Назва курсу	**«Методи шифрування в системі залишкових класів»**
Викладач (-і)	Касянчук Михайло Миколайович
Профайл викладача (-ів)	http://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	**kmm@wunu.edu.ua**
Сторінка курсу в moodle	https://moodle.wunu.edu.ua
Консультації	вівторок: 13-00, ауд. 6501. Онлайн- консультації*:* у Telegram-групі курсу або ZOOM кожного дня з 14 -00 до 18-00.

1. Анотація до курсу.

Даний курс розширює кругозір студентів в галузі криптографії на основі системи залишкових класів (СЗК) для використання в сучасних кіберсистемах; принципами побудови криптографічних алгоритмів на основі СЗК, основними криптографічними стандартами та їх використання в задачах захисту інформації; основним математичним апаратом та законами криптографії на основі СЗК у професійній діяльності; програмними та апаратними засобами, які реалізують основні криптографічні алгоритми для вирішення типових задач захисту інформації.

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 «Кібербезпека інформаційних та комп'ютерних систем», „Методи оптимізації", "Оцінка складності алгоритмів шифрування", 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.

Мета курсу "Методи шифрування в системі залишкових класів" полягає у формуванні у майбутніх фахівців умінь та компетенцій для забезпечення ефективного криптографічного захисту інформації, необхідних для подальшої роботи, їх навчанні застосуванню методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК-5. Розуміння принципів функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації, а також систем управління інформаційною безпекою.

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

СК-7. Здатність використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу й синтезу результатів досліджень.

Результати навчання:

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

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

ПРН-12. Вміти самостійно проводити експериментальні дослідження в предметній області згідно обраної наукової тематики.

ПРН-16. Уміти приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**PhD**
Спеціальність	**125 Кібербезпека**
Курс (рік навчання)	**перший**
Семестр	**2**
Рік викладання	**2023/2024**
Формат курсу	**Очний (offline, online)**
Нормативна \ вибіркова	**Обов'язкова**
Загальна кількість год/ кредитів	**120/5**
Лекції, год.	**20**
Лабораторні, год	**20**
Самостійна робота, год.	**80**

5. Перелік тем

Тема 1. Основи модулярної арифметики.
Тема 2. Теоретичні основи СЗК.
Тема 3. Форми СЗК.
Тема 4. Арифметичні операції в СЗК.
Тема 5. Симетричний криптоалгоритм без зміни базисних чисел.
Тема 6. Симетричний криптоалгоритм із зміною базисних чисел.
Тема 7. Симетричні криптоалгоритми з використанням МДФ СЗК.
Тема 8. Асиметричний криптоалгоритм без зміни базисних чисел.
Тема 9. Асиметричний криптоалгоритм із зміною базисних чисел.
Тема 10. Асиметричні криптоалгоритми з використанням МДФ СЗК.

6. Рекомендовані джерела інформації

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
3. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
4. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.

5. 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.

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

7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/

8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.

9. 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.

10. 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.

11. 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.

12. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С.63-71.

13. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С.65-73.

14. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.

7. Система оцінювання та вимоги.

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
Залік	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

8. Навчальні ресурси

№	Найменування
1.	**Обладнання:** проектор, комп'ютери з доступом до мережі Інтернет.
2.	Програмне забезпечення: VSCode, PyCharm, Visual Studio 2015, Visual Studio™ 2015, Visual Studio Team System 2015.

9. Політики курсу.

Академічна доброчесність. **Дотримання академічної доброчесності студентами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.