Силабус освітнього компонента
Програма навчальної дисципліни

Децентралізовані системи

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
4

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів

Детальніше про викладача на сайті кафедри

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджанс» ,

«Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.
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

Навчальна дисципліна "Децентралізовані системи" є вибірковою навчальною дисципліною. Вивчення дисципліни «Децентралізовані системи» присвячене різним підходам щодо розроблення і застосування алгоритмів, комп'ютерних програм, і їх нових компонентів, архітектури, масштабуванню і розподіленню для досягненню максимальних технічних і комерційних можливостей.

Мета та цілі дисципліни

Засвоєння студентами 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

КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. 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.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. 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 – 58год.

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

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

Теми лекційних занять

Тема 1. Децентралізація в інформаційних системах.
Поняття децентралізації для інформаційних систем. Децентралізовані файлообмінні системи. Застосування принципів децентралізації. Типова архітектура децентралізованих систем. Переваги та обмеження децентралізованих систем.
Тема 2. Децентралізація як підхід в інформаційних системах.
Піринговi 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.
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.
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.
Тема 5. Методи забезпечення конфіденційності у сучасних облікових системах.
Стандарти CryptoNote. Модель транзакцій MimbleWimble. Принципи гомоморфного шифрування. Quadratic Arithmetic Programs.
Тема 6. Розвиток децентралізованих технологій.
Влаштування протоколу Bitshares. Decentralised asset exchange. SmartCoins. Організація бази даних. Оптимізація виконання бізнес-логіки.
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.
Тема 8. Децентралізовані платформи електронного голосування.
Децентралізований підхід до проведення електронного голосування. Використання технології blockchain для системи електронного голосування.
Тема 9. Технології децентралізованих бірж.
Принципи функціонування децентралізованих бірж. Escrow. Atomic Swap. 0x Protocol. Internal exchanges.
Тема 10. Децентралізований аукціон.
Принцип роботи онлайн-аукціону. Принцип роботи децентралізованого онлайн-аукціону.
Тема 11. Використання концепцій sharding, off-chain і dag для масштабування облікових систем.
Використання off-chain протоколів. Sharding у blockchain-based системах. Обмін повідомленнями між shardchains. Конструкція та застосування Directed acyclic graph. Архітектура розподілених облікових систем на основі DAG.
Тема 12. Особливості і роль криптографічних зобов'язань в облікових системах.
Особливості та методи побудови криптографічних зобов’язань. Зобов’язання Педерсена. Підміна знань та підходи Nothing Up My Sleeve. Схема ElGamal commitment. Протокол ідентифікації Шнорра як інтерактивного схема докази з нульовим розголошенням. Схема ідентифікації Шнорра. Використання зобов’язань Педерсена для доказів із нульовим розголошенням. Використання зобов’язань Педерсена у Confidential Transaction. Алгоритми підпису, які будуються на використанні геш-функцій. Конструкція HORS. Схема підпису Меркла. Сімейство алгоритмів Sphincs.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Реалізація “baby” blockchain. Діаграма класів. Клас Hash. Клас KeyPair. Клас Signature.
Тема 2. Реалізація “baby” blockchain. Класс Account. Клас Operation. Клас Transaction.
Тема 3. Реалізація “baby” blockchain. Клас Block. Клас Blockchain.
Тема 4. Реалізація криптографічного алгоритму. Vigenère Cipher. Шифр AES.
Тема 5. Реалізація криптографічного алгоритму. SHA-1. Keccak.
Тема 6. Реалізація криптографічного алгоритму. RSA. ECDSA. Підписи Шнорра. Ring traceable signatures.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

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. Dragoslav D Siljak, Decentralized Control of Complex Systems, 2012. https://www.abebooks.com/9780486486147/Decentralized-Control-Complex-Systems-Dover-0486486141/plp
7. 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
8. 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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 20% семестрової оцінки;
•іспит: 40% семестрової оцінки.

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

Студент 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

28.08.2024 — Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП
Роман КОРОЛЬОВ