейн та цифрові валюти»

2.1. Мета вивчення дисципліни.

Метою дисципліни «**Блокчейн та цифрові валюти**» 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 та цифрові валюти**» отримання студентами теоретичних знань, спеціальних умінь і практичних навичок з використання технології блокчейн.

2.3. В результаті вивчення дисципліни студент повинен знати:

- методи, алгоритми та програмні засоби забезпечення цілісності та конфіденційності даних в технології блокчейн;
- криптографію на основі еліптичної кривої;
- структуру даних Дерева Merkle;
- принцип функціонування блокчейн;
- 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 різні типи платформ для розробки додатків на основі технології блокчейн.

3. Програма навчальної дисципліни: «Блокчейн та цифрові валюти»

Змістовий модуль 1. Технологія блокчейн.

Тема 1. Поняття криптовалюти. Історія криптовалюти біткоін. Використання криптовалюти. Отримання перших біткоінів. Альтернативні криптовалюти.

Література: 1, 2, 3.

Тема 2. Принципи роботи криптовалюти біткоін. Відправлення та отримання бітконів. Операції, блоки, гірництво та блокчейн. Звичайні форми транзакцій. Конструкція транзакції. Додавання транзакції до заголовку. Витрата транзакції.

Література: 2, 3, 4.

Тема 3. Основи криптографії. Поняття хеш – функції. Введення в криптографію відкритого ключа. Приватні та публічні ключі. Криптографія на основі еліптичної кривої. Генерування відкритого ключа. Біткоін адреси.

Тема 4. Різновиди цифрових підписів. Схеми одноразового підпису. Lamport one time signature. Чому одноразовий підпис "одноразовий"? Мультипідпис. Пороговий підпис. Груповий підпис. Кільцевий підпис. Сліпий підпис.

Література: 1, 2,

Тема 5. Принципи технології Blockchain. Структура блоку. Заголовок блоку. Блок генезису. З'єднання блоків у Blockchain. Дерево Меркле (Merkle). Дерева Merkle та спрощена перевірка платежу (SPV).

Література: 2, 5, 7.

Тема 6. Алгоритми доказу виконаної роботи. PoW (Proof-of-work). PoS (Proof of Stake), DPoS (delegated Proof of Stake), = Proof of Activity (PoW + PoS),
Proof of Burn, Proof of Capacity, Proof-of-Storage, PoSe (proof-of-service).

Література: 2, 3, 5.

Змістовий модуль 2. Проектування додатків на основі технології блокчейн.

Тема 7. Мережа Bitcoin. Архітектура однорангової мережі. Типи вузлів і їх задачі. Розширена мережа Bitcoin. Повні вузли. Бази даних транзакцій

Література: 2, 4, 7

Тема 8. Формати ключів у Bitcoin. Поняття стиснутого відкритого ключа. Формати особистих ключів. Формати відкритих ключів.

Література: 2, 4, 5

Тема 9. Проект Ethereum. Середовище розробки. Мови програмування для платформи Ethereum (Serpent; Mutan; Solidity; LLL). Ethereum –акаунти. Повіомлення і транзакції. Функція зміни стану в Ethereum. Виконання коду. Блокчейн і майнінг. Децентралізоване зберігання файлів.

Література: 2, 5, 7

Тема 10. Платформи для проектування додатків на основі технології блокчейн. Azure Blockchain Service Microsoft, IBM Watson IoT.

Література: 2, 4, 5.

Тема 11. Безпека та надійність Інтернет речей на основі технології блокчейн. Інтернет речей (IoT). Існуючі проблеми та загрозами при розгортанні IoT. Використання підходу на основі блокчейн.

Література: 2, 7, 8.

Тема 12. Використання технології блокчейн. «Розумні» контракти, Інтернет речей, логістика, юриспруденція, медицина, державні реєстри.

Література: 1, 3, 8, 9.

4. Структура залікового кредиту з дисципліни «Блокчейн та цифрові валюти»
4.1 Денна форма навчання

	Кількість годин					
	Лекції	Практичні заняття	ІРС	СРС	Тре-нінг, КПІЗ	Контро-льні заходи
Змістовий модуль 1. Технологія блокчейн						
Тема 1. Поняття криптовалюти.	2			5	3	Поточне опитування
Тема 2. Принципи роботи криптовалюти біткоін	2			8		Поточне опитування
Тема 3. Основи криптографії.	4	2	1	10		Поточне опитування
Тема 4. Різновиди цифрових підписів.	2	2	1	10		Поточне опитування
Тема 5. Принципи технології Blockchain	2	2		8		Поточне опитування
Тема 6. Алгоритми доказу виконаної роботи	4	2	1	8		Поточне опитування
Змістовий модуль 2. Проектування додатків на основі технології блокчейн						
Тема 7. Мережа Bitcoin.	2	2		8	3	Поточне опитування
Тема 8. Формати ключів у Bitcoin	2			8		Поточне опитування
Тема 9. Проект Ethereum.	2			10		Поточне опитування
Тема 10. Платформи для проектування додатків на основі технології блокчейн	2	2		8		Поточне опитування
Тема 11. Безпека та надійність Інтернет речей на основі технології блокчейн	2	2		8		Поточне опитування
Тема 12. Використання технології блокчейн	2			8		Поточне опитування
Разом	28	14	3	99	6	

5. Тематика практичних занять
Практичне заняття №1
Тема: *Принципи роботи криптовалюти біткоін.*
Питання д ля обговорення:
1. Відправлення та отримання біткоінів
2. Звичайні форми транзакцій.
3. Конструкція транзакції.

Література: 2, 3

Практичне заняття №2
Тема: *Основи криптографії-1*
Питання для обговорення:
1. Поняття хеш – функції.
2. Алгоритми обчислення хеш – функції.
3. Дослідження хеш – функції.

Література: 6.

Практичне заняття №3
Тема: *Основи криптографії-2*

Питання для обговорення:
1. Алгоритми шифрування з відкритими ключами.
2. Алгоритми шифрування із закритими ключами.
Література: 2,3, 5

Практичне заняття №4
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 №5
Тема: Алгоритми доказу виконаної роботи **ля обговорення**
Питання для обговорення:
1. PoW (Proof-of-work).
2. PoS (Proof of Stake),
3. DPoS (delegated Proof of Stake),
4. Proof of Activity (PoW + PoS),
5. Proof of Burn, Proof of Capacity, Proof-of-Storage, PoSe (proof-of-service)
Література: 4, 5.

Практичне заняття №6
Тема: Мережа Bitcoin
Питання для обговорення:
1. Архітектура однорангової мережі.
2. Типи вузлів і їх задачі.
3. Розширена мережа Bitcoin.

Література: 2, 3.

Практичне заняття №7
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, 6.

6. Комплексне практичне індивідуальне завдання
Варіанти КПІЗ з дисципліни «Блокчейн та цифрові валюти»

1. Студенти виконують завдання на тему "Розробка додатку на основі технології блокчейн". Кожен студент отримує варіант завдання. Завдання складається з таких розділів: постановка задачі; розробка структури та алгоритму роботи; розробка додатку з використанням блокчейн платформи; тестування додатку. Студент може самостійно запропонувати та погодити з викладачем тему КПІЗ.
2. Студенти можуть виконувати наукові дослідження з області Інтернет речей та технології блокчейн з апробацією результатів на щорічній науковій конференції молодих вчених та студентів ЗУНУ та на інших наукових форумах.

7. Самостійна робота

№ п/п	Тематика
1	Принципи роботи криптовалюти біткоін
2	Приватні та публічні ключі.
3	Криптографія на основі еліптичної кривої.
4	Генерування відкритого ключа. Біткоін адреси.
5	Поняття хеш – функції
6	Принципи технології Blockchain.
7	Дерево Меркле (Merkle)
8	Алгоритми доказу виконаної роботи
9	Архітектура однорангової мережі.
10	Мережа Bitcoin
11	Проект Ethereum
12	Блокчейн і майнінг
13	Платформи для проектування додатків на основі технології блокчейн
14	Безпека та надійність Інтернет речей на основі технології блокчейн.
15	Використання технології блокчейн: «Розумні» контракти
16	Використання технології блокчейн: Інтернет речей
17	Використання технології блокчейн: Логістика
18	Використання технології блокчейн: Юриспруденція
19	Використання технології блокчейн: Медицина
20	Використання технології блокчейн: державні реєстри.

8. Організація та проведення тренінгу з дисципліни «Блокчейн та цифрові валюти»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Реалізація блокчейну	1. Створення прототипу 2. Реалізація алгоритму Proof-of-Work 3. Постійна пам'ять та інтерфейс командного рядка 4. Транзакції 5. Адреси 6. Мережа
2	Запуск блокчейну	Тестування та дослідження роботи блокчейну. Область застосування та шляхи удосконалення блокчейну.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «**Блокчейн та цифрові валюти»** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- залікове модульне тестування та опитування;
- презентації результатів виконаних завдань та досліджень;
- оцінювання результатів КПІЗ;
- ректорська контрольна робота.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни “**Блокчейн та цифрові валюти** ” визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для заліку

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
30 %	40 %	30 %
1. Усне опитування на заняттях – max 6*4=24 бали. 2. Письмова робота – max 52 балів. 3. Практичне завдання – max 4*6=24 балів	1. Усне опитування на заняттях – max 6*4=24 балів. 2. Письмова робота – max 58 балів. 3. Практичне завдання – max 3*6=18 балів	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 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 - 12
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 12

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. A. Panarello, N.Tapas, G.Merlino, F.Longo, A.Puliafito “Blockchain and IoT integration: A systematic survey”. ***Sensors****, vol.***18(8),** *2575,* pp.1-37, 2018.
8. M. Salimitari, M. Chatterjee. “An Overview of Blockchain and Consensus Protocols for IoT Networks”. arXiv preprint arXiv:1809.05613, 2018.
9. B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, R.Ranjan. “IoT Chain: Establishing trust in the internet of things ecosystem using blockchain”. *IEEE Cloud Computing*, vol.5(4), pp.12-23, 2018.
10. 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
11. 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
12. 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