Назва курсу	**«Оцінка складності алгоритмів шифрування»**
Викладач (-і)	Якименко Ігор Зіновійович
Профайл викладача (-ів)	https://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	jiz@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.

Даний курс розширює кругозір аспірантів в області передових підходів та методів захисту інформації шляхом проведення досліджень їх криптостійкості, розробки відповідних заходів та їх впровадження.

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 оптимізації», «Криптографічні методи захисту інформації» 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 оцінки складності алгоритмів шифрування.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК-3. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та математичні експерименти при проведенні наукових досліджень.

СК-4. Здатність інтегрувати знання з різних дисциплін, застосовувати системний підхід та враховувати нетехнічні аспекти при розв’язанні інженерних задач та проведенні досліджень.

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-3. Уміти вести дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.

ПРН-6. Вміти розв’язувати задачі синтезу та аналізу об’єктів професійної діяльності кібербезпеки.

ПРН-13. Вміти обґрунтовувати вибір методів розв’язання науково-прикладних задач та критично оцінювати отримані результати, аргументовано захищаючи прийняті рішення.

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**доктор філософії**
Спеціальність	**125 Кібербезпека**
Курс (рік навчання)	**перший**
Семестр	**2**
Рік викладання	**2023/2024**
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. Предмет математичних основ захисту інформації.
2. Машинні моделі.
3. Класи складності P і NP. Поняття односторонньої функції та його роль в криптографії.
4. Основні поняття теорії ймовірностей. Випадкові величини та їх властивості. Рівномірний, біноміальний та інші розподіли. Поняття стійкості криптосистеми.
5. Основні поняття теорії груп.
6. Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення.
7. Хеш-функції. Криптографічні властивості.
8. Факторизація цілих чисел.
9. Криптографічні системи та їх класифікація.
10. Протоколи обміну ключами та їх реалізація: Діффі-Хеллмана та Ель Гамаля.

Рекомендовані джерела

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272с.
2. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Ришковець Ю. В. Алгоритмізація та програмування. Ч. 1 : навчальний посібник / Ю. В. Ришковець, В. А. Висоцька. – Львів : "Новий Світ-2000", 2020. – 337 с.
4. Ришковець Ю. В. Алгоритмізація та програмування. Ч. 2: навчальний посібник / Ю. В. Ришковець, В. А. Висоцька. – Львів : "Новий Світ-2000", 2020. – 314 с.
5. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

6. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.

7. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.

8. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138

9. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.

10. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.

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