

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



2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Блокчейн та децентралізовані системи»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практичні заняття (год.)	ІРС (год.)	Тренінг. (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	3	6	32	14	3	6	95	150	6

29.08.2025
[Signature]

Тернопіль – 2025

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

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол
№ 1 від 26. 08. 2025 р.

Завідувач кафедри кібербезпеки



Василь ЯЦКІВ

Гарант освітньо-професійної
програми



Михайло КАСЯНЧУК

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 та захист інформації»	Рік підготовки: <i>Денна – 3</i> Семестр: <i>Денна – 6</i>
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції (год): <i>Денна – 32</i> Практичні заняття (год): <i>Денна – 14</i>
Загальна кількість годин – 150		Самостійна робота (год): <i>Денна – 95</i> <i>Тренінг (год): денна – 6</i> Індивідуальна робота (год): <i>Денна – 3</i>
Тижневих годин – 10, 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 здобувачів 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 здобувачами теоретичних знань, спеціальних умінь і практичних навичок з використання технології блокчейн.

2.3. В результаті вивчення дисципліни здобувач 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 біткоїн;
- формати ключів у Bitcoin.

2.4. В результаті вивчення дисципліни здобувач 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.

Тема 2. Децентралізація та криптовалюта біткоїн.

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

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).

Тема 4. Механізм біткоїнів.

Біткоїн-операції. Сценарії біткоїнів. Застосування скриптів біткоїн. Біткоїн-блоки. Мережа біткоїнів. Обмеження та вдосконалення.

Тема 5. Як зберігати та використовувати біткоїни.

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

Тема 6. Видобуток біткоїнів.

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

Тема 7. Біткоїни та анонімність.

Основи анонімності. Як деанонізувати біткоїн. Змішування. Децентралізоване змішування. Zerocoin і Zerocash.

Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти

Тема 8. Політика та регулювання.

Консенсус у біткоїнах. Основне програмне забезпечення Bitcoin. Зацікавлені сторони: Хто відповідає? Коріння біткоїна. Уряди звертають увагу на біткоїн. Заборона відмивання грошей.

Тема 9. Альтернативні обчислювальні задачі.

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

Тема 10. Біткоїн як платформа.

Біткоїн як журнал лише додатків. Біткоїни як "розумне майно". Захист багатосторонніх лотерей у біткоїнах. Біткоїн як публічне джерело випадковості. Ринки прогнозування та канали даних у реальному світі.

Тема 11. Альткоїни та екосистема криптовалют.

Альткоїни: історія та мотивація. Декілька деталей альткоїнів. Взаємозв'язок між біткоїнами та альткоїнами. Майнінг злиття. Альткоїни з підтримкою біткоїнів, "Бічні ланцюги". Ethereum та смарт-контракти

Тема 12. Децентралізовані системи: майбутнє біткоїнів?

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

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

	Кількість годин					
	Лекції	Практичні заняття	ІРС	Тренінг	СРС	Контрольні заходи
Змістовий модуль 1. Технології блокчейн						
Тема 1. Криптографії та криптовалют	2		1	3	7	Поточне опитування
Тема 2. Децентралізація та криптовалюта біткоїн	2				8	
Тема 3. Алгоритми доказу виконаної роботи	4	2			8	
Тема 4. Механізм біткоїнів	4	2			8	
Тема 5. Як зберігати та використовувати біткоїни	4	2			8	
Тема 6. Видобуток біткоїнів	2	2			8	
Тема 7. Біткоїни та анонімність	2				8	
Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти						
Тема 8. Політика та регулювання	2		2	3	8	Поточне опитування
Тема 9. Альтернативні обчислювальні задачі	2	2			8	
Тема 10. Біткоїн як платформа	2	2			8	
Тема 11. Альткоїни та екосистема криптовалют	4	2			8	
Тема 12. Децентралізовані системи: майбутнє біткоїнів.	2				8	
Разом	32	14	3	6	95	

5. Тематика практичних занять

Практичне заняття №1

Тема: Принципи роботи криптовалюти біткоїн.

Питання для обговорення:

1. Відправлення та отримання біткоїнів
2. Звичайні форми транзакцій.
3. Конструкція транзакцій.

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.

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).

Практичне заняття №4

Тема: Алгоритми доказу виконаної роботи

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)

Практичне заняття №5

Тема: Мережа Bitcoin

Питання для обговорення:

1. Архітектура однорангової мережі.
2. Типи вузлів і їх задачі.
3. Розширена мережа Bitcoin.

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.

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.

6. Самостійна робота

Самостійне завдання здобувача полягає у виконанні наскрізного завдання «Розробка простого блокчейн-додатку».

Мета завдання. Ознайомити здобувачів з основами технології блокчейн, принципами її роботи, а також навчити їх розробляти прості додатки на основі блокчейн-технологій.

Завдання. Здобувачі повинні створити простий блокчейн-додаток, який реалізує функціонал зберігання та верифікації транзакцій. Додаток повинен включати наступні компоненти:

1. Структура блоку:
 - 1) ідентифікатор блоку (номер блоку);
 - 2) хеш попереднього блоку;
 - 3) час створення блоку;
 - 4) список транзакцій;
 - 5) хеш блоку.
2. Транзакції: створити просту структуру для транзакцій, яка включає:
 - 1) відправник;
 - 2) одержувач;
 - 3) сума;
 - 4) Час створення транзакції.

3. Основні функції:

- 1) додавання нового блоку до блокчейну;
- 2) верифікація цілісності блокчейну (перевірка хешу);
- 3) виведення інформації про блокчейн (всі блоки та транзакції).

Технології: мова програмування: Python/JavaScript/Java (на вибір).

Бібліотеки:

- 1) для Python: Flask для створення API, hashlib для хешування;
- 2) для JavaScript: Express для створення API, crypto для хешування;
- 3) для Java: Spring Boot для створення API, java.security для хешування.

Кроки виконання:

1. Дослідження:

- 1) ознайомитися з основами блокчейн-технології;
- 2) вивчити принципи роботи хеш-функцій та їх роль у блокчейні.

2. Розробка:

- 1) створити структуру блоку та транзакції;
- 2) реалізувати функцію додавання блоку до блокчейну;
- 3) реалізувати верифікацію блокчейну.

3. Тестування.

1. Провести тестування на коректність роботи додатку.
2. Перевірити, чи правильно відображаються дані про транзакції та блоки.

4. Презентація. Підготувати коротку презентацію (5-10 хвилин) про реалізований проект, описати обрані технології, алгоритми та результати тестування.

Термін виконання. Завдання має бути виконано та представлене до 15 навчального тижня.

Рекомендації:

- 1) використовуйте Git для контролю версій вашого проекту.
- 2) досліджуйте існуючі блокчейн-проекти для натхнення.
- 3) пам'ятайте про безпеку даних при розробці.

7. Організація та проведення тренінгу 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.

8. Методи навчання.

У освітньому процесі застосовуються: лекції, в тому числі з використання мультимедійного проєктора, практичні роботи, індивідуальні заняття; самостійна робота.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Блокчейн та децентралізовані системи» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання практичних робіт;
- оцінювання тренінгів;

– оцінювання результатів самостійної роботи.

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 та децентралізовані системи» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для заліку

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за захист робіт № 1-7.	Підсумкове модульне тестування за темами №1-12.	Визначається як середнє арифметичне з оцінок за виконання завдань тренінгу.	Визначається як оцінка за наскрізне завдання самостійної роботи.

Виконання практичних робіт:

90-100 балів: здобувач самостійно, без помилок, виконав усі кроки в рамках роботи, правильно задокументував етапи та вільно оперує поняттями та принципами, що відносяться до теми дисципліни.

75-89 балів: здобувач виконав завдання 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: здобувач виконав завдання роботи, але з суттєвими помилками, наприклад, не з першого разу чи не до кінця. Розуміння поставлених у роботі завдань є поверхневим та неповним.

1-59 балів: здобувач 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 теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 25 запитань кожна правильна відповідь дає 4 бали, 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 дисципліни.

75-89 балів: здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат, в процесі роботи виникали додаткові запитання.

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

1-59 балів: здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував достатній рівень навичок роботи з апаратним та програмним забезпеченням.

Самостійна робота.

1. Коректність реалізації (40 балів). 31 – 40 балів отримує рішення, яке повністю відповідає вимогам: транзакції мають чітку структуру (мінімум поля відправник/одержувач/сума та детерміноване серіалізування), блок містить індекс/мітку часу/список транзакцій/prev_hash/власний hash, додавання блоку перевіряє узгодженість prev_hash із hash попереднього блоку, а функція верифікації проходить увесь ланцюг, повторно обчислює хеші та коректно виявляє будь-яку модифікацію даних (у т.ч. всередині транзакцій).

16 – 30 балів, якщо ланцюг формально працює, але є прогалини (напр., не перевіряються всі блоки, неконсистентна серіалізація перед хешуванням, не обробляються крайові випадки).

1– 15 балів, якщо додавання/верифікація працюють нестабільно або ланцюг не виявляє спотворення даних.

2. Якість коду (30 балів). Оцінюється архітектура та підтримуваність: розділення на логічні сутності (напр., Transaction, Block, Blockchain), чисті інтерфейси, осмислені назви, відсутність дублювання, коментарі лише там, де це підсилює розуміння.

21 – 30 балів за чистий, модульний, протестований код з осмисленою історією комітів;

11 – 20 балів за робочий, але «монолітний» або слабко документований;

1-10 балів за спагеті-код, «хардкод», відсутність тестів та інструкцій.

3. Презентація (30 балів). 21 – 30 балів за чітку, структуровану доповідь 5–10 хв із фокусом на суті: мета проєкту, модель даних (формат транзакції/блоку), обрана хеш-функція і спосіб серіалізації, алгоритм додавання та верифікації, коротка демонстрація (нормальний сценарій + спроба підміни з показом, як це виявляється), результати тестування (які кейси, які очікувані/фактичні результати, час на побудову/перевірку N блоків), обмеження (напр., відсутність мережі/консенсусу/підписів) і можливі покращення. Слайди лаконічні, терміни вжиті коректно, є посилання на репозиторій.

11 – 20 балів за загалом зрозумілу, але перевантажену або недостатньо доказову доповідь без якісної демонстрації тестів чи без чітких висновків.

1-10 балів за нечітку структуру, плутанину в термінах, відсутність демонстрації або вихід за таймінг із малим змістом.

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		D (задовільно)
60–64	задовільно	E (достатньо)
35–59		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 - 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. Скрыбін, 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. Скрыбін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
3. V.Yatskiv, N.Yatskiv, O. Bandrivskiy. “Proof of Video Integrity Based on Blockchain”, in *Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on*, 2019, pp. 431-434.
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. 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.
6. 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>
7. Xu, J., Wang, C., & Jia, X. (2023). A survey of blockchain consensus protocols. *ACM Computing Surveys*, 55(13s), 1-35. <https://doi.org/10.1145/3579845>
8. Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain integration in the era of industrial metaverse. *Applied Sciences*, 13(3), 1353. <https://doi.org/10.3390/app13031353>
9. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3), 546. <https://doi.org/10.3390/electronics12030546>
10. Zhou, S., Li, K., Xiao, L., Cai, J., Liang, W., & Castiglione, A. (2023). A systematic review of consensus mechanisms in blockchain. *Mathematics*, 11(10), 2248. <https://doi.org/10.3390/math11102248>