Назва курсу	**«Криптографія в децентралізованих системах»**
Викладач (-і)	Яцків Василь Васильович
Профайл викладача (-ів)	https://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	vy(@)wunu.edu.ua
Сторінка курсу в moodle	https://moodle.wunu.edu.ua
Консультації	Очні консультації: вівторок: 14-00, ауд. 6501.Онлайн-консультації (zoom): вівторок з 15 -00 до 16-00.

1. Анотація до курсу.

Курс "Криптографія в децентралізованих системах" надає фундаментальні знання та практичні навички у сфері сучасної криптографії, що застосовується для захисту інформації у децентралізованих системах. Учасники курсу вивчатимуть ключові математичні задачі та криптографічні протоколи. Особлива увага приділяється методам забезпечення цілісності даних, безпеки протоколів згоди, а також перспективним напрямам, як-от постквантова криптографія, гомоморфне шифрування та докази з нульовим розголошенням (ZKP). Курс також розкриває переваги ZKP для підвищення конфіденційності та довіри у децентралізованих системах. Навчання орієнтоване на студентів і фахівців, які прагнуть отримати глибоке розуміння криптографії у сучасних та майбутніх інформаційних технологіях.

2. Пререквізити.

Раніше вивчені дисципліни необхідні для освоєння курсу: базовий обсяг знань з апаратного комп'ютерного, мережного та програмного забезпечення, систематичних та ґрунтовних знань із суміжних курсів «Методологія та організація наукових досліджень», «Методи оптимізаці», «Математичне моделювання та обчислювальні методи» а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

Постреквізити. Матеріал даної дисципліни може бути використаний при написанні дисертаційної роботи.

3. Мета та цілі курсу.

Метою дисципліни «Безпека та конфіденційність Інтернет-речей» є отримання знань та умінь, які необхідні для розробки та дослідження безпеки Інтернет речей.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі кібербезпеки.

СК-6. Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей.

Результати навчання:

В результаті вивчення дисципліни аспірант повинен:

ПРН-2. Знати сучасні методи проведення досліджень в галузі кібербезпеки.

ПРН-7. Вміти досліджувати проблеми кібербезпеки критичної інфраструктури.

ПРН-8. Вміти синтезувати науково обґрунтовані рішення по захисту інформації в комп'ютерних та кіберфізичних системах.

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**доктор філософії**
Спеціальність	**125 Кібербезпека та захист інформації**
Курс (рік навчання)	**перший**
Семестр	**2**
Рік викладання	**2024/2025**
Формат курсу	**Очний (offline)**
Нормативна \ вибіркова	**обов'язкова**
Загальна кількість год/ кредитів	**120/4**
Лекції, год.	**20**
Лабораторні, год	**20**
Самостійна робота, год.	**80**

5. Перелік тем

1. Вступ до криптографії та децентралізованих систем
2. Основні математичні задачі в криптографії
3. Криптографічні протоколи
4. Цілісність даних в децентралізованих системах
5. . Протоколи згоди та їх безпека у блокчейн-системах
6. Постквантова криптографія: теорія та алгоритми.
7. Постквантові криптосистеми на основі кодів
8. . Гомоморфне шифрування: теорія та застосування
9. Докази з нульовим розголошенням: концепція та застосування
10. Переваги та перспективи застосування ZKP в децентралізованих системах.

Рекомендовані джерела

Salami, Y., Khajevand, V., & Zeinali, E. (2023). Cryptographic algorithms: a review of the literature, weaknesses and open challenges. *J. Comput. Robot*, *16*(2), 46-56.

2. Aumasson, J. P. (2024). *Serious cryptography: a practical introduction to modern encryption*. No Starch Press, Inc.

3. Gancher, J., Sojakova, K., Fan, X., Shi, E., & Morrisett, G. (2023). A core calculus for equational proofs of cryptographic protocols. *Proceedings of the ACM on Programming Languages*, *7*(POPL), 866-892.

4. Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: A review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)* (pp. 146-151). IEEE.

5. Rana, S., Parast, F. K., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. *Journal of Information Security and Applications*, *78*, 103607.

6. Bashir, I. (2023). *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*. Packt Publishing Ltd.

7. Haidary Makoui, F., Gulliver, T. A., & Dakhilalian, M. (2023). A new code-based digital signature based on the McEliece cryptosystem. *IET Communications*, *17*(10), 1199-1207.

8. Agrawal, R., Ahn, J. H., Bergamaschi, F., Cammarota, R., Cheon, J. H., DM de Souza, F., & Wang, W. (2023, November). High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application. In Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (pp. 23-34).

9. Doan, T. V. T., Messai, M. L., Gavin, G., & Darmont, J. (2023). A survey on implementations of homomorphic encryption schemes. The Journal of Supercomputing, 79(13), 15098-15139.

10. The RareSkills Book of Zero Knowledge. Режим доступу: https://www.rareskills.io/zk-book

Політика оцінювання

● Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання екзамену відбувається із дозволу проректора з наукової роботи за наявності поважних причин (наприклад, лікарняний).

● Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%.

●Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Оцінка за курс визначається наступним чином:

Види оцінювання	% від остаточної оцінки
Екзамен	100

Шкала оцінювання аспірантів:

ECTS	Бали	Зміст
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом