МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

_____
М. В. Афанасьєв

БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУНКИ

робоча програма навчальної дисципліни

Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Освітній рівень	**другий (магістерський)**
Освітня програма	**Кібербезпека**

Вид дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *Кібербезпеки*
та інформаційних технологій Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри Кібербезпеки та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробник:
Шматко О.В., к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Анотація навчальної дисципліни: Дисципліна “Блокчейн: математичні проблеми та застосунки” є вибірковою навчальною дисципліною за спеціальністю 125 “Кібербезпека”. Вона викладається у другому семестрі магістратури в обсязі 150 год.(5 кредитів ECTS), зокрема: лекції – 12 год., лабораторні – 28 год., самостійна робота – 110 год. У курсі передбачено два змістових модулі та одна модульна контрольна робота. Завершується дисципліна екзаменом.

Предметом навчальної вивчення навчальної дисципліни є теоретичні концепції, математичні проблеми, принципи функціонування блокчейн, принципи розробки та застосування смарт-контрактів, інтелектуального обчислювального елементу блокчейн технологій.

Метою навчальної дисципліни є засвоєння теоретичних основ та отримання практичних навичок з розробки застосунків на основі блокчейн технологій, розгортання та виконання смарт-контрактів.

Головне завдання курсу – освоєння принципів розробки застосунків з використанням технологій блокчейн, принципів кодування, розгортання і виконання розумних (смарт) контрактів - обчислювального елементу технології blockchain. Інтелектуальні контракти дозволяють реалізовувати визначені користувачем операції довільної складності, які неможливі через прості протоколи криптовалют. Вони дозволяють користувачам реалізовувати умови, правила та політику доменних додатків. Інтелектуальні контракти - це потужна функція, яка при правильній розробці та кодуванні може призвести до автономних, ефективних і прозорих систем.

Курс	**1М**	
Семестр	**2**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**12**
	лабораторні	**28**
Самостійна робота		**110**
Форма підсумкового контролю	**Екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
Математичні основи криптології	Основи криптографічного захисту
Основи теорії інформації	Забезпечення інформаційної безпеки

2. Компетентності та результати навчання за дисципліною:

Загальні компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у практичних ситуаціях (Здатність до застосування концептуальних знань та певних знань сучасних досягнень у професійній діяльності)	РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
КЗ 2. Знання та розуміння предметної області та розуміння професії. (Здатність розуміти сутність та соціальну значущість майбутньої професійної діяльності, виявляти стійкий інтерес до неї)	РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки;
КЗ 6. Здатність до пошуку, обробки та аналізу інформації з різних джерел. (Здатність до самостійного пошуку, аналізу, синтезу та використання інформації, необхідної для ефективного розв'язання професійних завдань.)	РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
Фахові компетентності	Результати навчання
КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
КФ 2. Здатність до використання інформаційних і комунікаційних технологій	РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;

3. Програма навчальної дисципліни

Змістовий модуль 1. Математичні основи технології блокчейн.

Тема 1. Основи блокчейн

Блокчейн: визначення, властивості і приклади індустріального застосування. Блокчейн як технологія в основі біткоїн. Таксономія блокчейнов. Мережевий протокол і клієнти.

Тема 2. Математичні основи технології блокчейн

Основи криптографії. Криптографія з відритим ключем, RSA. ElGamal. Еліптичні криві. Інфраструктура криптографії з відкритим ключем. Докази з нульовим розголошенням. Схеми поділу секрету.

Тема 3. Алгоритми консенсусу блокчейн

Візантійський стійкий алгоритм консенсусу. FLP-неможливість. Типи мереж і приклади алгоритмів консенсусу в них. Можливості, обмеження і завдання блокчейна. Proof-of-X.

Змістовий модуль 2. Основи програмування застосунків блокчейн та smart contracts.

Тема 4. Основи створення застосунків з Ethereum

Рахунки Ethereum. Зовнішні рахунки Ethereum. Рахунки смарт-контрактів. Транзакції. Блоки Ethereum. Транзакції End-to-end. Створення smart contracts. Розгортання smart contracts.

Тема 5. Створення Smart Contracts

Solidity та файли Solidity. Створення програми. Коментарі. Контракти. Структура контракту. Змінні стану. Структура. Модифікатори. Події. Перерахування. Функції. Типи даних у Solidity.

Розумні контракти. Написання простого контракту. Створення контрактів. Абстрактні контракти. Інтерфейси.

Тема 6. Розгортання Smart Contracts

Налагодження контрактів. Налагодження. Редактор Remix. Використання подій. Використання блочного провідника.

Теми лабораторних робіт

Лабораторна робота №1. Дослідження криптографічних застосунків в технології блокчейн. Криптографія з відкритим ключем. Хеш-функції.

Лабораторна робота №2. Основи роботи з Ethereum. Створення та розгортання smart-contracts.

Лабораторна робота №3. Основи роботи з Remix. Розгортання та налагодження смарт-контрактів.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання

сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лекційних і лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

- здатність застосовувати знання у практичних ситуаціях (Здатність до застосування концептуальних знань та певних знань сучасних досягнень у професійній діяльності); Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки;
- знання та розуміння предметної області та розуміння професії. (Здатність розуміти сутність та соціальну значущість майбутньої професійної діяльності, виявляти стійкий інтерес до неї). Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки; Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- здатність до пошуку, обробки та аналізу інформації з різних джерел. (Здатність до самостійного пошуку, аналізу, синтезу та використання інформації, необхідної для ефективного розв’язання професійних завдань. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
- здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності;
- здатність до використання інформаційних і комунікаційних технологій. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп’ютерних мережах; використати спеціалізовані комп’ютерні програми в професійній діяльності;

- обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрольна робота	Усього
Змістовий модуль	Тема	Тиждень				
Змістовий модуль 1.	Тема 1	1				
		2	2			2
	Тема 2	3	2			2
		4	2			2
		5				
		6	2			2
	Тема 3	7	2			2
		8		8	18	26
		9	2			2
		10				
Змістовий модуль 2.	Тема 4	11				
		12	2	8		10
	Тема 5	13				
		14	2	8		10
	Тема 6	15				
		16	2			2
	екзамен					40
Усього			18	24	18	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	Зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1. Основна

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. – Львів : Видавництво Львівської політехніки, 2015. – 256 с.

2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

3. Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. – Львів : Видавництво Львівської політехніки, 2013. – 96 с

5.2. Додаткова

4. F. Reid, M. Harrigan, An analysis of anonymity in the bitcoin system,Security and Privacy in Social Networks (2013) 197–223.

5. Eyal, E. G. Sirer, Majority is not Enough: Bitcoin Mining is Vulner-able, 2013.

6. G. O. Karame, E. Androulaki, S. Capkun, Double-spending fast pay-ments in bitcoin, Proceedings of the 2012 ACM conference on Computerand communications security. (2012).

7. F. Glaser, L. Bezzenberger, Beyond Cryptocurrencies - A Taxonomy ofDecentralized Consensus Systems, in: European Conference on Infor-mation Systems, 57, pp. 1–18.

5.3. Інформаційні ресурси в Інтернеті

8. www.coindesk.com/information/applications-use-cases-blockchains/ - кейсі та прикладне застосування блок-чейн

9. https://www.nasdaq.com/article/4-innovative-use-cases-for-blockchain-cm901636 - інноваційне використання блокчейн

10. https://www.youtube.com/watch?v=cHe_ow9v094 - Starting 16 minutes

11. Сайт персональних начальних систем ХНЕУ імені С. Кузнеця за дисципліною «Блокчейн: математичні проблеми та застосунки» https://pns.hneu.edu.ua/course/view.php?id=5682.