КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
Кафедра прикладної статистики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____Людмила ОМЕЛЬЧУК
«___»_____20__ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Проблеми криптографії, оптимізації та аналізу ризиків»
Модуль 1. «Симетрична криптографія»

для студентів

галузь знань	**12 «Інформаційні технології»**
спеціальність	**124 «Системний аналіз»**
освітній рівень	**бакалавр**
освітня програма	«**Системний аналіз»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2024/2025**
Семестр	**7**
Кількість кредитів ECTS	1
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладач: доцент, канд. фіз.-мат. наук Михайло ШАРАПОВ

Пролонговано: на 20__/20__ н.р. _____(_____) «__»____20__р.

на 20__/20__ н.р. _____(_____) «__»____20__р.

КИЇВ – 2025

Розробник: Савчук Михайло Миколайович, член-кор. НАН України, доктор фіз.-мат. наук, професор кафедри Прикладної Статистики

ЗАТВЕРДЖЕНО
Зав. кафедри Прикладної Статистики

_____ (Ірина РОЗОРА)

Протокол № __ від «__» _____ 20___ р.

Схвалено. Гарант освітньо-професійної програми першого рівня вищої освіти "Системний аналіз" _____ Михайло ШАРАПОВ

Протокол від «____» _____ 20___ року №___

Голова науково-методичної комісії _____ Тетяна КАРНАУХ

(підпис)

1 Мета дисципліни – одержання студентами базових знань з класичної криптографії, криптоаналізу класичних шифрів, теорії Шеннона зв'язку в секретних системах – як основи теоретичної криптографії, вивчення алгоритмів симетричного шифрування та методів і схем побудови сучасних симетричних криптосистем.

2 Попередні вимоги до опанування або вибору навчальної дисципліни

знати: базові поняття математичного аналізу, дискретної математики, лінійної та загальної алгебри, теорії чисел, теорії ймовірностей, математичної теорії інформації, теорії алгоритмів, теорії складності обчислень.

вміти: вміти розробляти математичні моделі інформаційних процесів та алгоритмів.

володіти елементарними навичками: розв'язування задач дискретної математики, математичного аналізу, теорії ймовірностей та математичної статистики, лінійної алгебри, теорії інформації та кодування, теорії чисел, теорії скінченних полів.

3 Анотація навчальної дисципліни

Дисципліна «Симетрична криптографія» є складовою частиною циклу професійної підготовки фахівців за першим (бакалаврським) освітньо-кваліфікаційним рівнем галузі знань 12 Інформаційні технології за спеціальністю 124 «Системний аналіз» освітньо-професійної програми «Системний аналіз»; вона включає вивчення основних понять криптології, принципів роботи криптографічних систем, математичних моделей джерел інформації, понять стійкості, теоретичної та практичної секретності, включає вивчення класичних шифрів та сучасних симетричних систем блокового та потокового шифрування.

Викладається у 7-му семестрі, обсяг 16 год. (1 кредит ECTS), з них лекції – 16 год., консультацій – 1, самостійна робота – 13 год. Передбачено залік.

4 Завдання (навчальні цілі)

Набуття знань, умінь та навичок (компетентностей) відповідно до освітньої кваліфікації бакалавра з системного аналізу. Зокрема, розвивати:

- **СК2**. Здатність формалізувати проблеми, описані природною мовою, у тому числі за допомогою математичних методів, застосовувати загальні підходи до математичного моделювання конкретних процесів
- **СК8**. Здатність організовувати роботу з аналізу та проектування складних систем, створення відповідних інформаційних технологій та програмного забезпечення.
- **СК13.2**. Здатність проводити аналітично обґрунтоване планування експериментів і спостережень, здійснювати статистичний аналіз отриманих результатів та коректно їх інтерпретувати.

5 Результати навчання за дисципліною

Результат навчання (РН) **(1 – знати; 2 – вміти; 3. комунікація; 4. автономність та відповідальність)**		**Форми викладання та навчання**	**Методи оцінювання**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН.1	Знати і розуміти методи і способи криптографічного захисту інформації, основні криптографічні алгоритми і стандарти симетричного шифрування	Лекції, практичні, самостійна робота	Поточне оцінювання (ПО), контрольна робота	45
РН.2	Вміти проводити криптоаналіз та			

	оцінювати стійкість симетричних систем криптографічного захисту інформації		1,2залік	
РН.3	Виявляти здатність до самонавчання та продовження професійного розвитку	Самостійна робота	ПО	45
РН.3.1	Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу	Самостійна робота	ПО	5
РН.4	Демонструвати навички взаємодії з іншими людьми, уміння працювати в командах	Самостійна робота	ПО	5

6 Співвідношення результатів навчання дисципліни з програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН.1**	**РН.2**	**РН.3**	**РН.3.1**	**РН.4**
(з опису освітньої програми)					
ПРН01. Знати і вміти застосовувати на практиці диференціальне та інтегральне числення, ряди та інтеграл Фур'є, аналітичну геометрію, лінійну алгебру та векторний аналіз, функціональний аналіз та дискретну математику в обсязі, необхідному для вирішення типових завдань системного аналізу.	+	+			
ПРН05. Знати основні положення теорії метричних просторів, лебегівської теорії міри та інтеграла, теорії обмежених лінійних операторів в банахових та гільбертових просторах, застосовувати техніку і методи функціонального аналізу для розв'язання задач керування складними процесами в умовах невизначеності.	+	+			
ПРНСАПР2. Вміти розробляти алгоритмічне забезпечення для систем підтримки прийняття рішень та розв'язання задач системного аналізу.	+	+			
ПРНСАПР3. Вміти проектувати, реалізовувати, тестувати, впроваджувати, супроводжувати та експлуатувати програмне забезпечення комп'ютерних систем і мереж обробки даних і знань.			+	+	+

7 Схема формування оцінки

7.1 Форми оцінювання студентів:

- семестрове оцінювання:

1. Контрольна робота 1 (РН.1, РН.2): 40/24 балів
2. Поточне оцінювання (РН.1, РН.2 РН..3, РН.3.1, РН.4): 60/36 балів

- підсумкове оцінювання (у формі заліку):

Залікові бали визначаються як сума оцінок/балів за всіма успішно оціненими результатами навчання передбачених даною програмою. - Оцінки нижче від мінімального порогового рівня не додаються. - Мінімальний пороговий рівень для сумарної оцінки за всіма компонентами становить 60% від максимально можливої кількості балів.

7.2. Організація оцінювання.

Терміни проведення форм оцінювання:
1. Контрольна робота 1: після лекції №8.

7.3. Шкала відповідності оцінок

Зараховано / Passed	60-100
Не зараховано / Fail	0-59

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№ п/п	Назва лекції	Кількість годин		
		лекції	практичні	С/Р
	Частина 1 **Основи класичної криптографії. Основні поняття криптології. Теорія секретних систем Шеннона.**			
1	Задачі, напрямки та методи захисту інформації. Поняття про криптографічний захист інформації**.** Етапи історичного розвитку методів та способів криптографічного захисту інформації.	2		2
2	Класичні шифри: шифри перестановки, комбіновані шифри перестановки.	2		2
3	Класичні шифри: моноалфавітні підстановки і блокові шифри. Частотний криптоаналіз.	2		2
4	Класичні шифри поліалфавітної підстановки. Шифр Віженера та його криптоаналіз. Аперіодичні і потокові шифри.	2		2
5	Основні поняття математичної теорії інформації. Моделі джерел відкритого тексту. Ентропія і надлишковість на символ джерела.	2		1
6	Типи атак на криптосистеми. Поняття криптографічної стійкості. Теорія секретних систем Шеннона. Принципи Шеннона побудови практично стійких шифрів.	2		2
7	Криптографічні властивості булевих функцій. Стандарти блокового шифрування DES, ГОСТ28147-89 та AES.	2		1
8	Принципи потокового шифрування. Регістри зсуву з лінійним зворотним зв'язком. Сучасні потокові шифри, побудовані на регістрах зсуву.	1		1
9	*Контрольна робота.*	1		
	ВСЬОГО	**16**		**13**

Загальний обсяг 17 *год.*
Лекції **–16** *год.*
Консультація - 1
Самостійна робота **– 13** *год.*

Перелік питань для підготовки до контрольних заходів

1. Цілі, напрямки, методи і аспекти захисту інформації. Криптологія. Задачі криптографії та криптоаналізу. Початкові поняття криптології та етапи розвитку.
2. Етапи розвитку методів і способів криптографічного захисту інформації. Класифікація криптосистем і напрямків криптографії.
3. Класична криптографія: терміни, поняття, позначення, типи шифрів. Визначення шифру загальної перестановки, блокової перестановки.
4. Класичні шифри перестановки: Скітала, частоколу, табличні перестановки, грати Кардано, магічні квадрати.
5. Визначення шифру підстановки, типи шифрів заміни. Моноалфавітні підстановки: визначення, загальний шифр простої підстановки. Шифри класичної криптографії: Цезаря, афінної заміни, шифр Полібія, тюремний, книжковий шифр. Частотний криптоаналіз.
6. Блокові підстановки: шифр Плейфера, афінна біграмна та l-грамна заміна, шифр Хілла.
7. Визначення поліалфавітної підстановки. Класичні шифри: Цезаря, Віженера, шифр з автоключем.
8. Аперіодичні шифри: книжковий шифр з бігучим рядком, шифр Вернама (одноразовий блокнот). Модульне шифрування, порівняння з потоковими шифрами.
9. Поняття ентропії, властивості ентропії, сумісна, умовної ентропія, взаємна інформація.
10. Джерела дискретних сигналів, моделі відкритого тексту. Ентропія на символ джерела, надлишковість.
11. Правило Керкгоффса. Ієрархія типів атак на криптосистему за рівнем доступної криптоаналітику інформації.
12. Основні поняття криптографії та криптоаналізу. Поняття стійкості, теоретична і практична стійкість за Шенноном. Загальна схема секретного зв'язку. Математична модель Шеннона симетричного шифру.
13. Цілком таємна криптосистема. Необхідні і достатні умови цілковита таємності. Цілковита таємність шифру Вернама.
14. Межа Шеннона для цілком таємного шифру. Функція ненадійності ключа і відстань однозначності.
15. Принципи Шеннона: розсіювання і перемішування. Підхід до побудови стійких криптосистем, запропонований Шенноном.
16. Криптографічні властивості булевих функцій. Невиродженість, збалансованість, лавинний ефект, кореляційний імунітет, нелінійність, відсутність заборон, згладжування.
17. Симетричні блокові шифри. Стандарт шифрування DES: схема роботи, характеристики, недоліки. Модифікації алгоритму DES.
18. Стандарт шифрування ДСТУ ГОСТ 28147:2009: схема роботи, характеристики.
19. Стандарти шифрування AES**,** ДСТУ 7624:2014 «Калина». Основні характеристики.
20. Принципи потокового шифрування. Регістри зсуву з лінійним зворотним зв’язком.
21. Внесення нелінійності у схеми на основі регістрів зсуву із лінійним зворотним зв’язком.
22. Потокові шифри побудовані на регістрах зсуву: A5/1, SNOW 2.0, Національний стандарт потокового шифрування ДСТУ 8845:2019 – шифр «Струмок».

9. Рекомендовані джерела

1. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.

2. Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я. Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.
3. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
4. Задірака В.К., Олексюк О.С. Комп"ютернакриптологія. – К.: 2002. – 504 с.
5. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформациию. – К.: Вища щкола, 2002. – 457 с.
6. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека. Термінологічний навчальний довідник. – К.: 2004. – 508 с.
7. Alfred Menezes A., Paul van Oorschot, Scoot Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.