**Силабус освітнього компонента**
Програма навчальної дисципліни

# Комплексний тренінг «Блокчейн: математичні проблеми та застосунки»

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Професійна підготовка, Вибіркова

**Рівень освіти**
Другий (магістерський)

**Форма навчання**
Денна, заочна

**Семестр**
2

**Мова викладання**
Українська, англійська

## 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. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту 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 заняття, самостійна робота, консультації. Підсумковий контроль – диференційований 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.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. 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.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН23. 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 – 16 год., практичні роботи – 32 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Вища математика, Основи програмування, Комп'ютерні мережі, Математичні основи криптології, Основи криптографічного захисту.

### 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. Вступ до блокчейн-технологій. Архітектура блокчейн-систем.** Основні концепції блокчейну: децентралізація, розподілені реєстри, криптографія. Історія розвитку блокчейну: від біткоїна до сучасних платформ. Переваги та виклики блокчейн-технологій. Структура блоків та ланцюгів блоків. Децентралізовані мережі: вузли, транзакції, блоки, механізми синхронізації. Типи блокчейнів: публічні, приватні, | 2 |

| | |
|---|---|
| консорціумні блокчейни. | |
| **Тема 2. Криптографія в блокчейні.** Основи криптографії: хеш-функції та їх роль у блокчейні. Симетрична та асиметрична криптографія. Алгоритми цифрових підписів та їх застосування у блокчейні. | 2 |
| **Тема 3. Математичні проблеми масштабованості блокчейну.** Проблеми збільшення розміру блоків та швидкості транзакцій. Рішення для масштабування. Вплив масштабованості на безпеку та продуктивність. | 2 |
| **Тема 4. 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. | 2 |
| **Тема 5. Безпека блокчейну та захист даних. Блокчейн у кібербезпеці.** Блокчейн як механізм захисту від атак. Методи захисту конфіденційності та забезпечення цілісності даних. Механізми захисту смарт-контрактів та цифрової ідентифікації. Використання блокчейну для захисту інформації та управління доступом. Застосування блокчейну для забезпечення конфіденційності даних та аутентифікації. Криптографічні методи захисту інформації у блокчейні. | 2 |
| **Тема 6. 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. | 2 |
| **Тема 7. 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. | 2 |
| **Тема 8. Практичні аспекти розробки блокчейн-рішень.** Інструменти для розробки блокчейн-додатків. Розробка децентралізованих додатків. Підготовка та тестування блокчейн-рішень для реальних сценаріїв. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Огляд та налаштування блокчейн-інфраструктури.** Ознайомлення з архітектурою блокчейн-систем, принципами роботи вузлів (нод), консенсусом і структурою блоків. Практичне налаштування середовища для роботи з блокчейном (Ethereum, Hyperledger, Ganache тощо). | 4 | 0,1 |
| **Тема 2. Робота з криптографічними алгоритмами.** Вивчення принципів криптографії, що використовуються в блокчейні: геш-функції, цифрові підписи, шифрування відкритим ключем. Практичне застосування бібліотек для | 4 | 0,1 |

| | | |
|---|---|---|
| реалізації криптографічних алгоритмів. | | |
| **Тема 3. Розробка смарт-контрактів на платформі Ethereum.** Створення та тестування смарт-контрактів мовою Solidity. Ознайомлення з інструментами Remix IDE, Truffle, Hardhat. Виконання простих транзакцій у тестовій мережі. | 4 | 0,1 |
| **Тема 4. Верифікація та безпека смарт-контрактів.** Дослідження типових вразливостей у смарт-контрактах. Застосування методів статичного та динамічного аналізу для перевірки їх безпеки. Тестування контрактів із використанням інструментів аудиту. | 4 | 0,1 |
| **Тема 5. Створення власного токену.** Розробка токену стандарту ERC-20 або ERC-721. Вивчення процесу розгортання токену в тестовій мережі Ethereum. Аналіз принципів функціонування токенів у децентралізованих екосистемах. | 4 | 0,1 |
| **Тема 6. Застосування блокчейну для кібербезпеки.** Розгляд сценаріїв використання блокчейну для забезпечення цілісності, автентичності та доступності даних. Реалізація прототипу рішення для зберігання цифрових відбитків (хешів) у блокчейні. | 4 | 0,1 |
| **Тема 7. Масштабованість блокчейн-систем.** Аналіз проблем продуктивності блокчейну та методів їх вирішення. Практичне дослідження шардингу, офчейн-транзакцій та рішень другого рівня (Layer 2). | 4 | 0,1 |
| **Тема 8. Розробка рішень для корпоративного блокчейну.** Ознайомлення з корпоративними платформами (Hyperledger Fabric, Corda). Проєктування моделі приватного блокчейну для підприємства. Створення прототипу системи децентралізованого обміну даними між організаціями. | 4 | 0,1 |
| **Загальна кількість годин** | **32** | $\sum_{i=1}^{n} a_i = 0{,}8$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Архітектура блокчейн-систем і криптографічні основи їх функціонування.** У роботі розглядаються базові принципи роботи блокчейн-систем: структура блоків, типи мереж, механізми консенсусу та роль криптографії. Особлива увага приділяється геш-функціям, цифровим підписам і криптографічним методам забезпечення цілісності та автентичності даних у блокчейні. | 0,1 |
| **Тема 2. Смарт-контракти, безпека та майбутні тенденції розвитку блокчейн-технологій.** Робота спрямована на оцінку знань із практичного використання блокчейну: створення та верифікація смарт-контрактів, методи захисту даних, запобігання вразливостям. Також розглядаються перспективи розвитку технології — | 0,1 |

| | |
|---|---|
| інтеграція у корпоративні системи, вплив квантових обчислень і нові підходи до підвищення масштабованості та безпеки блокчейнів. | |
| **Загалом** | $\sum_{i=1}^{m} b_i$=0,2 |

### Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

**Опрацювання теоретичного матеріалу**

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Принципи роботи алгоритмів консенсусу (PoW, PoS, DPoS, PBFT, PoA).** Порівняння ефективності, безпеки та енергоспоживання різних алгоритмів. | 8 |
| **Тема 2. Економічні моделі в блокчейн-екосистемах (Tokenomics).** Аналіз ролі токенів у підтримці стабільності та стимулюванні користувачів. | 8 |
| **Тема 3. Смарт-контракти у сфері фінансів (DeFi).** Децентралізовані біржі, кредитування, страхування та ризики їх використання. | 7 |
| **Тема 4. NFT (невзаємозамінні токени) та їх правовий статус.** Технологічні та правові аспекти створення, використання й захисту NFT. | 7 |
| **Тема 5. Застосування блокчейну в електронному урядуванні.** Прозорість реєстрів, електронне голосування, цифрова ідентифікація. | 7 |
| **Тема 6. Використання блокчейну в логістиці та ланцюгах постачання.** Відстеження товарів, захист від підробок, підвищення ефективності бізнес-процесів. | 7 |
| **Тема 7. Захист конфіденційності у блокчейні: Zero-Knowledge Proofs, zk-SNARKs, zk-STARKs.** Принципи роботи доказів з нульовим розголошенням і їх практичне застосування. | 7 |
| **Тема 8. Блокчейн і Інтернет речей (IoT).** Безпечна взаємодія між пристроями, децентралізоване керування даними. | 7 |
| **Тема 9. Регулювання блокчейн-технологій у світі та в Україні.** Огляд законодавчих ініціатив, оподаткування, AML/KYC вимог. | 7 |
| **Тема 10. Квантова загроза для блокчейн-систем і шляхи її подолання.** Аналіз потенційних ризиків від квантових обчислень і розробка постквантових алгоритмів безпеки. | 7 |
| **Загальна кількість годин** | **72** |

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

## Література, навчальні матеріали та інформаційні ресурси

### 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/ibtait.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. Євсеєв, 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.maaldatalabs.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. Khokhlachova, 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

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), $k_4$ |
|---|---|---|---|
| 0,8 | 0,2 | | |

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 (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**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 |  | **Гарант ОП**<br>Ольга КОРОЛЬ |