



Технологія блокчейн та розподілені системи

Робоча програма навчальної дисципліни (Силабус)

• Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>11 Математика і статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>очна(денна)</i>
Рік підготовки, семестр	<i>I курс, весняний семестр</i>
Обсяг дисципліни	<i>5 кредити / 150 годин Лекційних занять: 36 год. Лабораторні роботи: 18 год. Самостійна робота студентів: 96 год.</i>
Семестровий контроль/ контрольні заходи	<i>Іспит, модульна контрольна робота</i>
Розклад занять	<i>Rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: д.т.н., Кудін Антон Михайлович, pplayshner@gmail.com Лабораторні: Селюх Поліна Валентинівна,</i>
Розміщення курсу	<i>Посилання на дистанційний ресурс pplayshner@gmail.com</i>

• Програма навчальної дисципліни

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

Постановки задач забезпечення безпеки сучасного кіберпростору суттєво відрізняються від традиційних задач забезпечення безпеки інформації. Одна з основних відмінностей сучасного кіберпростору – можливість самоуправління, в тому числі – за рахунок децентралізованих керуючих систем. Відомо, що структури даних та процеси, які використовуються в системах відповідають їх принципам функціонування, саме тому блокчейн-технології широко використовуються в сучасному кіберпросторі. Зберігання та обробка даних за допомогою блокчейн технології є одним з різновидів розподіленої обробки даних, основним механізмом захисту яких є криптографічні механізми захисту. Отже предметом вивчення дисципліни є криптографічні технології захисту блокчейнів та децентралізованих додатків.

Метою вивчення дисципліни є оволодіння студентами сучасними методами, навичками, вміннями та способами побудови систем криптографічного захисту інформації для блокчейн-систем та систем децентралізованих додатків.

--	--	--

--	--	--

Після засвоєння освітнього компоненту студенти мають продемонструвати такі результати навчання:

1) Знання:

- особливості блокчейну як об'єкту захисту інформації;*
- основних криптографічних механізмів та протоколах, які використовуються в блокчейнах;*
- аналізу стійкості та ефективності за обраними критеріями протоколів узгоджень;*
- проектування та розробки системи криптографічного захисту 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:

Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.

Здатність генерувати нові ідеї та нестандартні підходи до їх реалізації, адаптуватись та діяти в нових ситуаціях, виявляти ініціативу, інноваційність та підприємливість.

Фахові компетентності:

Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог.

Здатність проводити наукові дослідження з розроблення нових та адаптацією існуючих математичних та комп'ютерних моделей для дослідження різноманітних процесів, явищ і систем, проводити відповідні чисельні експерименти з аналізом одержаних результатів.

Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем

Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази

--	--	--

--	--	--

Програмні результати¹ навчання:

Використовувати та адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач.

Здійснювати математичне і комп'ютерне моделювання складних систем та процесів, обчислювальні експерименти з використанням сучасних методів інтелектуального аналізу даних та комп'ютерних технологій

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

Дисципліна «Технологія блокчейн та розподілені системи» частково використовує знання та вміння, набуті у ході вивчення курсів «Алгебра та геометрія», «Дискретна математика», «Програмування», «Теорія складності», «Асиметричні криптосистеми та протоколи», «Математичне моделювання», «Спеціальні розділи криптології», «Теорія інформації та кодування» та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням блокчейн-технологій та розподілених систем.

2. Зміст навчальної дисципліни

Лекції.

Тема 1. Блокчейн як об'єкт аналізу.

Лекція 1. Блокчейн як інструмент реалізації розподілених систем.

Лекція 2. Блокчейн як криптографічний об'єкт.

Лекція 3. Блокчейн як інструмент реалізації розподілених/децентралізованих систем обробки інформації та криптовалют: перше наближення.

Лекція 4. Блокчейн як принцип побудови систем обробки даних.

Тема 2. Надійність та анонімність блокчейнів.

Лекція 5. Стійкість блокчейну до розділення на підсистеми. Поняття про надійність функціонування блокчейну.

Лекція 6. Анонімність децентралізованих додатків.

Тема 3. Блокчейн-платформи.

Лекція 7. Блокчейн платформи. Платформа Hyperledger Linux Foundation. Hyperledger Fabric.

Лекція 8. Блокчейн платформи. Основи реалізації додатків на платформі Hyperledger Fabric.

Лекція 9. Блокчейн платформи. Платформа Ethereum

Лекція 10. Блокчейн платформи. Платформа DASH.

¹ Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

--	--	--

Лекція 11. Блокчейн платформи. Платформа Lisk.

Лекція 12. Блокчейн платформи. Платформа NEO.

Лекція 13. Блокчейн платформи. Lisk під мікроскопом. Зв'язність блокчейнів.

Лекція 14. Блокчейн платформи. Платформа Fantom. Масштабованість блокчейнів.

Лекція 15. Блокчейн платформи. Платформа Tezos.

Лекція 16. Блокчейн платформи. Платформа Binance.

Лекція 17. Блокчейн платформи. Платформа Cosmos.

Лекція 18. Майбутнє блокчейн-платформ

3. 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. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
3. Narayanan, Arvind, and Bonneau, Joseph, et al. Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction. Princeton University Press, 2016.
4. Koblitz N. A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987.- P.312.

● Навчальний контент

4. Методика опанування навчальної дисципліни (освітнього компонента)

Найменування розділів, тем	Розподіл за видами занять				
	Разом	Лекц.	Лабораторні роботи	МКР	СРС в т.ч. КР
Тема 1. Блокчейн як об'єкт аналізу.	22	8	6		8
Тема 2. Надійність та анонімність блокчейнів.	20	4	12		4
Тема 3. Блокчейн-платформи.	70	24			46
Підготовка до іспиту	36				36
Разом в семестрі:	150	36	18	2	94

5 Самостійна робота студента/аспіранта

Самостійна робота студента складається з:

--	--	--

--	--	--

- підготовки до МКР та іспиту шляхом опанування лекційного матеріалу,
- підготовки до захисту лабораторних робіт.

	<i>Вид самостійної роботи</i>	<i>Кількість годин СРС</i>
1	<i>Підготовка до лекційних занять</i>	12
2	<i>Підготовка до лабораторних робіт</i>	27
3	<i>Підготовка до МКР</i>	25
4	<i>Підготовка до іспиту</i>	30
		94

● **Політика та контроль**

5. Політика навчальної дисципліни (освітнього компонента)

● **Порушення термінів виконання завдань та заохочувальні бали**

<i>Заохочувальні бали</i>		<i>Штрафні бали</i>	
<i>Критерій</i>	<i>Ваговий бал, додається до рейтингу</i>	<i>Критерій</i>	<i>Ваговий бал, віднімається від базового балу</i>
<i>Активність на заняттях</i>	<i>+2 бали</i>	<i>Невчасне здання лабораторної роботи</i>	<i>-2 бали</i>

● **Відвідування занять**

Відвідування лекцій, практичних та лабораторних занять, а також відсутність на них, не оцінюється. Однак, студентам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал, розв'язуються супутні задачі, необхідні для виконання лабораторних робіт та успішного написання МКР. В разі великої кількості пропусків студент може бути недопущений до іспиту, якщо не встигне виконати навчальний план по лабораторних роботах та МКР.

● **Пропущені контрольні заходи**

Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

--	--	--

--	--	--

- **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 працівників 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 контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами (згідно “Положення про систему забезпечення якості вищої освіти у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського”, “Положення про організацію навчального процесу”).

6. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

- **Рейтингова система оцінювання**

№ з/п	Контрольний захід	Макс. бал	Ваговий коеф.	Кількість	Всього
1.	МКР	5	2	1	10
2.	Лабораторні роботи	5	2	3	30
3.	Іспит	5	12	1	60
	Всього				100

- **Умови допуску до іспиту**

Обов'язкова умова допуску до іспиту	Критерій
Поточний рейтинг	$RD \geq 18$
Модульна контрольна робота	Написана на позитивну оцінку (3 з 5)
Лабораторні роботи	Виконано не менше 2-х лабораторних робіт на позитивну оцінку (3 з 5)

- **Таблиця переведення рейтингових балів до оцінок за університетською шкалою ²**

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
$95 \leq RD \leq 100$	Відмінно	-

² Оцінювання результатів навчання здійснюється за рейтинговою системою оцінювання відповідно до рекомендацій Методичної ради КПІ ім. Ігоря Сікорського, ухвалених протоколом №7 від 29.03.2018 року.

--	--	--

--	--	--

$85 \leq RD \leq 94$	<i>Дуже добре</i>	-
$75 \leq RD \leq 84$	<i>Добре</i>	-
$65 \leq RD \leq 74$	<i>Задовільно</i>	-
$60 \leq RD \leq 64$	<i>Достатньо</i>	-
$RD < 60$	<i>Незадовільно</i>	-
<i>Невиконання умов допуску</i>	<i>Не допущено</i>	-

● **Іспит**

Підсумковим контролем є іспит. У цьому разі рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 40 балів). На іспиті студент одержує білет, в якому містяться два теоретичних питання, кожне з яких оцінюється на 20 балів та практична задача, правильний та повний розв'язок якої оцінюється на 20 балів, відповідно повні та правильні розв'язки всіх завдань білету оцінюються в 60 балів.

7. Додаткова інформація з дисципліни (освітнього компонента)

- Сертифікати проходження дистанційних чи онлайн курсів за відповідною тематикою можуть бути зараховані, якщо в програмі курсу розглянуто всі питання, які входять до змісту навчальної дисципліни (п.3) ;

- Перелік питань до іспиту повністю відповідає змісту дисципліни.

Нижче наведений орієнтовний перелік теоретичних питань до іспиту. Цей перелік може корегуватись якщо якісь теми були зменшені або збільшені в обсязі.

1. Комплексний підхід до визначення блокчейну.
2. Способи побудови систем обробки інформації та їх характеристики.
3. Загальні труднощі відомих протоколів консенсусу.
4. Побудова протоколів узгодження з теоретико-інформаційної стійкістю.
5. Реалізації протоколу типу «Proof-of-Assurance».
6. Геш-функція блокчейну: особливості криптоаналізу.
7. Визначення криптографічного протоколу NIZK з блокчейн-ядром.
8. Порівняння блокчейну із базами даних.
9. Блокчейн для краудсорсінгу обчислень.
10. CAP гіпотеза для баз даних та блокчейнів.
11. Надійність блокчейну.
12. Методи забезпечення анонімності блокчейну.
13. Методи деанонімізації в блокчейнах.
14. Характеристики блокчейну як принцип обробки даних.
15. Основні властивості та приклади децентралізованих додатків

--	--	--

- | | | |
|--|--|--|
| | | |
|--|--|--|
16. *Hyperledger Fabric — універсальний блокчейн.*
 17. *Загальна архітектура Hyperledger Fabric.*
 18. *Смарт-контракти Hyperledger Fabric – chaincode.*
 19. *Hyperledger Linux Foundation*
 20. *Dash та інші клони Bitcoin.*
 21. *Особливості криптографічних механізмів Dash*
 22. *Архітектура та особливості Lisk*
 23. *Архітектура та особливості NEO.*
 24. *Протокол узгодження dBFT 2.0.*
 25. *Зв'язність блокчейнів.*

Лабораторні роботи.

Цикл лабораторних робіт дозволяє студентам придбати такі навички та уміння:

- вміння працювати з системою Ethereum;
- реалізація смарт-контрактів;
- елементи створення децентралізованих додатків.

Завдання сформовані таким чином, що кожна з бригад може обрати один з двох типів лабораторних робіт:

перший тип спрямований на більш теоретичний характер роботи, в якому студенти повинні виступити як системний аналітик, який розробляє технічні вимоги (технічне завдання) на систему, другий тип спрямований на більш практичний характер роботи, в якому студенти виступають як корпоративний архітектор та програміст, який розробляє прикладну програмну систему.

Кількість студентів в бригаді – 2-3 студента.

Кількість балів за кожну лабораторну роботу – від 15 до 30 балів.

Лабораторна робота № 1.

Тема: „Розгортання систем Ethereum та криптовалюти”.

Мета роботи: «Отримання навичок налаштування платформ виконання смарт-контрактів та криптовалют».

Необхідні теоретичні відомості містяться на ресурсах мереж Internet, зокрема:

<https://medium.com/swlh/how-to-set-up-a-private-ethereum-blockchain-c0e74260492c>

<https://serveradmin.ru/ustanovka-i-nastroyka-nodyi-bitcoin-ethereum-dash-litecoin-cardano/>

https://medium.com/@pradeep_thomas/how-to-setup-your-own-private-ethereum-network-f80bcbaea088

Завдання на лабораторну роботу.

Для першого типу лабораторних робіт

Провести порівняльний аналіз особливостей розгортання систем криптовалют у порівнянні із системою Ethereum. Зробити висновок про можливість чи неможливість взаємозаміни модулів різних систем та пояснити причини.

Для другого типу лабораторних робіт

--	--	--

Провести налаштування обраної системи та виконати тестові операції в системі.

Варіанти завдань:

1. Система Ethtrium.
2. Bitcoin
3. Dash
4. NEO
5. Litecoin

Лабораторна робота № 2.

Тема: Реалізація смарт-контракту або анонімної криптовалюти.

Мета роботи: «Отримання навичок роботи із смарт-контрактами або анонімними криптовалютами»

Завдання на лабораторну роботу

Для першого типу лабораторних:

дослідження методів анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin;

оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

Для другого типу лабораторних робіт:

розгортання та запуск обраної анонімної валюти, протоколювання майнінгу, пошук слідів деанонімізації;

розгортання та запуск обраного смарт-контракту, підвищення ефективності роботи смарт-контракту з точки зору витрати гасу;

розробка власного смарт-контракту.

Варіанти завдань:

1. Існуючий смарт-контракт системи Ethtrium (<https://docs.soliditylang.org/en/v0.5.3/solidity-by-example.html>).
2. Власний смарт-контракт системи Ethtrium.
3. Monero
4. ZCash
5. Dash

Лабораторна роботи № 3.

Тема: Дослідження безпечної реалізації та експлуатації децентралізованих додатків.

--	--	--

--	--	--

Мета роботи: отримання навичок роботи із децентралізованими додатками та оцінка безпеки інформації при їх функціонуванні

Для першого типу лабораторних робіт:

дослідження вимог OWASP (безпека web-додатків) та складання аналогічних вимог для обраної системи децентралізованих додатків.

Для другого типу лабораторних робіт:

розробка децентралізованого додатку (наприклад, захисту інтелектуальної власності цифрового контенту) на обраній системі децентралізованих додатків.

Варіанти завдань.

Студенти самостійно обирають будь-яку з існуючих систем децентралізованих додатків на базі блокчейну.

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри ММЗІ, д.т.н., с.н.с. Кудін Антон Михайлович

Ухвалено кафедрою ММЗІ (протокол № 6 від 19.06.2024 р.)

Погоджено Методичною комісією НН ФТІ (протокол № 6 від 27.06.2024)

--	--	--