Силабус освітнього компонента
Програма навчальної дисципліни

Децентралізовані системи

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Спеціальна (фахова),Вибірковаа

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
4

Мова викладання
Українська, англійська

Викладачі, розробники

Гаврилова Алла Андріївна

alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації», «Безпека в DevOps», «Організація та безпека баз даних», «Управління ІТ-проєктами та їх безпека» у студентів бакалавріату
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Децентралізовані системи" є вибірковою навчальною дисципліною. Предметом вивчення навчальної дисципліни є теоретичні концепції, принципи функціонування, розробки та застосування до комплексних децентралізованих технологій, принципів формування mesh networks.

Мета та цілі дисципліни

Засвоєння теоретичних основ та отримання практичних навичок використання децентралізованих технологій, принципів формування mesh networks.

Формат занять

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

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Комп'ютерні мережі, Комплексні системи захисту інформації, Безпека в інформаційно-комунікаційних системах, Основи математичного моделювання систем безпеки

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, практичні заняття, співбесіда, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Децентралізація в інформаційних системах. Поняття децентралізації для інформаційних систем. Децентралізовані файлообмінні системи. Застосування принципів децентралізації. Типова архітектура децентралізованих систем. Переваги та обмеження	2

децентралізованих систем	
Тема 2. Децентралізація як підхід в інформаційних системах. Пірингові мережі та протокол BitTorren. Принципи побудови одноранговій файлообмінної мережі. Принцип роботи та застосування Distributed Hash Table. Концепція web-of-trust. Принципи функціонування web-of-trust, BitMessage, IPFS. Алгоритм досягнення консенсусу у Filecoin	2
Тема 3. Криптографія у децентралізованих системах. Генерація та обробка ключових даних. Принципи генерації ключів. Генератори випадкових послідовностей. Генератори псевдовипадкових послідовностей. Функції породження ключів (KDF). Протоколи обміну ключами. Протокол Діффі-Хеллмана на еліптичних кривих. Протокол EKE. Концепція та застосування Merkle Tree. Різновиди цифрових підписів. Lamport one time signature. Winternitz one time signature. Мультипідпис. Пороговий підпис. Груповий підпис. Кільцевий підпис. Сліпа підпис.	2
Тема 4. Bitcoin як платформа. One-way peg and two-way peg sidechains. Пристрій Lightning Network. Механізм штрафування за шахрайство у каналі. Принципи роботи та застосування atomic swap. Застосування atomic swaps децентралізованими біржами. Proof-of-stake алгоритми досягнення консенсусу. Основні недоліки та ризики при використанні proof-of-stake.	2
Тема 5. Методи забезпечення конфіденційності у сучасних облікових системах. Стандарти CryptoNote. Модель транзакцій MimbleWimble. Принципи гомоморфного шифрування. Quadratic Arithmetic Programs	2
Тема 6. Розвиток децентралізованих технологій. Наштування протоколу Bitshares. Decentralised asset exchange. SmartCoins. Організація бази даних. Оптимізація виконання бізнес-логіки	2
Тема 7. Застосування децентралізованих підходів для організації різних систем. Принципи функціонування та розвиток mesh network. Популярні протоколи для організації mesh-мереж. Децентралізовані системи цифрової ідентифікації. Протоколи OpenID та OpenID Connect. Розширення можливостей глобальної системи ідентифікації за допомогою технології blockchain.	2
Тема 8. Децентралізовані платформи електронного голосування. Децентралізований підхід до проведення електронного голосування. Використання технології blockchain для системи електронного голосування	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми практичних/семінарських занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Реалізація “baby” blockchain. Діаграма класів. Клас Hash. Клас KeyPair. Клас Signature.	2	1
Тема 2. Реалізація “baby” blockchain. Клас Account. Клас Operation. Клас Transaction	2	1
Тема 3. Реалізація “baby” blockchain. Клас Block. Клас Blockchain.	2	1

Тема 4. Реалізація криптографічного алгоритму. Vigenère Cipher. Шифр AES.	2	1
Тема 5. Реалізація криптографічного алгоритму. SHA-1. Keccak.	2	1
Тема 6. Реалізація криптографічного алгоритму. RSA. ECDSA. Підписи Шнорра. Ring traceable signatures	2	1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i=6$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Мережна безпека	2
Тема 2. Безпека ОС і кінцевих вузлів	2
Загалом	$\sum_{i=1}^{m} b_i=4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу.

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Технології децентралізованих бірж. 1. Принципи функціонування децентралізованих бірж. 2. Escrow. 3. Atomic Swap. 4. 0x Protocol. 5. Internal exchanges.	14
Тема 2. Децентралізований аукціон. 1. Принцип роботи онлайн-аукціону. 2. Принцип роботи децентралізованого онлайн-аукціону.	14
Тема 3. Використання концепцій sharding, off-chain і dag для масштабування облікових систем. 1. Використання off-chain протоколів. 2. Sharding у blockchain-based системах. 3. Обмін повідомленнями між shardchains. 4. Конструкція та застосування Directed acyclic graph 5. Архітектура розподілених облікових систем на основі DAG.	15
Тема 4. Особливості і роль криптографічних зобов'язань в облікових системах. 1. Особливості та методи побудови криптографічних зобов’язань. 2. Зобов’язання Педерсена. 3. Підміна знань та підходи Nothing Up My Sleeve. 4. Схема ElGamal commitment. 5. Протокол ідентифікації Шнорра як інтерактивного схема докази з нульовим розголошенням. 6. Схема ідентифікації Шнорра	15

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

1. Онлайн-курс «Безпека кінцевих вузлів»
https:// https://www.netacad.com/launch?id=91d8317a-f1bb-4284-9c49-48845e8bd4d4&tab=curriculum&view=bbbfbe90-c990-513d-bd24-f45fab585fd2.

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

1. Dragoslav D Siljak, Decentralized Control of Complex Systems, 2012. https://www.abebooks.com/9780486486147/Decentralized-Control-Complex-Systems-Dover-0486486141/plp
2. Arthur G.O. Mutambara. Decentralized Estimation and Control for Multisensor Systems, 2019. https://www.perlego.com/book/1493337/decentralized-estimation-and-control-for-multisensor-systems-pdf
3. Anuj Bhatia. Centralized vs Decentralized Air-conditioning Systems: Quick Book, 2015. https://www.cedengineering.com/userfiles/M05-012%20-%20Centralized%20Vs.%20Decentralized%20Air%20Conditioning%20Systems%20-%20US.pdf

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
0,6	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:

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

де: *П* – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$К$ – 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.

$$К = \frac{К_1 \cdot b_1 + К_2 \cdot b_2 + ... + К_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $К$, *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 (потрібне додаткове вивчення)	FX
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** Сергій ЄВСЕЄВ