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

Кафедра програмного забезпечення комп'ютерних систем

ТЕХНОЛОГІЯ BLOCK CHAIN

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
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	*4 рік підготовки, 2 семестр*
Обсяг дисципліни	*Лекції: 36 год., комп'ютерний практикум: 18 год., самостійна робота: 66 год.*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота, календарний контроль*
Розклад занять	*Згідно розкладу на осінній семестр поточного навчального року (http://roz.kpi.ua/)*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: аспірант, асистент, *Жикін Юрій Сергійович, yzhykin@protonmail.com* Комп'ютерний практикум: аспірант, асистент, *Жикін Юрій Сергійович, yzhykin@protonmail.com*
Розміщення курсу	GitHub: https://github.com/rodentrabies/nobsbitcoin

Програма навчальної дисципліни

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

Навчальна дисципліна «Технологія Block Chain» 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 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.*

***Предмет** дисципліни – теоретичні та практичні основи створення та вивчення існуючого програмного коду для роботи з криптовалютними протоколами.*

*Вивчення дисципліни «Технологія Block Chain» сприяє формуванню у здобувачів освіти **фахових компетентностей (ФК)**, необхідних для розв'язання практичних задач професійної діяльності, пов'язаної з розробленням, вдосконаленням та експлуатацією інформаційно-пошукових систем:*
***ФК06** Здатність аналізувати, вибирати і застосовувати методи.*

ФК07 *Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.*
ФК08 *Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.*
ФК14 *Здатність до алгоритмічного та логічного мислення.*

Вивчення дисципліни «Технологія Block Chain» сприяє формуванню у студентів наступних ***програмних результатів навчання*** *(ПРН) за освітньою програмою:*
ПРН01 *Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.*
ПРН05 *Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об'єктно-орієнтованого аналізу та математичного моделювання для розроблення програмного забезпечення.*
ПРН13 *Знати і застосовувати методи розроблення алгоритмів, конструювання програмного забезпечення та структур даних і знань.*
ПРН15 *Мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення.*
ПРН19 *Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.*

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

Дисципліні «Технологія Block Chain» передують дисципліни нормативні дисципліни навчального плану підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення.

Отримані при засвоєнні дисципліни «Технологія Block Chain» теоретичні знання знадобляться здобувачам освіти при розробленні бакалаврських дипломних робіт, магістерських дисертацій за спеціальністю 121 Інженерія програмного забезпечення.

3. 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

Залік

4. 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.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	Тип навчального заняття	Опис навчального заняття
Тема 1. Історичний та економічний контекст виникнення та розвитку криптовалютних тенологій		
1	*Лекція 1*	*Вступ. Економічні та ідеологічні причини виникнення Біткоїна. Гроші. Примітивні гроші. Гроші як метал. Гроші як гарантія від держави. Стабільна валюта.*
2	*Лекція 2*	*Що таке Біткойн. Історія Біткойну. Користувачі Біткоїна.*
3	*Лекція 3*	*Для чого потрібен Біткойн. Збереження купівельної спроможності. Індивідуальна автономія.*
Тема 2. Блокчейн-протокол Біткоїн		
4	*Лекція 4*	*Як працює Біткоїн. Транзакції. Блоки. Майнінг. Блокчейн.*
5	*Комп'ютерний практикум 1*	*Знайомство та встановлення існуючої реалізації біткойн-протоколу 1.*
6	*Комп'ютерний практикум 2*	*Знайомство та встановлення існуючої реалізації біткойн-протоколу 2.*
7	*Лабораторна робота 1*	*Виконання завдання за варіантом*
8	*Лекція 5*	*Біткойн клієнт. Референтна імплементація. Робота з клієнтом мережі. Альтернативні клієнти.*
9	*Лекція 6*	*Ключі, адреси, гаманці. Публічні та приватні ключі та криптографія. Криптографія еліптичних кривих. Біткойн адреси.*
10	*Комп'ютерний практикум 3*	*Налаштування Біткоїн-гаманця на операційних системах Linux, Android та iOS.*
11	*Лекція 7*	*Транзакції. Життєвий цикл транзакцій. Структура, входи та виходи транзакцій. Скрипти та скриптова мова програмування.*

12	*Лекція 8*	*Скрипти та скриптова мова програмування транзакцій.*
13	*Комп'ютерний практикум 4*	*Створення програми для роботи з Біткоїн-скриптом, статичний аналіз скриптів.*
14	*Лекція 9*	*Біткойн мережа. Архітектура мережі. Типи та ролі вершин мережі. Пули транзакцій.*
15	*Лекція 10*	*Блокчейн. Структура блоку. Заголовок блоку. Ідентифікатори блоку: хеш заголовку блоку та висота блоку.*
16	*Комп'ютерний практикум 5*	*Створення програми для синхронізації та зберігання бази даних заголовків блоків.*
17	*Лабораторна робота 2*	*Виконання завдання за варіантом*
18	*Лекція 11*	*Зв'язок блоків в блокчейн. Дерева Меркла.*
19	*Лекція 12*	*Майнінг і консенсус. Децентралізований консенсус. Незалежна верифікація транзакцій. Агрегація транзакцій в блоки.*
20	*Комп'ютерний практикум 6*	*Створення програми для читання, парсингу та простої валідації даних ланцюга Біткоїна.*
21	*Лабораторна робота 3*	*Виконання завдання за варіантом*
22	*Лекція 13*	*Нагороди за блоки, комісії. Алгоритм "Proof of Work". Складність задачі "Proof of Work" та її коригування. Валідація блоку.*
Тема 3. Відкриті проблеми криптовалютного протоколу Біткоїн		
23	*Лекція 14*	*Майнінг та гонки хеш-потужностей. Атаки на консенсус. Безпека біткойну. Принципи безпеки. Рекомендації до безпеки.*
24	*Комп'ютерний практикум 7*	*Створення програми для взаємодії з одноранговою мережею Біткоїна. Gossip-протокол.*
25	*Лекція 15*	*Потенціальні покращення та нові розробки. Потенціальні проблеми та вектори атак. Мережа Lightning. Платіжні канали.*
Тема 4. Альтернативні криптовалюти, їх переваги та недоліки		
26	*Лекція 16*	*Альтернативні блокчейни та їх застосування.*
27	*Комп'ютерний практикум 8*	*Робота з програмним забезпечення для взаємодії з протоколами-надбудовами над Біткоїн-протоколом.*
28	*Лекція 17*	*Ethereum.*
29	*Лекція 18*	*Monero.*

30	*Комп'ютерний практикум 9*	*Робота з програмним забезпеченням Ethereum і Monero.*

6. Самостійна робота студента/аспіранта

Дисципліна «Технологія Block Chain» 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 (5).

№ 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*	*3*	*1;3;6;7*
6	*Підготовка до комп'ютерного практикуму 2*	*3*	*1;3;6;7*
7	*Виконання лабораторної роботи 1*	*7*	*1;3;6;7*
8	*Підготовка до лекції 5*	*1*	*1;3;6;7*
9	*Підготовка до лекції 6*	*1*	*1;3;6;7*
10	*Підготовка до комп'ютерного практикуму 3*	*3*	*1;3;6;7*
11	*Підготовка до лекції 7*	*1*	*1;3;6;7*
12	*Підготовка до лекції 8*	*1*	*1;3;6;7*
13	*Підготовка до комп'ютерного практикуму 4*	*3*	*1;3;6;7*
14	*Підготовка до лекції 9*	*1*	*1;3;6*
15	*Підготовка до лекції 10*	*1*	*1;3;6*
16	*Підготовка до комп'ютерного практикуму 5*	*3*	*1;3;6;7*
17	*Виконання лабораторної роботи 2*	*7*	*1;3;6;7*
18	*Підготовка до лекції 11*	*1*	*1;3;7*
19	*Підготовка до лекції 12*	*1*	*1;3;7*
20	*Підготовка до комп'ютерного практикуму 6*	*3*	*1;3;6;7*
21	*Виконання лабораторної роботи 3*	*7*	*1;3;6;7*
22	*Підготовка до лекції 13*	*1*	*1;3;7*
23	*Підготовка до лекції 14*	*1*	*1;5;6;7*
24	*Підготовка до комп'ютерного практикуму 7*	*3*	*1;3;6;7*
25	*Підготовка до лекції 15*	*1*	*1;5;6;7*
26	*Підготовка до лекції 16*	*1*	*1;4*
27	*Підготовка до комп'ютерного практикуму 8*	*3*	*1;3;6;7*
28	*Підготовка до лекції 17*	*1*	*1;4*

29	*Підготовка до лекції 18*	*1*	*1;4*
30	*Підготовка до комп'ютерного практикуму 9*	*3*	*1;3;5;6;7*

Політика та контроль

7. 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.

Правила призначення заохочувальних та штрафних балів є наступними. Заохочувальні бали нараховуються за:
- точні та повні відповіді в опитуваннях за матеріалами лекцій (максимальна кількість балів за опитування - 3 бали).

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

Протягом семестру студенти виконують 3 лабораторних роботи. Максимальна кількість балів за кожний комп'ютерний практикум: 20 балів.

Бали нараховуються за:
- якість виконання комп'ютерного практикуму: 0-5 бали;
- відповідь під час захисту комп'ютерного практикуму: 0-3 бали;
- своєчасне представлення роботи до захисту: 0-2 бали.

Критерії оцінювання якості виконання:
10 балів – робота виконана якісно, в повному обсязі;
8 балів – робота виконана якісно, в повному обсязі, але має недоліки;
6 бали – робота виконана в повному обсязі, але містить незначні помилки;
4 бали – робота виконана в повному обсязі, але містить суттєві помилки;
2 балів – робота виконана не в повному обсязі.

Критерії оцінювання відповіді:
6 бали – відповідь повна, добре аргументована;
4 бали –відповідь вірна, але має недоліки або незначні помилки;
2 бал – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

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

Модульна контрольна робота складається з 4 теоретичних питань. Кожне питання оцінюється 10 балами.

Критерії оцінювання кожного теоретичного запитання модульної контрольної роботи:
10 балів – відповідь вірна, повна, добре аргументована;
8-9 балів – відповідь вірна, розгорнута, але не дуже добре аргументована;
6-7 балів – в цілому відповідь вірна, але має недоліки;
4-5 балів – у відповіді є незначні помилки;
1-3 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Максимальна кількість балів за виконання та захист комп'ютерних практикумів:
20 балів × 3 комп. практ. + 40 балів × 1 мкр = 100 балів.

*Протягом семестру на практичних заняття під час захисту комп'ютерних практикумів відбуваються **опитування за темою поточного заняття**. Бали за відповіді на запитання входять у бали за захист комп'ютерних практикумів. Кількість **запитань за темою поточного заняття** для одного студента є необмеженою.*

Рейтингова шкала з дисципліни дорівнює:
$R = R_C = 100$ балів.

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
На першій атестації (4-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 10 балів (50% від максимальної кількості балів, яку може отримати студент, захистивши 1 лабораторну роботу).
На другій атестації (7-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 30 балів (50 % від максимальної кількості балів, яку може отримати студент, захистивши 3 комп'ютерних практикуми).

Семестровий контроль: залік
Умови допуску до семестрового контролю:
При семестровому рейтингу (R_C) не менше 60 балів та зарахуванні усіх робіт комп'ютерного практикуму, студент отримує залік «автоматом» відповідно до таблиці (Таблиця відповідності рейтингових балів оцінкам за університетською шкалою).

Якщо студент не погоджується з оцінкою «автоматом», то може спробувати підвищити свою оцінку шляхом відповіді на 3-5 запитань за темами, що роглядаються у даному курсі.

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)