



Силабус освітнього компонента

Програма навчальної дисципліни



Блокчейн та смарт-технології в електронному документообігу

Шифр та назва спеціальності

К4 – Управління інформаційною безпекою

Інститут

ІНІ комп'ютерних наук та інформаційних технологій

Спеціалізація

Кафедра

Кібербезпеки (328)

Освітня програма

Управління інформаційною безпекою

Тип дисципліни

Обов'язкова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна

Семестр

7

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 статей 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](#)



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 "Блокчейн та смарт- технології в електронному документообігу" є обов'язковою навчальною дисципліною.

Мета та цілі дисципліни

Засвоєння теоретичних основ використання блокчейн технології, основи криптовалют та смарт-контрактів в електронному документообігу. 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

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність спілкуватися іноземною мовою.

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.

СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.

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.

РН4. Вільно спілкуватися державною мовою.

РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

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 інформаційною 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-комунікаційних 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 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Моделювання інформаційних систем, Основи криптографічного захисту, Інструментальні засоби програмування.

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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Технологія Блокчейн не тільки BitCoin. Технологія Блокчейн не тільки BitCoin. Централізовані та децентралізовані мережі – основні поняття. Основні поняття майнінгу. Транзакції. Проблема візантійських генералів. Направлений ациклічний граф.	4
Тема 2. Принцип роботи BitCoin. Реєстр – основа біткоїна. Принцип роботи биткоїн. Біткоїн-транзакції. Майданчики обміну.	4
Тема 3. Застосування криптографії в блокчейн. Основні вимоги до криптографічних геш-функцій. Формування ключів. Основи використання еліптичної кривої при формуванні ключів. Можливі труднощі з консенсусом. Протокол BITMESSAGE.	4
Тема 4. Правила формування блоків в блокчейн. Правила формування блоку. Затримки підтвердження транзакцій.	4
Тема 5. Правила роботи блокчейн в біткоїн. Основні вимоги щодо формування транзакції, правильного блоку. Основні підходи до завдання умов щодо розподілу і держати монет. Схема Bitcoin-транзакції. BITCOIN SCRIPT. Операції у BITCOIN SCRIPT. Використання механізму LOCKTIME.	4
Тема 6. Проведення транзакцій та формати ключів в біткоїн. Кодування BASE58CHECK. Управління ключами в мережі биткоїн. Ключі, їх формування. Створення транзакції. Структура транзакції. Входи та виходи транзакції. Формування правильного блоку.	3
Тема 7. Формування SmartCoins. Смарт-контракти на MARKET PEGGED ASSETS. Маржинальна торгівля, основні поняття та принципи побудови. Криптовалютні біржі з можливістю торгівлі з плечом. Ризики маржинальної торгівлі. Опції підвищення конфіденційності користувачів.	3
Тема 8. Облікова система Atomic Swap. Ідея Atomic Swaps і вимоги до облікової системи. Дії користувачів при атомарному обміні. Обмеження ATOMIC SWAPS.	3
Тема 9. Блокчейн та смарт-контракти. Результат виконання смарт-контракту. Критерії відмінності такласифікація платформ смарт-контрактів. Життєвий цикл смарт-контракту та популярні шаблони умов. Смарт-контракти у токенизації. Види токенів та їх відмінності. Підходи до створення STABLECOIN.	3
Загальна кількість годин	32

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Основи взаємодії з інтерфейсом Bitcoin-вузла. Робота спрямована на ознайомлення з базовою структурою Bitcoin-мережі та механізмами взаємодії з повним вузлом через інтерфейс командного рядка (CLI) або RPC-інтерфейс. Студент виконує підключення до вузла, переглядає блоки, транзакції, баланс гаманця, формує прості запити та аналізує відповіді Bitcoin Core.	4	0,1
Тема 2. Робота з тестовою мережею Ethereum (Ropsten/Goerli/Sepolia). У цій роботі студенти підключаються до тестової мережі Ethereum, створюють гаманець, отримують тестові ETH, вивчають структуру транзакцій та газу, виконують відправку транзакцій. Окрема частина роботи — взаємодія зі смарт-контрактами через Etherscan або спеціальні інструменти (Remix IDE, Web3 libraries).	3	0,1
Тема 3. Робота з тестовою мережею Monero. Лабораторна робота знайомить студентів із принципами конфіденційних транзакцій Monero. Виконується взаємодія з тестовою мережею, створення гаманців, перегляд прихованих адрес, перевірка транзакцій через спеціалізовані інструменти, використання RPC-інтерфейсу Monero-вузла для надсилання й аналізу транзакцій.	3	0,1
Тема 4. Основи взаємодії з інтерфейсами тестової мережі EOS. Студенти знайомляться з архітектурою EOS та її моделью облікових записів, ресурсів і смарт-контрактів. Практична частина передбачає створення тестового акаунта, отримання ресурсів (CPU, NET, RAM), виконання транзакцій, виклик простих смарт-контрактів через інструменти EOSIO CLI. Аналізуються результати та особливості механізму консенсусу DPoS.	3	0,1
Тема 5. Робота з децентралізованим сховищем даних IPFS. Мета роботи — освоєння принципів роботи децентралізованого файлового сховища IPFS. Студент встановлює локальний IPFS-вузол, додає файли, отримує їхні хеш-ідентифікатори, перевіряє розповсюдження даних у мережі, досліджує механізм Content-Addressing та Pinning. Також розглядається взаємодія IPFS з Web-додатками та блокчейн-системами.	3	0,1
Загальна кількість годин	16	$\sum_{i=1}^n a_i = 0,5$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Теми 1–4: Основи блокчейну, Bitcoin та криптографія. Контрольна робота спрямована на перевірку розуміння базових принципів технології блокчейн, відмінностей між централізованими та децентралізованими мережами, механізмів транзакцій та майнінгу, а також	0,1

криптографічних основ: геш-функцій, ключів, еліптичних кривих та консенсусу.

Теми 5–9: Транзакції, SmartCoins, Atomic Swap та смарт-контракти.

0,1

Контрольна робота охоплює глибокі аспекти роботи Bitcoin: формати ключів, структуру транзакцій, Bitcoin Script, а також технології SmartCoins, Atomic Swap та смарт-контракти різних платформ.

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. Консенсусні алгоритми в блокчейні та їх застосування в документообігу.

8

Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance (PBFT) та їх вплив на швидкість і безпеку обміну документами.

Тема 2. Розумні контракти (Smart Contracts) у бізнес-процесах.

8

Автоматизація погодження, підписання та зберігання документів за допомогою смарт-контрактів.

Тема 3. Токенізація документів та цифрові активи.

7

Як перетворити документи на токени для відстеження власності та контролю доступу.

Тема 4. Приватність та шифрування в блокчейн-системах документообігу.

7

Методи забезпечення конфіденційності та захисту персональних даних у блокчейні.

Тема 5. Інтеграція блокчейну з існуючими ERP та DMS-системами.

7

Практичні приклади інтеграції блокчейн-рішень у корпоративні системи документообігу.

Тема 6. Розподілені реєстри для електронного підпису та автентифікації документів.

7

Використання блокчейн для перевірки підписів та походження документів.

Тема 7. Регуляторні та юридичні аспекти використання блокчейну в документообігу.

7

Законодавство щодо електронного підпису, цифрових контрактів та зберігання даних.

Тема 8. Протоколи міжмережевого документообігу на базі блокчейн.

7

Обмін документами між організаціями у різних блокчейн-мережах.

Тема 9. Аудит та контроль змін у документах за допомогою блокчейну.

7

Механізми відстеження історії документів та їх версій.

Тема 10. Майбутні тренди блокчейн-технологій в електронному документообігу.

7

NFT-документи, децентралізовані автономні організації (DAO) для документообігу, інтеграція з AI для автоматичної обробки документів.

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.

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. Новікова Наталія. Термінологія криптовалют. Самвидав, 2018. – 23 с.
<https://www.google.com.ua/books/edition/%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F+%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2/EwJTDwAAQBAJ?hl=ru&gbpv=1&dq=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F+%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82.&printsec=frontcover>
4. Wanjala Peter. A Beginner's Journey to Ethereum's Smart Contracts. [Peter Namisiko Wanjala], 2018. – 189 p.
<https://f.eruditor.link/file/2515045/>
5. Vaneetvelde Kenny. Ethereum Projects for Beginners (code).Packt Publishing, 2018. – 92 p.
[https://www.google.com.ua/books/edition/Ethereum+Projects+for+Beginners/eWdmDwAAQBAJ?hl=ru&gbpv=1&dq=Kenny.+Ethereum+Projects+for+Beginners+\(code\).Packt+Publishing,+2018.+%E2%80%93+92+p.&printsec=frontcover](https://www.google.com.ua/books/edition/Ethereum+Projects+for+Beginners/eWdmDwAAQBAJ?hl=ru&gbpv=1&dq=Kenny.+Ethereum+Projects+for+Beginners+(code).Packt+Publishing,+2018.+%E2%80%93+92+p.&printsec=frontcover)
6. Skvorc Bruno. Learn Ethereum: The Collection. SitePoint, 2018. – 447 p.
<https://f.eruditor.link/file/2600916/>
7. 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>
8. 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>
9. 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

10. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>
11. Євсєєв С. П. Кібербезпека: основи кодування та криптографії/ С. П. Євсєєв, О. В. Мілов, С. Е. Остапов, О. В. Северінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
12. Агєєв А. І. Криптовалюти, ринки та інститути / А. І. Агєєв, Є. Л. Логінов // Економічні стратегії. - 2018. - № 1. - С. 94-107.
https://www.inesnet.ru/wp-content/mag_archive/2018_01/es2018-01-094-107_Ageev_Loginov.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
0,5	0,2		0,3

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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I ,...) 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 O 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 ЄВСЄЄВ

30.08.2025



Гарант ОП

Роман КОРОЛЬОВ