МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

_____ Микола ДИВАК

«_____»_____ 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Методи шифрування в системі залишкових класів»

Ступінь вищої освіти (освітньо – кваліфікаційний рівень) – **доктор філософії**

Галузь знань – **12 Інформаційні технології**

Спеціальність – **125 Кібербезпека та захист інформації**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	СРС (год.)	Разом (год.)	Екз. (сем.)
Денна	1	2	20	20	80	120	2

Тернопіль – ЗУНУ
2024

Робоча програма складена на основі освітньо-наукової програми підготовки доктора філософії, галузь знань 12 - «Інформаційні технології», спеціальності: 125 “Кібербезпека та захист інформації” затвердженої Вченою радою ЗУНУ (протокол № 11 від 26 червня 2024 р.)

Робочу програму склав д.т.н., професор, професор кафедри кібербезпеки Касянчук Михайло Миколайович

Розглянуто та схвалено групою забезпечення спеціальності,
протокол № 1 від 30 серпня 2024 р.

Голова ГЗС _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи шифрування в системі залишкових класів»

Опис дисципліни «Методи шифрування в системі залишкових класів»

Дисципліна «Методи шифрування в системі залишкових класів»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 4	Галузь знань: 12 - Інформаційні технології	Вибіркова
Кількість залікових модулів	Спеціальності – 125 “Кібербезпека та захист інформації”	Рік підготовки: *Денна – 1* Семестр: *Денна – 2*
Кількість змістових модулів – 2	Ступінь вищої освіти – доктор філософії	Лекції: *Денна – 20* Практичні заняття: *Денна – 20*
Загальна кількість годин – 120		Самостійна робота: *Денна – 80*
Тижневих годин: з них аудиторних: 4		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Методи шифрування в системі залишкових класів»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Методи шифрування в системі залишкових класів» є отримання знань та умінь, які необхідні для розробки, дослідження та використання методів шифрування в системі залишкових класів (СЗК).

2.2. Завдання вивчення дисципліни:

Завдання дисципліни **«Методи шифрування в системі залишкових класів»** дати студентам теоретичну та практичну підготовку для розробки, дослідження та використання методів шифрування в СЗК.

2.3 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.

2.4. Результати навчання

В результаті вивчення дисципліни аспірант повинен:

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.

3. Зміст дисципліни «Методи шифрування в системі залишкових класів»

Змістовий модуль 1. Теоретичні основи СЗК та її форм.

Тема 1. Основи модулярної арифметики.

Ділення з остачею. Алгоритм Евкліда, його наслідок. Порівняння. Конгруенції. Властивості конгруенцій. Система лишків. Пошук оберненого елемента. Функція Ейлера. Теореми Ейлера та Ферма.

Література: 1, 2, 4.

Тема 2. Теоретичні основи СЗК.

Переведення чисел з позиційної системи числення в СЗК. Відновлення позиційного представлення числа із СЗК. Китайська теорема про залишки. Алгоритм Гарнера. Метод додавання добутку модулів.

Література: 1, 2, 3.

Тема 3. Форми СЗК.

Звичайна цілочисельна форма СЗК. Розмежована форма СЗК. Нормалізована форма СЗК. Досконала (ДФ) та модифікована досконала форми (МДФ) СЗК. Методи побудови ДФ та МДФ СЗК.

Література: 1, 2, 5.

Тема 4. Арифметичні операції в СЗК.

Додавання та віднімання в СЗК. Множення в СЗК. Піднесення до степеня в СЗК. Арифметичні операції в різних формах СЗК.

Література: 1, 2, 10.

Змістовий модуль 2. Симетричні криптоалгоритми в СЗК.

Тема 5. Симетричний криптоалгоритм без зміни базисних чисел.

Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 2, 6.

Тема 6. Симетричний криптоалгоритм із зміною базисних чисел.

Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 4, 9.

Тема 7. Симетричні криптоалгоритми з використанням МДФ СЗК.

Побудова МДФ СЗК. Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 2, 9, 10.

Змістовий модуль 3. Асиметричні криптоалгоритми в СЗК.

Тема 8. Асиметричний криптоалгоритм без зміни базисних чисел.

Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 2, 4.

Тема 9. Асиметричний криптоалгоритм із зміною базисних чисел.

Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 2, 5

Тема 10. Асиметричні криптоалгоритми з використанням МДФ СЗК.

Побудова МДФ СЗК. Генерація ключів. Формула шифрування. Формула розшифровування. Приклад використання. Коректність, стійкість та надійність алгоритму.

Література: 1, 2, 8.

4. Структура залікового кредиту з дисципліни «Методи шифрування в системі залишкових класів»

	Кількість годин	
	Лекції	Практичні заняття
Змістовий модуль 1. ***Теоретичні основи СЗК та її форм***		
Тема 1. Основи модулярної арифметики	2	
Тема 2. Теоретичні основи СЗК	2	2
Тема 3. Форми СЗК	2	2
Тема 4. Арифметичні операції в СЗК	2	2
Змістовий модуль 2. Симетричні криптоалгоритми в СЗК		
Тема 5. Симетричний криптоалгоритм без зміни базисних чисел	2	2
Тема 6. Симетричний криптоалгоритм із зміною базисних чисел	2	4
Змістовий модуль 2. Апаратні та програні вразливості		
Тема 7. Симетричні криптоалгоритми з використанням МДФ СЗК	2	2
Змістовий модуль 3. Асиметричні криптоалгоритми в СЗК		
Тема 8. Асиметричний криптоалгоритм без зміни базисних чисел.	2	2
Тема 9. Асиметричний криптоалгоритм із зміною базисних чисел	2	2
Тема 10. Асиметричні криптоалгоритми з використанням МДФ СЗК	2	2
Разом	20	20

5. Тематика практичних (семінарських або лабораторних) занять

Практичне заняття №1

Тема: Основи модулярної арифметики.

Мета: вивчення та дослідження основ медулярної арифметики.

Питання для обговорення:

1. Ділення з остачею. Алгоритм Евкліда, його наслідок.

2. Порівняння. Конгруенції.

3. Властивості конгруенцій. Система лишків.

4. Пошук оберненого елемента.

5. Функція Ейлера. Теореми Ейлера та Ферма..
Література: 1-11.

Практичне заняття №2
Тема: Теоретичні основи СЗК.
Мета: Вивчення та дослідження теоретичних основ СЗК
Питання для обговорення:
1. Переведення чисел з позиційної системи числення в СЗК.
2. Відновлення позиційного представлення числа із СЗК.
3. Китайська теорема про залишки.
4. Алгоритм Гарнера.
5. Метод додавання добутку модулів

Література: 1-11.

Практичне заняття №3
Тема: Форми СЗК.
Мета: Вивчення та дослідження різних форм СЗК.
Питання для обговорення:
1. Звичайна цілочисельна форма СЗК.
2. Розмежована форма СЗК.
3. Нормалізована форма СЗК.
4. Досконала (ДФ) та модифікована досконала форми (МДФ) СЗК.
5. Методи побудови ДФ та МДФ СЗК.

Література: 1-11.

Практичне заняття №4
Тема: Арифметичні операції в СЗК.
Мета: вивчення та дослідження методів виконання арифметичних операцій в СЗК.
Питання для обговорення:
1. Додавання та віднімання в СЗК.
2. Множення в СЗК.
3. Піднесення до степеня в СЗК.
4. Арифметичні операції в різних формах СЗК

Література: 1-11.

Практичне заняття №5
Тема: Симетричний криптоалгоритм без зміни базисних чисел.
Мета: Вивчення та дослідження симетричного криптоалгоритму без зміни базисних чисел.
Питання для обговорення:
1. Генерація ключів.
2. Формула шифрування.

3. Формула розшифровування.
4. Приклад використання.
5. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

Практичне заняття №6

Тема: Симетричний криптоалгоритм із зміною базисних чисел.

Мета: Вивчення та дослідження симетричного криптоалгоритму із зміною базисних чисел.

Питання для обговорення:

1. Генерація ключів.
2. Формула шифрування.
3. Формула розшифровування.
4. Приклад використання.
5. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

Практичне заняття №7

Тема: Симетричні криптоалгоритми з використанням МДФ СЗК.

Мета: Вивчення та дослідження симетричних криптоалгоритмів із використанням МДФ СЗК.

Питання для обговорення:

1. Побудова МДФ СЗК.
2. Генерація ключів.
3. Формула шифрування.
4. Формула розшифровування.
5. Приклад використання.
6. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

Практичне заняття №8

Тема: Асиметричний криптоалгоритм без зміни базисних чисел.

Мета: Вивчення та дослідження асиметричного криптоалгоритму без зміни базисних чисел.

Питання для обговорення:

1. Генерація ключів.
2. Формула шифрування.
3. Формула розшифровування.
4. Приклад використання.
5. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

Практичне заняття №9

Тема: Асиметричний криптоалгоритм із зміною базисних чисел.

Мета: Вивчення та дослідження асиметричного криптоалгоритму із зміною базисних чисел.

Питання для обговорення:

1. Генерація ключів.
2. Формула шифрування.
3. Формула розшифровування.
4. Приклад використання.
5. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

Практичне заняття №10

Тема: Асиметричні криптоалгоритми з використанням МДФ СЗК.

Мета: Вивчення та дослідження асиметричних криптоалгоритмів із використанням МДФ СЗК.

Питання для обговорення:

1. Побудова МДФ СЗК.
2. Генерація ключів.
3. Формула шифрування.
4. Формула розшифровування.
5. Приклад використання.
6. Коректність, стійкість та надійність алгоритму.

Література: 1-11.

6. Самостійна робота

№ п/п	Тематика	К-сть годин
1	Напрями підвищення ефективності використання СЗК	4
2	Перспективи використання різних форм СЗК	4
3	Методи аналітичного пошуку коефіцієнтів базисних чисел.	4
4	Побудова ДФ СЗК на основі дробових перетворень	4
5	Узагальнення методу дробових перетворень	4
6	Побудова ДФ СЗК методом факторизації	4
7	Застосування ДФ СЗК у КТЗ	5
8	Побудова МДФ СЗК методом перемноження модулів	4
9	Побудова МДФ СЗК методом факторизації	5
10	Побудова МДФ СЗК на основі теореми Вієта	4
11	Побудова МДФ СЗК на основі розв’язку систем конгруенцій	4

12	Побудова МДФ СЗК на основі послідовності Фібоначчі	4
13	Побудова МДФ СЗК для багато розрядних чисел	5
14	Апаратна реалізація методів побудови ДФ СЗК	4
15	Програмна реалізація методів побудови ДФ СЗК	5
16	Апаратна реалізація методів побудови МДФ СЗК	4
17	Програмна реалізація методів побудови МДФ СЗК	4
18	Побудова трьохмодульного криптоалгоритму Рабіна	4
19	Побудова трьохмодульного криптоалгоритму Рабіна на основі МДФ СЗК.	4
Разом:		**80**

7. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни **«Методи шифрування в системі залишкових класів»** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- оцінювання виконання практичних завдань;
- презентації та виступи на наукових заходах;
- інші види індивідуальних та групових завдань;
- залікове модульне тестування та опитування.

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)

8. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**

1.	Мультимедійний проектор	1 - 10
2.	Комп’ютерна лабораторія. Доступ до Інтернету.	1 - 10

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128p.
4. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
5. 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/
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.