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 децентралізовані системи»
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, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	3	6	28	14	3	8	97	150	6

31.08.2023

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 кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант ОП _____ Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Блокчейн та децентралізовані системи»

Дисципліна «Блокчейн та децентралізовані системи»	**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 – 3	Спеціальність 125 «Кібербезпека»	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 – 97* *Тренінг, КПІЗ (год).* *Денна – 8* Індивідуальна робота (год): *Денна – 3*
Тижневих годин – 11, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни «Блокчейн та децентралізовані системи»

2.1. Мета вивчення дисципліни.

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

2.3. В результаті вивчення дисципліни студент повинен знати:

− принципи та переваги децентралізації;

- 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.

− застосовувати алгоритми консенсус у децентралізованих системах..

3. Програма навчальної дисципліни: «Блокчейн та децентралізовані системи»

Змістовий модуль 1. **Технології блокчейн.**

Тема 1. Вступ до криптографії та криптовалют.

Криптографічні хеш-функції. Хеш-вказівники та структури даних. Цифрові підписи. Відкриті ключі як ідентичність. Проста криптовалюта.

Література: 1, 2.

***Тема* 2**. Децентралізація та криптовалюта біткоін.

Централізація проти децентралізації. Розподілений консенсус. Консенсус без ідентичності з використанням ланцюжка блоків. Стимули та доказ роботи.

Література: 1, 2.

***Тема 3*.** 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: 1, 3, 5.

Тема 4. Механізм біткоінів.

Біткоін-операції. Сценарії біткоінів. Застосування скриптів біткоін. Біткоін-блоки.

Мережа біткоінів. Обмеження та вдосконалення.

Література: 2, 3, 6

Тема 5. *Я*к зберігати та використовувати біткоіни.

Просте локальне сховище. Гаряче та холодне зберігання. Розбиття та спільне використання ключів. Інтернет-гаманці та біржі. Платіжні послуги. Комісія за транзакції. Ринки валютних бірж.

Література: 1, 2, 3.

Тема 6. Видобуток біткоінів.

Завдання майнерів біткоінів. Обладнання для майнінгу. Енергоспоживання та екологія. Гірничі стимули та стратегії.

Література: 1, 2, 4,

Тема 7. Біткоіни та анонімність.

Основи анонімності. Як деанонімізувати біткоін. Змішування. Децентралізоване змішування. Zerocoin і Zerocash.

Література: 1, 2, 5,

Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти

Тема 8. Політика та регулювання.

Консенсус у біткоінах. Основне програмне забезпечення Bitcoin. Зацікавлені сторони: Хто відповідає? Коріння біткоіна. Уряди звертають увагу на біткоін. Заборона відмивання грошей.

Література: 2, 3, 9.

Тема 9. Альтернативні обчислювальні задачі.

Основні вимоги до обчислювальних задач (головоломок). Стійкі до ASIC головоломки. Підтвердження корисної роботи. Головоломки, що не підлягають передачі. Доказ ставки та віртуальний майнінг.

Література: 2, 3, 10

Тема 10. Біткоін як платформа.

Біткоін як журнал лише додатків. Біткоіни як "розумне майно". Захист багатосторонніх лотерей у біткоінах. Біткоін як публічне джерело випадковості. Ринки прогнозування та канали даних у реальному світі.

Література: 2, 3, 4, 10.

Тема 11. Альткоїни та екосистема криптовалют.

Альткоїни: історія та мотивація. Декілька деталей альткоїнів. Взаємозв'язок між біткоінами та альткойнами. Майнінг злиття. Альткойни з підтримкою біткоінів, "Бічні ланцюги". Ethereum та смарт-контракти

Література: 1, 2, 4.

Тема 12. Децентралізовані системи: майбутнє біткоінів?

Ланцюг блоків як засіб для децентралізації. Шляхи до блокування ланцюгової інтеграції. Шаблон для децентралізації. Коли децентралізація є гарною ідеєю?

Література: 1, 2, 5, 10.

4. Структура залікового кредиту
з дисципліни «Блокчейн та децентралізовані системи» (денна форма навчання)

	Кількість годин					
	Лекції	Прак-тичні заняття	СРС	ІРС	Тренінг, КПІЗ	Контро-льні заходи
Змістовий модуль 1. Технології блокчейн						
Тема 1. Криптографії та криптовалюти	2		7		4	Опитування під час заняття
Тема 2. Децентралізація та криптовалюта біткоін	2		8			Опитування під час заняття
Тема 3. Алгоритми доказу виконаної роботи	4	2	10	1		Опитування під час заняття, оцінювання практ. занять
Тема 4. Механізм біткоінів	2	2	8	1		Опитування під час заняття, оцінювання практ. занять
Тема 5. Як зберігати та використовувати біткоіни	2	2	8			Опитування під час заняття, оцінювання практ. занять
Тема 6. Видобуток біткоінів	2	2	8	1		Опитування під час заняття, оцінювання практ. занять
Тема 7. Біткоіни та анонімність	2		8			Опитування під час заняття
Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти						
Тема 8. Політика та регулювання	2		8		4	Опитування під час заняття
Тема 9. Альтернативні обчислювальні задачі	2	2	8			Опитування під час заняття, оцінювання практ. занять
Тема 10. Біткоін як платформа	2	2	8			Опитування під час заняття, оцінювання практ. занять
Тема 11. Альткоїни та екосистема криптовалют	4	2	8			Опитування під час заняття, оцінювання практ. занять
Тема 12. Децентралізовані системи: майбутнє біткоінів.	2		8			Опитування під час заняття
Разом	28	14	97	3	8	

5. Тематика практичних (семінарських або лабораторних) 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, 10.

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. Комплексне практичне індивідуальне завдання
Варіанти КПІЗ з дисципліни «**Блокчейн та децентралізовані системи**»
Розробка системи виявлення та запобігання вторгнень.
1. Постановка задачі.
2. Збір інформації та пошук цілей.
3. Визначення структури системи
4. Розробка правил
5. Дослідження роботи системи.
6. Висновки.

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	Протоколи Whisper и Swarm
11	Структура смарт-контракту
12	Мережа Bitcoin
13	Проект Ethereum
14	Блокчейн і майнінг
15	Платформи для проектування додатків на основі технології блокчейн
16	Безпека та надійність Інтернет речей на основі технології блокчейн
17	Використання технології блокчейн: «Розумні» контракти
18	Використання технології блокчейн: Інтернет речей
19	Використання технології блокчейн: Логістика
20	Використання технології блокчейн: Юриспруденція
21	Використання технології блокчейн: Медицина
22	Використання технології блокчейн: державні реєстри

8. Організація та проведення тренінгу з дисципліни з дисципліни «Блокчейн та децентралізовані системи»

№ 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 « » використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

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

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Блокчейн та децентралізовані системи**» 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 7*3=21 бали. 2. Письмова робота – max 55 балів. 3. Практичне завдання – max 4*6=24 балів	1. Усне опитування на заняттях – max 5*3=15 балів. 2. Письмова робота – max 55 балів. 3. Практичне завдання – max 3*10=30 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. Drescher, D. *Blockchain basics* (Vol. 276). Berkeley, CA: Apress. 2017. http://www.softouch.on.ca/kb/data/Blockchain%20Basics.pdf
4. 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.
5. 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.
6. M. Salimitari, M. Chatterjee. "An Overview of Blockchain and Consensus Protocols for IoT Networks". arXiv preprint arXiv:1809.05613, 2018.
7. 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.
8. 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.
9. 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.
10. 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