Силабус освітнього компонента
Програма навчальної дисципліни

Blockchain: основи та приклади застосування

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
5

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».
Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.
Детальніше про викладача на сайті кафедри

ВОРОПАЙ Наталя Ігорівна

voropay.n@gmail.com
Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 30 наукових та навчально-методичних праць.. Провідний лектор з дисциплін: «Технології програмування Ч.1», «Децентралізовані системи», «Захист об´єктів критичної інфраструктури» , «Антивірусний захист інформації», «Блокчейн та смарт-технології в електронному документообігу».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Блокчейн – новітня технологія, інтерес до якої зріс разом з популярністю криптовалют. Але є десятки інших способів використання блокчейна у відриві від криптовалюти. Блокчейн-технологію відносять до головного технологічного прориву з часів винаходу Інтернету. Навчальна дисципліна "Blockchain: основи та приклади застосування" є вибірковою навчальною дисципліною.

Мета та цілі дисципліни

Засвоєння теоретичних основ використання блокчейн технології, основи криптовалют та смарт-контрактів. Вивчення дисципліни сприяє освоєнню принципів застосування криптографічних методів у блокчейн технологіях; знання основних принципів криптовалют; основні обмеження та ризики створення та використання криптовалют; ознайомлення з методологічними основами розробки та функціонування блокчейн платформ.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов’язань.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об’єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Основи математичного моделювання, Основи криптографічного захисту, Безпека в інформаційно-комунікаційних системах.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Технологія Блокчейн не тільки BitCoin. Принцип роботи BitCoin. Технологія Блокчейн не тільки BitCoin. Централізовані та децентралізовані мережі – основні поняття. Основні поняття майнінгу. Транзакції. Проблема візантійских генералів. Направлений ациклічний граф. Реєстр – основа біткоїна. Принцип роботи біткоїн. Біткоїн-транзакції. Майданчики обміну.	2

Тема 2. Правила формування блоків в блокчейн. Правила формування блоку. Затримки підтвердження транзакцій.	2
Тема 3. Токенізація та смарт-контракти. Яку роль грають смарт-контракти у токенізації? Види токенів та їх відмінності Що необхідно для вибухового зростання ціни та прийняття BTC? Як придбати токени?	2
Тема 4. Принципи формування та особливості Bitcoin Script. Основні підходи до завдання умов щодо розподілу і трати монет. Схема BITCOIN-ТРАНЗАКЦІЇ BITCOIN SCRIPT. Операції у BITCOIN SCRIPT. Приклад виконання BITCOIN SCRIPT для P2PKH. Приклад з MULTISIGNATURE. Використання механізму LOCKTIME. Нестандартні транзакції за допомогою BITCOIN SCRIPT. Статистика транзакцій у мережі BITCOIN. Статистика входів транзакцій. Статистика об'єму монет від типу транзакції, що передаються. Які ще «TRANSACTION PUZZLES» можна знайти у транзакціях BITCOIN?	2
Тема 5. Формування Atomic Swap. Ідея ATOMIC SWAPS і вимоги до облікової системи. Дії користувачів при ATOMIC SWAPS. Принципи роботи ATOMIC SWAPS. Обмеження ATOMIC SWAPS. Застосування ATOMIC SWAPS децентралізованими біржами. Проблема PANIC SELLS.	2
Тема 6. Проведення транзакцій та формати ключів у BitCoin. Кодування BASE58CHECK. Управління ключами в мережі биткоїн. Ключі, їх формування. Створення транзакції. Структура транзакції. Входи та виходи транзакції. Формування вірного блоку.	2
Тема 7. Блокчейн та IoT. Введення в блокчейн. Перспективи блокчейну. Proof-of-work, POW,PoW. Proof of Stake,метод захисту у криптовалютах для доказу частки володіння. Цифровий підпис. Децентралізована бухгалтерська книга. Перехід від технології M2M до технології IOT. Можливі загрози. Інформаційна безпека інтернету речей. Asset taxonomy. Threat taxonomy. Attack scenario criticality. Заходи безпеки. Заходи безпеки на основі блокчейн. Блокчейн щодо безпеки Інтернету речей. За межами мережі: обладнання Blockchain-IoT.	2
Тема 8. Апаратне та програмне забезпечення безпеки. Апаратне забезпечення. Схема MUSIG. Криптографічні зобов'язання. Зобов'язання Педерсена. Кодування основного секрету. Типи детерміністичних гаманців. Генерація ключів для HD WALLET. Функції породження ключів. Принципи кільцевого підпису. Головне завдання цифрового гаманця. Оброблення та зберігання ключів на сервері. Холодні, теплі та гарячі гаманці. CoinJoin.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Основи взаємодії з інтерфейсом Bitcoin вузла. Ознайомлення з роботою Bitcoin Core та його інтерфейсами. Студенти вчаться налаштовувати локальний вузол, досліджувати структуру блоків і транзакцій, а також виконувати базові операції через консольні команди.	2	0,1
Тема 2 Робота з тестовою мережею Ethereum.	2	0,1

Практика взаємодії з мережею Ethereum у тестовому середовищі. Виконання транзакцій, створення та деплой смарт-контрактів у середовищі Remix або Truffle, аналіз роботи тестових токенів.		
Тема 3. Робота з тестовою мережею Monero. Вивчення особливостей конфіденційних транзакцій у Monero. Студенти навчаються генерувати гаманці, надсилати й отримувати монети у тестовій мережі, а також аналізувати особливості використання ключів і механізму кільцевих підписів.	4	0,1
Тема 4. Основи взаємодії з інтерфейсами тестової мережі EOS. Дослідження архітектури та можливостей EOS. Виконання базових операцій з акаунтами та смарт-контрактами через інтерфейси командного рядка (cleos) та веб-інструменти. Вивчення відмінностей EOS від інших блокчейн-платформ.	4	0,1
Тема 5. Робота з децентралізованим сховищем даних IPFS. Практичне ознайомлення з протоколом IPFS. Студенти навчаються встановлювати IPFS, додавати та отримувати файли з децентралізованої мережі, а також аналізувати переваги й обмеження децентралізованого зберігання даних.	4	
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i$=0,4

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Еволюція технологій блокчейну: від Bitcoin до сучасних рішень. Дослідження еволюції технології блокчейн від створення Bitcoin до появи альтернативних мереж та сучасних рішень. Студенти аналізують принципи роботи Proof-of-Work та Proof-of-Stake, роль майнінгу, проблеми масштабованості, а також порівнюють централізовані й децентралізовані підходи. Особлива увага приділяється прикладам реального застосування блокчейну поза межами криптовалют.	0,1
Тема 2. Смарт-контракти та безпека транзакцій у блокчейні. Дослідження принципів функціонування смарт-контрактів та їх роль у токенізації й децентралізованих застосунках. Студенти вивчають приклади використання Bitcoin Script та Ethereum Smart Contracts, аналізують ризики, пов'язані з виконанням контрактів, уразливості (наприклад, «DAO Hack»), а також підходи до забезпечення безпеки транзакцій.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Історія розвитку блокчейн-технологій. Етапи становлення від Bitcoin до сучасних багатофункціональних платформ.	6
Тема 2. Proof-of-Work vs Proof-of-Stake.	6

Порівняння алгоритмів консенсусу за критеріями енергоспоживання, швидкості та безпеки.	
Тема 3. Lightning Network. Технологія другого рівня для масштабування Bitcoin і прискорення транзакцій.	6
Тема 4. Стабільні монети (Stablecoins). Криптовалюти, прив'язані до фіатних валют чи активів для зменшення волатильності.	6
Тема 5. NFT (невзаємозамінні токени). Унікальні цифрові активи для мистецтва, ігор та авторського права.	6
Тема 6. Zero-Knowledge Proofs (ZKP). Метод підтвердження інформації без її розкриття, важливий для приватності у блокчейні.	6
Тема 7. DAOs (децентралізовані автономні організації). Нова форма управління проектами через смарт-контракти без централізованого контролю.	6
Тема 8. DeFi (децентралізовані фінанси). Фінансові сервіси на блокчейні без посередників (банків чи бірж).	6
Тема 9. Криптографія у блокчейні. Використання хеш-функцій і цифрових підписів для забезпечення цілісності та захисту транзакцій.	5
Тема 10. Регуляторні аспекти блокчейну та криптовалют. Сучасні підходи до правового регулювання у світі та в Україні.	5
Загальна кількість годин	**58**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0e26ed5b-990d-4271-85f8-573434a7722f/content
2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.
3. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
4. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

5. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

6. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher. chrome-https://lms.maaldatalabs.com/uploads/Blockchain_basic.pdf.
7. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder.
https://books.google.com.ua/books?id=LchFDAAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,4	0,2		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно	FX

	(потрібне додаткове вивчення)	
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ