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.

# 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.) | Практ. (семін.) (год.) | ІРС (год.) | Тренінг, (год.) | Самост. робота студ. (год.) | Разом (год.) | Залік (сем.) |
|---|---|---|---|---|---|---|---|---|---|
| Денна | 3 | 6 | 32 | 14 | 3 | 6 | 95 | 150 | 6 |

30.08.2024

Тернопіль – 2024

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

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26. 08. 2024 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол № 1 від 30. 08. .2024 р.

Голова групи
забезпечення спеціальності _____ 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<br>12 Інформаційні технології | **Статус дисципліни**<br>вибіркова<br><br>**Мова навчання**<br>українська |
| Кількість залікових модулів – 3 | Спеціальність<br>125 «Кібербезпека» | Рік підготовки:<br>*Денна – 3*<br><br>Семестр:<br>*Денна – 6* |
| Кількість змістових модулів – 2 | Ступінь вищої освіти – бакалавр | Лекції (год):<br>*Денна – 32*<br><br>Практичні заняття (год):<br>*Денна – 14* |
| Загальна кількість годин – 150 | | Самостійна робота (год):<br>*Денна – 95*<br>*Тренінг (год): денна – 6*<br>Індивідуальна робота (год):<br>*Денна – 3* |
| 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 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.*** Як 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 | Контро-льні заходи |
| Змістовий модуль 1. Технології блокчейн | | | | | | |
| Тема 1. Криптографії та криптовалюти | 2 | | 7 | 1 | 3 | Поточне опитування |
| Тема 2. Децентралізація та криптовалюта біткоін | 2 | | 8 | | | |
| Тема 3. Алгоритми доказу виконаної роботи | 4 | 2 | 8 | | | |
| Тема 4. Механізм біткоінів | 4 | 2 | 8 | | | |
| Тема 5. Як зберігати та використовувати біткоіни | 4 | 2 | 8 | | | |
| Тема 6. Видобуток біткоінів | 2 | 2 | 8 | | | |
| Тема 7. Біткоіни та анонімність | 2 | | 8 | | | |
| Змістовий модуль 2. Застосування блокчейн та альтернативні криптовалюти | | | | | | |
| Тема 8. Політика та регулювання | 2 | | 8 | 2 | 3 | Поточне опитування |
| Тема 9. Альтернативні обчислювальні задачі | 2 | 2 | 8 | | | |
| Тема 10. Біткоін як платформа | 2 | 2 | 8 | | | |
| Тема 11. Альткоїни та екосистема криптовалют | 4 | 2 | 8 | | | |
| Тема 12. Децентралізовані системи: майбутнє біткоінів. | 2 | | 8 | | | |
| Разом | 32 | 14 | 95 | 3 | 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, 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. Самостійна робота**

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

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

Завдання. Студенти 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) чеш 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)ю

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.

Критерії оцінювання:

1) коректність реалізації (40%);
2) якість коду (30%);
3) презентація (30%).

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<br>2. Реалізація алгоритму Proof-of-Work<br>3. Постійна пам'ять та інтерфейс командного рядка<br>4. Транзакції<br>5. Адреси<br>6. Мережа |

| | | |
|---|---|---|
| 2 | Запуск блокчейну | Тестування та дослідження роботи блокчейну. Область 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 та децентралізовані системи**» 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 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 лабораторних робіт № 1-7. | Підсумкове модульне тестування за темами №1-12. | Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу. | Визначається як оцінка за наскрізне завдання самостійної роботи. |

**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. 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.
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