Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра програмного забезпечення комп'ютерних систем

МЕТОДИ БЛОКЧЕЙН

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 рік підготовки, 2 семестр*
Обсяг дисципліни	*Лекції: 36 год., комп'ютерний практикум: 18 год., самостійна робота: 96 год.*
Семестровий контроль/ контрольні заходи	*Залік, календарний контроль, модульна контрольна робота*
Розклад занять	*Згідно розкладу на осінній семестр поточного навчального року (http://roz.kpi.ua/)*
Мова викладання	*Українська, Англійська*
Інформація про керівника курсу / викладачів	*Лектор: асистент, Жикін Юрій Сергійович, yzhykin@protonmail.com* *Комп'ютерний практикум: асистент, Жикін Юрій Сергійович,*
Розміщення курсу	GitHub: https://github.com/rodentrabies/nobsbitcoin

2. Програма навчальної дисципліни

3. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна «Методи Блокчейн» має сформувати у здобувачів освіти компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з роботою з блокчейн-системами та систем розподіленого консенсусу.

***Метою** навчальної дисципліни «Методи Блокчейн» є ознайомлення студентів з сучасними технологіями і засобами розробки криптовалютних систем; набуття ними практичних навичок роботи з технологіями та принципами, що лежать в їх основі, таких як криптографія, комп'ютерні мережі, теорія інформації та економіка.*

***Предметом** дисципліни «Методи Блокчейн» є теоретичні та практичні основи створення та вивчення існуючого програмного коду для роботи з криптовалютними протоколами.*

*Вивчення дисципліни «Методи Блокчейн» підсилює **фахові компетенції (ФК)** та сприяє **програмним результатам навчання (ПРН)** за освітньою програмою:*
***ФК03** Здатність проєктувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів.*

ФК06 *Здатність ефективно керувати фінансовими, людськими, технічними та іншими проєктними ресурсами у сфері інженерії програмного забезпечення.*
ПРН02 *Оцінювати і вибирати ефективні методи і моделі розроблення, впровадження, супроводу програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.*
ПРН21 *Вміти модифікувати існуючі та розроблювати нові методи і алгоритми класифікації та кластеризації даних, враховуючи особливості предметної галузі.*
ПРН28 *Вміти реалізовувати інноваційні проєкти у галузі інженерії програмного забезпечення мультимедійних та інформаційно-пошукових систем від ідеї до впровадження на ринку програмного забезпечення.*

4. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішному вивченню дисципліни «Методи Блокчейн» передує вивчення нормативних дисциплін «Основи комп'ютерних систем та мереж», «Безпека програмного забезпечення», та вибіркової «Теорія інформації та кодування» навчального плану підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення.

Отримані при засвоєнні дисципліни «Методи Блокчейн» теоретичні знання та практичні уміння забезпечують успішне виконання курсових проєктів та магістерських дисертацій за спеціальністю 121 Інженерія програмного забезпечення.

5. Зміст навчальної дисципліни

Тема 1. Історичний та економічний контекст виникнення та розвитку криптовалютних технологій

Тема 2. Блокчейн-протокол Біткоїн

Тема 3. Відкриті проблеми криптовалютного протоколу Біткоїн

Тема 4. Альтернативні криптовалютні технології, їх переваги та недоліки

Модульна контрольна робота

Екзамен

6. Навчальні матеріали та ресурси

Базова література:

1. Біткоїн та криптовалютні технології. [Електронний ресурс]. Режим доступу: https://github.com/rodentrabies/nobsbitcoin.

Додаткова література:

2. Saifedean Ammous. Bitcoin Standard. The Decentralized Alternative to Central Banking. Wiley; 1st edition, 2018, 304 p.
3. Mastering Bitcoin / Andreas Antonopoulos. [Електронний ресурс]. Режим доступу: https://github.com/bitcoinbook/bitcoinbook.
4. Mastering Ethereum / Andreas Antonopoulos, Gavin Wood. [Електронний ресурс]. Режим доступу: https://github.com/ethereumbook/ethereumbook.
5. Mastering the Lightning Network / Andreas Antonopoulos, Olaoluwa Osuntokun, Rene Pickhardt. [Електронний ресурс]. Режим доступу: https://github.com/lnbook/lnbook.
6. Референтна реалізація протоколу Біткоїн. [Електронний ресурс]. Режим доступу: https://github.com/bitcoin/bitcoin.
7. Saifedean Ammous. Programming Bitcoin: Learn How to Program Bitcoin from Scratch. O'Reilly Media; 1st edition, 2019, 322 p.

7. Навчальний контент

8. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	Тип навчального заняття	Опис навчального заняття
Тема 1. Історичний та економічний контекст виникнення та розвитку криптовалютних технологій		
1	*Лекція 1. Вступ*	*Економічні та ідеологічні причини виникнення Біткоїну. Гроші. Примітивні гроші. Гроші як метал. Гроші як гарантія від держави. Стабільна валюта.* *СРС: п.6 №1*
2	*Лекція 2. Що таке Біткойн (частина 1)*	*Що таке Біткойн. Історія Біткойну. Користувачі Біткойну.* *СРС: п.6 №2*
3	*Лекція 3. Що таке Біткойн (частина 2)*	*Для чого потрібен Біткойн. Збереження купівельної спроможності. Індивідуальна автономія.* *СРС: п.6 №3*
Тема 2. Блокчейн-протокол Біткоїн		
4	*Лекція 4. Як працює Біткойн*	*Як працює Біткойн. Транзакції. Блоки. Майнінг. Блокчейн.* *СРС: п.6 №4*
5	*Комп'ютерний практикум 1*	*Знайомство та встановлення існуючої реалізації біткойн-протоколу.* *СРС: п.6 №5*
6	*Лекція 5. Біткойн клієнт*	*Біткойн клієнт. Референтна імплементація. Робота з клієнтом мережі. Альтернативні клієнти.* *СРС: п.6 №6*
7	*Лекція 6. Ключі, адреси, гаманці*	*Ключі, адреси, гаманці. Публічні та приватні ключі та криптографія. Криптографія еліптичних кривих. Біткойн адреси.* *СРС: п.6 №7*
8	*Лекція 7. Транзакції*	*Транзакції. Життєвий цикл транзакцій. Структура, входи та виходи транзакцій.*

		Скрипти та скриптова мова програмування. *СРС: п.6 №8*
9	*Комп'ютерний практикум 2*	*Робота з Біткоїн-транзакціями: створення, надсилання, відслідковування.* *СРС: п.6 №9*
10	*Лекція 8. Скрипти та скриптова мова програмування транзакцій*	*Скрипти та скриптова мова програмування транзакцій. Основні види скриптів. Конструювання скриптів (замикання та розмикання). Неповнота за Т'юрінгом.* *СРС: п.6 №10*
11	*Лекція 9. Біткойн мережа*	*Біткойн мережа. Архітектура мережі. Типи та ролі вершин мережі. Пули транзакцій.* *СРС: п.6 №11*
12	*Лекція 10. Блокчейн*	*Блокчейн. Структура блоку. Заголовок блоку. Ідентифікатори блоку: хеш заголовку блоку та висота блоку.* *СРС: п.6 №12*
13	*Лекція 11. Зв'язок блоків в блокчейн*	*Зв'язок блоків в блокчейн. Дерева Меркла.* *СРС: п.6 №13*
14	*Лекція 12. Майнінг і консенсус*	*Майнінг і консенсус. Децентралізований консенсус. Незалежна верифікація транзакцій. Агрегація транзакцій в блоки.* *СРС: п.6 №14*
15	*Лекція 13. Нагороди за блоки*	*Нагороди за блоки, комісії. Алгоритм "Proof of Work". Складність задачі "Proof of Work" та її коригування. Валідація блоку.* *СРС: п.6 №15*
16	*Комп'ютерний практикум 3*	*Створення програми для читання, парсингу та простої валідації даних ланцюга Біткоїна.* *СРС: п.6 №16*
Тема 3. Відкриті проблеми криптовалютного протоколу Біткоїн		
17	*Лекція 14. Майнінг та гонки хеш-потужностей*	*Майнінг та гонки хеш-потужностей. Атаки на консенсус. Безпека біткойну.*

		Принципи безпеки. Рекомендації до безпеки. *СРС: п.6 №17*
18	*Лекція 15. Потенціальні покращення та нові розробки*	*Потенціальні покращення та нові розробки. Потенціальні проблеми та вектори атак. Мережа Lightning. Платіжні канали.* *СРС: п.6 №18*
19	*Комп'ютерний практикум 4*	*Створення програми для взаємодії з одноранговою мережею Біткоїна. Gossip-протокол.* *СРС: п.6 №19*
Тема 4. Альтернативні криптовалюти, їх переваги та недоліки		
20	*Лекція 16. Альтернативні блокчейни та їх застосування (частина 1)*	*Альтернативні блокчейни та їх застосування. Ethereum.* *СРС: п.6 №20*
21	*Лекція 17. Альтернативні блокчейни та їх застосування (частина 2)*	*Альтернативні блокчейни та їх застосування. Monero.* *СРС: п.6 №21*
22	*Комп'ютерний практикум 5*	*Створення програми для роботи з Біткоїн-скриптом, статичний аналіз скриптів.* *СРС: п.6 №22*
Модульна контрольна робота		

9. Самостійна робота студента/аспіранта

Дисципліна «Методи Блокчейн» ґрунтується на самостійній підготовці до занять. Лекційний матеріал охоплює загальну архітектуру протоколів Блокчейн, але для виконання комп'ютерних практикумів необхідно розглянути деталі протоколу, що зводиться до вивчення існуючої літератури та коду референтної реалізації.

№ з/п	*Назва теми, що виноситься на самостійне опрацювання*	*Кількість годин*	*Література*
1	*Підготовка до лекції 1*	*1*	*1;2*
2	*Підготовка до лекції 2*	*1*	*1;2*
3	*Підготовка до лекції 3*	*1*	*1;2*
4	*Підготовка до лекції 4*	*1*	*1;2*
5	*Підготовка до комп'ютерного практикуму 1*	*7*	*1;3;6;7*

6	*Підготовка до лекції 5*	*1*	*1;3;6;7*
7	*Підготовка до лекції 6*	*1*	*1;3;6;7*
8	*Підготовка до лекції 7*	*1*	*1;3;6;7*
9	*Підготовка до комп'ютерного практикуму 2*	*7*	*1;3;6;7*
10	*Підготовка до лекції 8*	*1*	*1;3;6;7*
11	*Підготовка до лекції 9*	*1*	*1;3;6*
12	*Підготовка до лекції 10*	*1*	*1;3;6*
13	*Підготовка до лекції 11*	*1*	*1;3;7*
14	*Підготовка до лекції 12*	*1*	*1;3;7*
15	*Підготовка до лекції 13*	*1*	*1;3;7*
16	*Підготовка до комп'ютерного практикуму 3*	*7*	*1;3;5;6;7*
17	*Підготовка до лекції 14*	*1*	*1;5;6;7*
18	*Підготовка до лекції 15*	*1*	*1;5;6;7*
19	*Підготовка до комп'ютерного практикуму 4*	*7*	*1;3;5;6;7*
20	*Підготовка до лекції 16*	*1*	*1;4*
21	*Підготовка до лекції 17*	*1*	*1;4*
22	*Підготовка до комп'ютерного практикуму 5*	*7*	*1;3;5;6;7*
23	*Підготовка до модульної контрольної роботи*	*14*	*1-7*
24	*Підготовка до екзамену*	*30*	*1-7*

10. Політика та контроль

11. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних занять є обов'язковим.

Відвідування занять комп'ютерного практикуму може бути епізодичним та за потреби консультації/захисту робіт комп'ютерного практикуму.

Правила поведінки на заняттях: активність, повага до присутніх, відключення телефонів.

Дотримання політики академічної доброчесності.

Правила захисту робіт комп'ютерного практикуму: роботи повинні бути зроблені відповідно до поставлених задач та згідно з варіантом.

12. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Протягом семестру студенти виконують 5 комп'ютерних практикумів. Максимальна кількість балів за кожний комп'ютерний практикум: 6 балів.

Бали нараховуються за:
- якість виконання комп'ютерного практикуму: 0-3 бали;
- відповідь під час захисту комп'ютерного практикуму: 0-2 бали;

- своєчасне представлення роботи до захисту: 0-1 бал.

Критерії оцінювання якості виконання:
3 бали – робота виконана якісно, в повному обсязі;
2 бали – робота виконана якісно, в повному обсязі, але має недоліки;
0-1 бал – робота виконана не в повному обсязі.

Критерії оцінювання відповіді:
2 бали – відповідь повна, добре аргументована;
1 бал – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Критерії оцінювання своєчасності представлення роботи до захисту:
1 бали – робота представлена до захисту не пізніше вказаного терміну;
0 балів – робота представлена до захисту пізніше вказаного терміну.

Максимальна кількість балів за виконання та захист комп'ютерних практикумів:
6 балів × 5 комп. практ. = 30 балів.

*Завдання на **модульну контрольну роботу** складається з 2 теоретичних питань. Відповідь на кожне теоретичне запитання оцінюється 10 балами.*

Критерії оцінювання теоретичного запитання модульної контрольної роботи:
9-10 балів – відповідь вірна, повна, добре аргументована;
7-8 балів – відповідь вірна, але погано аргументована;
5-6 балів – відповідь вірна, але неповна та погано аргументована;
3-4 бали – у відповіді є незначні помилки;
1-2 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Максимальна кількість балів за кожну модульну контрольну роботу:
10 балів × 2 теоретичні запитання = 20 балів.

Семестрова складова рейтингової шкали Rc = 50 балів, вона визначається як сума балів, отриманих за виконання та захист комп'ютерних практикумів і результатів модульного контролю. Екзаменаційна складова рейтингової шкали RE = 50 балів.

*Завдання **на екзамен** складається з 5 теоретичних. Відповідь на кожне теоретичне запитання оцінюється 10 балами.*
Критерії оцінювання теоретичного питання екзаменаційної роботи:
9-10 балів – відповідь вірна, повна, добре аргументована;
7-8 балів – відповідь вірна, але погано аргументована ;
5-6 балів – відповідь вірна, але неповна та погано аргументована;
3-4 бали – у відповіді є незначні помилки;
1-2 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Максимальна кількість балів за екзаменаційну роботу:
10 балів × 5 теоретичних запитання = 50 балів.

Рейтингова шкала з дисципліни за семестр дорівнює:

R_C *= 30 балів + 20 балів = 50 балів.*
$R = R_C + R_E = R_{комп.практ} + R_{МКР} + R_{екз.} = 30+20+50$ *балів = 100 балів*

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
На першій атестації (8-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 3 бали (50% від максимальної кількості балів, яку може отримати студент, захистивши 1 комп'ютерний практикум).
На другій атестації (14-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 9 балів (50 % від максимальної кількості балів, яку може отримати студент, захистивши 3 комп'ютерних практикуми).

*Семестровий контроль: **екзамен**.*
Умови допуску до семестрового контролю:
При семестровому рейтингу (R_C) не менше 60% (30 балів) та зарахуванні усіх робіт комп'ютерного практикуму.

Необхідною умовою допуску до екзамену є виконання і захист комп'ютерного практикуму.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено аспірантом, асистентом, Жикіним Ю.С.

Ухвалено кафедрою ПЗКС (протокол №8 від 25.01.2023)

Погоджено Методичною комісією факультету прикладної математики (протокол №6 від 27.01.2023)