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

Кафедра математичних методів
захисту інформації

Вступ до технології блокчейн та криптовалют

Робоча програма навчальної дисципліни (Силабус)

Реквізити освітньої компоненти

Рівень вищої освіти	***перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 «Прикладна математика»*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна*
Рік підготовки, семестр	*4- курс, 2 семестр*
Обсяг дисципліни	*120 годин / 4 кредити ECTS* *Лекції: 36 годин.* *Лабораторні: 18 годин.* *СРС: 66 годин.*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота*
Розклад занять	*Rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *д.т.н., с.н.с. Кудін Антон Михайлович, pplayshner@gmail.com,* *д.т.н., проф. Ковальчук Людмила Василівна* Лабораторні: *Фесенко Андрій В'ячеславович*
Розміщення курсу	Посилання на дистанційний ресурс https://ela.kpi.ua/handle/123456789/52476

Програма навчальної дисципліни

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

Сучасний кіберпростір - це система, в якій самостійно виникають сигнали, які ведуть до керування процесами збереження певного стану системи, самоорганізуюча, децентралізована та розподілена інформаційна система. Структури даних та процеси, які використовуються в системі повинні бути адекватні принципам функціонування системи, саме тому блокчейн-технології притаманні сучасному кіберпростору. Основу блокчейн-технологій складають криптографічні протоколи, вивчення яких і є предметом навчальної дисципліни.

Метою вивчення дисципліни є оволодіння студентами сучасними методами, навичками, вміннями та способами аналізу стійкості криптографічних протоколів блокчейнів, безпечної реалізації блокчейн технологій.

Після засвоєння освітнього компоненту студенти мають продемонструвати такі результати навчання:

1) Знання:

- визначення і властивостей блокчейну та його складових;
- основних криптографічних механізмах та протоколах, які використовуються в блокчейнах;
- основ аналізу стійкості та ефективності за обраними критеріями протоколів узгоджень;
- основ проектування та розробки блокчейн технологій.

2) Уміння:

- проведення криптографічного аналізу основних характеристик протоколів узгодження блокчейну;
- розгортання програмної платформи та окремих інструментів розробки блокчейнів;
- розробки системи смарт-контрактів:
- проведення оцінки стійкості до криптоаналізу криптографічних систем, реалізованих за технологією децентралізованих додатків.

3) Досвід: навички прикладного криптоаналізу та створення криптографічних систем.

Після засвоєння навчальної дисципліни «Спеціальні розділи криптології» студенти мають продемонструвати такі програмні компетентності та результати навчання за освітньою програмою:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями;
ЗК 3 – Здатність генерувати нові ідеї (креативність);
ЗК 4 – Здатність бути критичним і самокритичним;
ЗК 6 – Здатність до абстрактного мислення, аналізу та синтезу;
ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел;
ЗК 8 – Знання та розуміння предметної області та розуміння професійної діяльності;

Фахові компетентності

ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі;
ФК 14 – Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв’язання, що забезпечує потрібні точність і надійність результату;

Програмні результати навчання

РН 1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці;
РН 2 – Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами;
РН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв’язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів;

РН 7 – Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач;
РН 14 – Виявляти здатність до самонавчання та продовження професійного розвитку;
РН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

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

Дисципліна «Спеціальні розділи криптології» використовує знання та вміння, набуті у ході вивчення курсів «Дискретна математика», «Програмування», «Теорія складності», «Симетрична кріптографія», «Асиметричні криптосистеми та протоколи», «Математичне моделювання», «Теорія інформації та кодування» та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням сучасних криптосистем.

3. Зміст навчальної дисципліни

Розділ 1. Основні поняття технології блокчейн.

Тема 1.1 Загальні поняття про технологіїю блокчейну. Блокчейни криптовалют.

Розділ 2. Протоколи консенсусу (узгодження) блокчейнів.

Тема 2.1. Протоколи узгодження блокчейну. Стислий аналіз основних ідей.

Тема 2.2 Технологічні основи блокчейну. Розподілені алгоритми.

Тема 2.3 Протоколи консенсусу. Сучасні «візантійські» протоколи. . Протоколи гібридного типу, засновані на протоколах Proof-of-Stack. Протокол Casper.

Тема 2.4 Протоколи консенсусу. Інші протоколи консенсусу.

Розділ 3. Програмна модель блокчейну. Аспекти реалізації технології блокчейну.

Тема 3.1. Реалізація блокчейн технології. Програмна модель блокчейн. Аспекти реалізації смарт-контрактів та розподілених додатків в блокчейні.

Тема 3.2. Реалізація блокчейн технологій смарт-контрактів. Особливості налаштування блокчейну Ethereum під ОС Ubuntu. Безпека розподілених прикладних програм

Розділ 4. Спеціальні питання технології блокчейн.

Тема 4.1 Масштабирование блокчейнов.

Тема 4.2. Блокчейн та NFT

Розділ 5. Математичні моделі функціонування блокчейнів та криптовалют

Тема 5.1 Означення та основні характеристики блокчейну.

Тема 5.2 Створення примітивних криптовалют та аналіз їх вразливостей.

Тема 5.3 Протокол консенсусу Proof-of-Work.

Тема 5.4 Аналіз роботи Накамото та виправлення помилок.

Тема 5.5 Протокол консенсусу Proof-of-Stake як альтернатива протоколу Proof-of-Work.

Тема 5.6 Імовірність дабл спенд атаки для протоколу Proof-of-Work. Критичний вплив часу синхронізації.

Тема 5.7 Анонімність у блокчейні. Інші найсучасніші криптографічні протоколи, що використовуються у блокчейні.

Тема 5.8 Протоколи доведення без розголошення – один з «наймодніших» напрямків у блокчейні.

Тема 5.9 SNARKи (succinct non-interactive argument for knowlage) як один з найбільш вживаних протоколів доведення без розголошення.

4. Навчальні матеріали та ресурси

Базова література:

1. Положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського. – 2020. [Електронний ресурс] – Режим доступу: http://osvita.kpi.ua/node/39
2. Вступ до технології блокчейн та криптовалют. Частина 1. Теоретичні засади функціонування блокчейн-технологій [Електронний ресурс]: навчальний посібник к для здобувачів ступеня бакалавра за освітньою програмою «Математичні методи криптографічного захисту інформації»» спеціальності 113 «Прикладна математика» / Л. В. Ковальчук, А. М. Кудін, Н. В. Кучинська ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3.49 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 142 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/52476
3. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
4. Narayanan, Arvind, and Bonneau, Joseph, et al. Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction. Princeton University Press, 2016.
5. Koblitz N. A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – P.312.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1.	Тема 1.1 Загальні поняття про технологіїю блокчейну. Блокчейни криптовалют. Основні питання: 1. Основні ідеї блокчейн 2. Приклади для вивчення: криптовалюти та реєстри 3. Блокчейн як основа криптовалюти 4. Приклад для вивчення: блокчейн Bitcoin 5. Відмінності криптовалют від фіатних валют.
2.	Тема 2.1. Протоколи узгодження блокчейну. Стислий аналіз основних ідей. Основні питання:

	1. Протоколи узгодження – загальні поняття. 2. Протоколи узгодження типу Proof-of-Work. 3. Розвиток протоколів узгодження. Вади протоколів узгодження, заснованих на складності обчислень. 4. Протоколи узгодження типу Proof-of-Stack. 5. Вади протоколів узгодження, заснованих на накопиченні цінних ресурсів
3.	Тема 2.2 Технологічні основи блокчейну. Розподілені алгоритми. Основні питання: 1. Загальні поняття розподілених алгоритмів. 2. Задача двох генералів, генералів та лейтенантів, візантійських генералів. 3. Класичні задачі проектування інформаційних систем, засновані на «візантійських» протоколах 4. Розподілені алгоритми узгодження. 5. «Візантійські» протоколи узгодження. 6. Обчислювальна складність розподілених алгоритмів
4.	Тема 2.3 Протоколи консенсусу. Сучасні «візантійські» протоколи. . Протоколи гібридного типу, засновані на протоколах Proof-of-Stack. Протокол Casper. Основні питання: 1. Типи сучасних «візантійських» протоколів 2. Протокол Paxos 3. Протокол PBFT та RAFT 4. Порівняльна ефективність за складністю ймовірнісних та детермінованих версій «візантійських» протоколів. 5. Гібридизація протоколів узгодження. 6. Основні ідеї протоколу Casper. 7. Аналіз практичних ситуацій, які призвели до розробки Casper-подібних протоколів. Протокол Casper FFG – основні ідеї. Основні властивості та умови безпечної роботи Casper FFG. Етапи переходу Etherium на нові протоколи узгодження.
5	Тема 2.4 Протоколи консенсусу. Інші протоколи консенсусу. Основні питання: 1. Протоколи типу Delegated Proof of Stack. 2. Протоколи типу Proof-of-Activity. 3. Протоколи типу Proof-of-Burn. 4. Протоколи типу Proof-of-Capacity. 5. Протоколи консенсусу типу Proof-of-Reputation. 6. Узагальнення поняття цінного ресурсу в протоколах консенсусу. 7. Протоколи типу Proof-of-Accuracy. Поняття Чебишовського радіусу інформації в теорії складності алгоритмів.
6.	Тема 3.1. Реалізація блокчейн технології. Програмна модель блокчейн. Аспекти реалізації смарт-контрактів та розподілених додатків в блокчейні. Основні питання: 1. Особливості блокчейнів, які впливають на формування програмної моделі 2. Програмна модель блокчейну 3. Основні проблемні задачі реалізації блокчейну. 4. Засоби розробки програмного забезпечення розподілених інформаційних систем.мАспекти реалізації смарт-контрактів та розподілених додатків в блокчейні. Solidity. Деякі особливості реалізації платформи Etherium.мПоняття про смарт-контракти. 5. Особливості мови Solidity. Нащадок JavaScript. Нащадок C++. Solidity – власні риси. 6. Можливості універсальних мов програмування щодо розробки смарт-контрактів. 7. Платформи розробки під мову Solidity

7.	Тема 3.2. Реалізація блокчейн технологій смарт-контрактів. Особливості налаштування блокчейну Ethereum під ОС Ubuntu. Безпека розподілених прикладних програм. Основні питання: 1. Алгоритм розробки першого смарт-контракту для платформи Ethereum. Алгоритми запусків смарт-контрактів для платформи Ethereum. Налаштування блокчейну Etherium під ріні програмно-апаратні платформи. 2. Загальні поняття про безпеку децентралізованих додатків на блокчейн-платформах (Dapps security). Вимоги до безпеки реалізації децентралізованих додатків. 3. Порівняльний аналіз вимог OWASP безпеки Web-додатків та вимог безпеки децентралізованих додатків.
8.	Тема 4.1 Масштабирование блокчейнов. Основні питання: 1. CAP-гіпотеза для блокчейнів. CAP-гіпотеза для баз даних. 2. Методи масштабування блокчейнів.
9.	Тема 4.2. Блокчейн та NFT. Основні питання: 1. Поняття про NFT 2. Застосування NFT в блокчейнах 3. Криптовалюти та NFT 4. NFT та криптобіржи.
10.	Тема 5.1 Означення та основні характеристики блокчейну. Основні питання: 1. Основні криптографічні механізми, які використовуються в блокчейні. 2. Додаткові властивості криптографічної геш-функції. 3. Децентралізація проти централізації.
11	Тема 5.2 Створення примітивних криптовалют та аналіз їх вразливостей. Основні питання: 1. Створення примітивних криптовалют. 2. Найпростіші атаки. Необхідність довіреної сторони. А як же децентралізація?
12	Тема 5.3 Протокол консенсусу Proof-of-Work. Основні питання: 1. Основна ідея протоколу консенсусу. 2. Захист від найпростіших атак (дабл спенд атака, сибіл атака, цензоршіп атака).
13	Тема 5.4 Аналіз роботи Накамото та виправлення помилок. 1. Основні ідеї роботи Накамото. Прообраз протоколу Proof-of-Work як захисту від Ddos-атак. 2. Суттєві імовірнісні помилки у доведенні сформульованих тверджень. 3. Недоліки протоколу Proof-of-Work.
14	Тема 5.5 Протокол консенсусу Proof-of-Stake як альтернатива протоколу Proof-of-Work. Основні питання: 1. Основні ідеї та деталі протоколу Proof-of-Stake. 2. Переваги протоколу Proof-of-Stake у порівнянні з протоколом Proof-of-Work. 3. Основні атаки, захист від цих атак та отримання конкретних оцінок імовірності до дабл спенд атаки. 4. Блоки підтвердження як захист від дабл спенд атаки.
15	Тема 5.6 Імовірність дабл спенд атаки для протоколу Proof-of-Work. Критичний вплив часу синхронізації.

	Основні питання: 1. Математичне обґрунтування імовірності атаки у моделі з неперервним часом та миттєвою синхронізацією (робота Грунспана). 2. Модель з ненульовим часом синхронізації. Приклади чисельних результатів.
16	Тема 5.7 Анонімність у блокчейні. Інші найсучасніші криптографічні протоколи, що використовуються у блокчейні. Основні питання: 1. Що саме є анонімним у блокчейні? 2. Використання міксерів (Bitcoin та Dash). 3. Використання кільцевих підписів для забезпечення анонімності (Monero).
17	Тема 5.8 Протоколи доведення без розголошення – один з «наймодніших» напрямків у блокчейні. Основні питання: 1. Сутність доведення без розголошення. Основні необхідні характеристики на прикладі «Печери Алі-Баби». 2. Математика у протоколах доведення без розголошень. 3. Основні приклади протоколів доведення без розголошення. 4. Еврістика Фіата-Шаміра. Цифровий підпис як не інтерактивний протокол доведення без розголошення.
18	Тема 5.9 SNARKи (succinct non-interactive argument for knowlage) як один з найбільш вживаних протоколів доведення без розголошення. Основні питання: 1. Математика: відображення спарювання на еліптичних кривих. 2. SNARK-протоколи на прикладі протоколу GRO-16. Використання у криптовалюті zcash.

Лабораторні заняття

№ з/п	Назва теми заняття та перелік основних питань
1.	Вивчення блокчейн-платформи з відкритим кодм NaiveCoin. Отримати навики роботи із блокчейн-платформою на прикладі системи із відкритоим кодом naivecoin. Основні питання: 1.Розгорнути віртуальну однорангову (Peer-to-peer) мережу на базі системи віртуалізації VirtualBox або еквіваленті. 2. Розгорнути систему naivecoin. 3. Провести транзакції в системі naivecoin. 4. Провести аналіз ефективності блокчейну naivecoin.

6. Самостійна робота студента

Самостійна робота студента складається з:

- *підготовки до МКР шляхом опанування лекційного матеріалу та виконання заданих на лекціях завдань, віднесених на кожній лекції для самостійного опанування студентів;*
- *підготовки до захисту лабораторної роботи.*

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонуються завдання для самостійного опанування. Для виконання

цих завдань слід скористатися рекомендованою літературою та конспектом лекцій. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед лабораторними заняттями вивчити або повторити відповідний теоретичний матеріал Для перевірки засвоєння теоретичного матеріалу відповідні питання включені до модульної контрольної роботи; підготовка до МКР вимагає ретельного повторення теоретичного матеріалу лекцій у години самостійної роботи.

Самостійна робота студента

№ з/п	**Вид самостійної роботи**	**Кількість годин СРС**
1.	Підготовка до лабораторних робіт	33
2.	Підготовка до МКР	33
	Загалом	**66**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, що розвивають практичні уміння та навички.

Правила захисту лабораторних робіт, індивідуальних завдань

Виконання лабораторної роботи є обов'язковим. Лабораторна може виконуватись на будь-яких програмно-апаратних платформах та платформах віртуалізації.

Пропущені контрольні заходи

Результат модульної контрольної роботи для студента, який не з'явився на контрольний захід, є нульовим. Повторне написання модульної контрольної роботи допускається за попередньою домовленістю з викладачем.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Норми етичної поведінки

Норми етичної поведінки студентів і викладачів визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

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

Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:

№	Контрольний захід	Бал	Кількість	Всього
1	Модульна контрольна робота	50	1	50
2	Лабораторна робота	50	1	50
	Всього			100

Здобувачі, що мають рейтинг ≥60 балів отримують залік без додаткових випробувань.
Зі здобувачами, які мають рейтингову оцінку менше 60 балів, а також з тими, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить семестровий контроль у вигляді додаткової контрольної роботи або співбесіди.

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):

Склав: проф. каф. ММЗІ д.т.н., с.н.с. Кудін Антон Михайлович, проф. каф. ММЗІ д.т.н., проф. Ковальчук Л.В.

Ухвалено кафедрою математичних методів захисту інформації (протокол № 2/2022 від 16.02.2022)

Погоджено Методичною комісією НН ФТІ факультету (протокол № 6 від 30.06.2022)