



Силабус освітнього компонента Програма навчальної дисципліни



Комплексний тренінг “Блокчейн: математичні проблеми та застосунки”

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Професійна підготовка, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники



ЄВСЕЄВ Сергій Петрович

serhii.yevseyev@khp.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](#)

Загальна інформація

Анотація

Навчальна дисципліна Комплексний тренінг “Блокчейн: математичні проблеми та застосунки” присвячена глибокому вивченню блокчейн-технологій та їхнього використання у захисті інформації. Курс охоплює математичні аспекти побудови блокчейн-систем, протоколи консенсусу, криптографічні алгоритми та практичні підходи до створення і безпечного впровадження блокчейн-рішень. Курс завершується комплексним тренінгом із розробки та впровадження блокчейн-рішень, де студенти застосовують отримані знання для вирішення реальних проблем з використанням сучасних інструментів.

Мета та цілі дисципліни

Метою дисципліни є формування у студентів глибокого розуміння блокчейн-технологій з точки зору кібербезпеки та захисту інформації, а також надання практичних навичок у розробці та впровадженні блокчейн-рішень для захисту даних і створення безпечних систем.

Формат занять

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

Компетентності

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

PH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

PH19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

PH21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

PH23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Мережева та хмарна безпека, Вебезпека, Бездротова та мобільна безпека.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до блокчейн-технологій.

Основні концепції блокчейну: децентралізація, розподілені реєстри, криптографія. Історія розвитку блокчейну: від біткоїна до сучасних платформ. Переваги та виклики блокчейн-технологій.

Тема 2. Архітектура блокчейн-систем.

Структура блоків та ланцюгів блоків. Децентралізовані мережі: вузли, транзакції, блоки, механізми синхронізації. Типи блокчейнів: публічні, приватні, консорціумні блокчейни.

Тема 3. Криптографія в блокчейні.

Основи криптографії: хеш-функції та їх роль у блокчейні. Симетрична та асиметрична криптографія. Алгоритми цифрових підписів та їх застосування у блокчейні.

Тема 4. Математичні проблеми масштабованості блокчейну.

Проблеми збільшення розміру блоків та швидкості транзакцій. Рішення для масштабування. Вплив масштабованості на безпеку та продуктивність.

Тема 5. Смарт-контракти: архітектура та застосування.

Концепція смарт-контрактів: принципи роботи та основи програмування. Розробка та тестування смарт-контрактів на базі Ethereum. Потенційні вразливості та захист смарт-контрактів.

Тема 6. Безпека блокчейну та захист даних.

Блокчейн як механізм захисту від атак. Методи захисту конфіденційності та забезпечення цілісності даних. Механізми захисту смарт-контрактів та цифрової ідентифікації.

Тема 7. Блокчейн у кібербезпеці.

Використання блокчейну для захисту інформації та управління доступом. Застосування блокчейну для забезпечення конфіденційності даних та аутентифікації. Криптографічні методи захисту інформації у блокчейні.

Тема 8. Інтеграція блокчейн-технологій у корпоративні системи.

Приватні та консорціумні блокчейн-системи для корпоративного середовища. Моделі управління ланцюгами постачання, реєстрами та контрактами на базі блокчейну. Безпека корпоративних блокчейн-рішень.

Тема 9. Майбутнє блокчейн-технологій: квантова криптографія та нові протоколи.

Можливі загрози квантових обчислень для блокчейну. Перспективи використання квантової криптографії для захисту блокчейнів. Тенденції розвитку нових протоколів консенсусу та безпеки.

Тема 10. Практичні аспекти розробки блокчейн-рішень.

Інструменти для розробки блокчейн-додатків. Розробка децентралізованих додатків. Підготовка та тестування блокчейн-рішень для реальних сценаріїв.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Огляд та налаштування блокчейн-інфраструктури.

Тема 2. Робота з криптографічними алгоритмами.

Тема 3. Розробка смарт-контрактів на платформі Ethereum.

Тема 4. Верифікація та безпека смарт-контрактів.

Тема 5. Створення власного токєну.

Тема 6. Застосування блокчейну для кібербезпеки.

Тема 7. Масштабованість блокчейн-систем

Тема 8. Розробка рішень для корпоративного блокчейну

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. Blockchain and decentralized systems : in three volumes. V.3 P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kharkiv : PROMART, 2022. – 288 p. : 178 figures; 7 tables; references: 145 titles. URL: http://library.kpi.kharkov.ua/files/new_postupleniya/blocv3.pdf
2. Melanie Swan Blockchain: Blueprint for a New Economy URL: https://books.google.com.ua/books?id=RHJmBgAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
3. Інформаційна безпека та інформаційні технології. – Х.; ТОВ “ДІСА ПЛЮС”, 2019. - 322 с. [Електронний ресурс]. – Режим доступу : http://library.kpi.kharkov.ua/files/new_postupleniya/ibtaait.pdf
4. Кібербезпека та інформаційні технології. – Х.; ТОВ “ДІСА ПЛЮС”, 2020. -380 с. [Електронний ресурс]. – Режим доступу : https://dspace.sfa.org.ua/bitstream/123456789/1550/1/Abdalla_traffic.pdf
5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. [Електронний ресурс]. – Режим доступу : <http://kist.ntu.edu.ua/textPhD/tzi.pdf>.

6. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсєєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с. [Електронний ресурс]. – Режим доступу : <http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf>

Додаткова література :

7. Daniel Drescher. Blockchain Basics: A Non-Technical Introduction in 25 Steps URL:

https://lms.maaldataabs.com/uploads/Blockchain_basic.pdf

8. William Stallings. Cryptography and Network Security: Principles and Practice URL:

<https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security-principles-and-practice-7th-global-edition.pdf>

9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. [Електронний ресурс]. – Режим доступу :

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. [Електронний ресурс]. – Режим доступу :

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

11. 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. [Електронний ресурс]. – Режим доступу :

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% семестрової оцінки;
- залік: 30% 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
Ольга КОРОЛЬ