Силабус курсу
БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУВАННЯ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Дисципліна циклу: вибіркова
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Наталія ЯЦКІВ
Контактна інформація	n.yatskiv@wunu.edu.ua

Опис дисципліни

Метою дисципліни «**Блокчейн: математичні проблеми та застосування**» є сформувати в здобувачів цілісне науково-практичне розуміння блокчейн-технологій як класу розподілених криптографічних протоколів, заснованих на строгих математичних моделях.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/-	Вступ до блокчейн-технологій та розподілених реєстрів	Аналізувати моделі розподілених реєстрів, їхні властивості (незмінність, прозорість, довіра без посередників) та відмінності між блокчейном і альтернативними DLT.	Поточне опитування
2/2	Криптографічні примітиви в блокчейні	Досліджувати криптографічні примітиви (хеш-функції, MAC, мерклеві дерева, випадкові біти) та обґрунтовувати їхню роль у забезпеченні цілісності й автентичності даних.	Поточне опитування
2/2	Асиметрична криптографія в блокчейні	Аналізувати застосування асиметричної криптографії (ECDSA/EdDSA, Schnorr, агреговані та мультипідписи) для керування ідентичністю й підписом транзакцій.	Поточне опитування
2/2	Алгоритми консенсусу в технології блокчейн	Оцінювати стійкість, продуктивність і допущення безпеки алгоритмів консенсусу (PoW, PoS, BFT-варіанти) в різних загрозових моделях.	Поточне опитування

2/-	Теорія складності та криптографічні задачі	Обґрунтовувати зв’язок між класами складності та криптографічними задачами (односпрямованість, колізійна стійкість, дискретний логарифм, факторизація) у контексті безпеки протоколів.	Поточне опитування
2/-	Архітектура блокчейн-мереж	Аналізувати архітектуру блокчейн-мереж (рівні P2P, мережеві протоколи, зберігання стану, індексація, ноди/ролі) та їхній вплив на масштабованість і надійність.	Поточне опитування
2/-	Тріада блокчейн: масштабованість, безпека, децентралізація	Оцінювати компроміси тріади «масштабованість – безпека – децентралізація» і обґрунтовувати вибір дизайн-рішень для різних застосувань.	Поточне опитування
2/2	Смарт-контракти та платформи	Забезпечувати коректний життєвий цикл смарт-контрактів (розробка, тестування, деплой, оновлення) на типових платформах, дотримуючись кращих практик безпеки.	Поточне опитування
2/-	Аналіз вразливостей смарт-контрактів	Досліджувати уразливості смарт-контрактів (реентрансі, переповнення, front-running, access control) та аналізувати їх інструментами аудиту й формальної верифікації.	Поточне опитування
2/-	Методи захисту блокчейн-мереж	Забезпечувати захист блокчейн-мереж шляхом застосування моделей загроз, мережевої сегментації, моніторингу, key-/wallet-менеджменту та політик реагування на інциденти.	Поточне опитування
4/2	Zero-Knowledge Proofs у блокчейні	Обґрунтовувати застосування Zero-Knowledge Proofs (zk-SNARK/zk-STARK, Bulletproofs) для приватності й масштабування, оцінюючи припущення безпеки та вимоги до довіри.	Поточне опитування
2/2	Post-Quantum криптографія для блокчейну	Оцінювати постквантові підходи (KEM/DSA, геш- та кодові схеми, решітки) для інтеграції в блокчейн, враховуючи сумісність і продуктивність.	Поточне опитування
2/2	Блокчейн та IoT / кіберфізичні системи	Аналізувати архітектурні патерни інтеграції блокчейну з IoT/КФС, забезпечуючи автентифікацію пристроїв, цілісність телеметрії та безпечні оновлення.	Поточне опитування
2/-	Перспективні напрямки розвитку блокчейну	Досліджувати перспективні напрями (Layer-2, шардінг, модульні ланцюги, DA-шари, міжланцюгові протоколи) та оцінювати їхній вплив на екосистему.	Поточне опитування
2/-	Тенденції та майбутнє безпеки блокчейну	Обґрунтовувати майбутні тенденції безпеки блокчейну (MEV-резистентність, конфіденційні обчислення, формальна специфікація протоколів).	Поточне опитування

Рекомендовані джерела інформації

1. Опорний конспект лекцій з курсу «Блокчейн: математичні проблеми та застосування» для студентів спеціальності F5 «Кібербезпека та захист інформації» /Укл.: Яцків Н.Г., Яцків В.В. – Тернопіль: Вектор, 2025. – 76 с.
2. Song, J. *Programming bitcoin: Learn how to program bitcoin from scratch*. O'Reilly Media, 2019, 321 p.
3. Liu, X., Yang, H., Li, G., Dong, H., & Wang, Z. (2021). A blockchain-based auto insurance data sharing scheme. *Wireless Communications and Mobile Computing*, Volume 2021, Article ID 3707906 https://doi.org/10.1155/2021/3707906
4. Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T., & Zhao, C. (2021). Blockchain-based efficient device authentication protocol for medical cyber-physical systems. *Security and Communication Networks*, Volume 2021, *2021*, Article ID 5580939, 13 p. https://doi.org/10.1155/2021/5580939
5. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, *23*(2), 947. https://doi.org/10.3390/s23020947
6. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain – Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, *23*(2), 947. https://doi.org/10.3390/s23020947
7. Bashir, I. Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3. Packt Publishing Ltd. 2023, 819 p.
8. Antonopoulos, A. M., & Harding, D. A. Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.", 2023.
9. Blockchain/Cryptocurrency. Режим доступу: https://asecuritysite.com/blockchain/
10. Elliptic Curve Cryptography (ECC). Режим доступу: https://asecuritysite.com/ecc/
11. Blockchain Demo. Режим доступу: https://andersbrownworth.com/blockchain/
12. REMIX. Режим доступу: https://remix.ethereum.org

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Блокчейн: математичні проблеми та застосування**» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Визначається як середнє арифметичне з оцінок отриманих на заняттях.	Модульна робота.	Оцінка за виконання та презентацію завдання тренінгу.	Оцінка за виконане завдання самостійної роботи.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)