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

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
Кашпур О.Ф.
«28» 08 2020 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	**2022/2023**
Семестр	**7**
Кількість кредитів ECTS	**2,5**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: **член-кор. НАН України, доктор фіз.-мат.наук Савчук М.М.**

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

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

КИЇВ – 2020

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

ЗАТВЕРДЖЕНО
Завідувач кафедри Прикладної Статистики

_____ (Лебєдєв Є.О.)

Протокол № 1 від «27» серпня 2020 р.

Схвалено Гарантом освітньо-професійної програми першого рівня вищої освіти

«Системний аналіз» _____ М.М. Шарапов

«28» серпня 2020 року

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від «28» серпня 2020 року №1

Голова науково-методичної комісії _____ **(Омельчук Л.Л.)**
(підпис) (прізвище та ініціали)

«28» серпня 2020 року

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: програмувати на мові високого рівня, 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, теоріі 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 28 год. (2,5 кредити ECTS), з них лекції – 28 год.., самостійна робота – 47 год. Передбачено 2 змістовні частини та залік.

4 Завдання (навчальні цілі)

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

- **К18.** Здатність формалізувати проблеми, описані природною мовою, у тому числі за допомогою математичних методів, застосовувати загальні підходи до математичного моделювання конкретних процесів, в тому числі, в інформаційних системах.
- **К24.** Здатність організовувати роботу з аналізу та проектування складних систем, створення відповідних інформаційних технологій та програмного забезпечення.
- **ФКСАС 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, самостійна робота	Поточне оцінювання (ПО), контрольна	45

РН.2	Вміти проводити криптоаналіз та оцінювати стійкість симетричних систем криптографічного захисту інформації		робота 1,2 залік	
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)					
ПР01. Знати і вміти застосовувати на практиці диференціальне та інтегральне числення, ряди та інтеграл Фурьє, аналітичну геометрію, лінійну алгебру та векторний аналіз, функціональний аналіз та дискретну математику в обсязі, необхідному для вирішення типових завдань системного аналізу.	+	+			
ПР05. 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.	+	+			
ПРСАС 2. Застосовувати вивчені методи системного і статистичного аналізу, обробки даних та імітаційного моделювання.	**+**	**+**			
ПРСАС 3. Знати алгоритми і коректно застосовувати на практиці методи прогнозування.			+	+	+

7 Схема формування оцінки

7.1 Форми оцінювання студентів:

- семестрове оцінювання:

1. Контрольна робота 1 (РН.1, РН.2): 40/24 балів
2. Контрольна робота 2 (РН.1, РН.2): 40/24 балів
3. Поточне оцінювання (РН.1, РН.2 РН..3, РН.3.1, РН.4): 20/12 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 №7.
2. Контрольна робота 2: після лекції №14.

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	семінари	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		3
2	Основні поняття математичної теорії інформації. Моделі джерел відкритого тексту, ентропія на символ джерела.	2		3
3	Класичні шифри: моноалфавітні підстановки, методи криптоаналізу.	2		*3*
4	Класичні шифри: поліалфавітні підстановки, шифр Віженера та його криптоаналіз.	2		3
5	Класичні шифри: шифри перестановки. Комбіновані шифри. Загальна класифікація шифрів.	2		3
6	Основні поняття криптології. Загальна схема таємного зв'язку. Математична модель шифру в теорії секретних систем Шеннона.	2		3
7	Теоретична та практична секретність. Цілком таємні криптосистеми за Шенноном. Ненадійність ключа і відкритого тексту. Відстань однозначності. Принципи Шеннона для побудови стійких криптосистем.	1		4
	Контрольна робота 1	1		2
	Частина 2 **Криптографічні властивості булевих функцій. Сучасні системи блокового і потокового шифрування**			
8	Булеві функції та способи їх зображення. Складність булевих функцій.	2		2
9	Класи і криптографічні властивості булевих функцій.	2		*3*
10	Принципи побудови сучасних блокових систем шифрування. Схема Фейстела. Стандарт блокового шифрування DES.	2		2
11	ДСТУ ГОСТ 28147-89 та інші шифри фейстелівської схеми. Режими використання блокових шифрів.	2		3
12	Алгоритм блокового шифрування Rijndael. Стандарт	2		4

	блокового шифрування України «Калина».			
13	Потокові системи шифрування. Регістри зсуву з лінійним зворотним зв’язком.	2		4
14	Приклади сучасних потокових шифрів: A5/1, LILI 128, RC4.	1		3
	Контрольна робота	1		2
	ВСЬОГО	**28**		**47**

Загальний обсяг **75** *год.*[1], в тому числі:
Лекцій **–28** *год.*
Самостійна робота **– 47** *год.*

Перелік питань для підготовки до контрольних робіт

1. Цілі, напрямки, методи і аспекти захисту інформації. Криптологія. Задачі криптографії та криптоаналізу. Початкові поняття криптології та етапи розвитку.
2. Класична криптографія: терміни, поняття, позначення, типи шифрів. Визначення шифру загальної перестановки.
3. Класичні шифри перестановки: Скітала, частоколу, табличні перестановки, грати Кардано, магічні квадрати.
4. 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.
5. Табличні підстановки: шифр Плейфера, афінна біграмна заміна, шифр Хілла.
6. Визначення поліалфавітної підстановки. Модульне шифрування, порівняння з потоковими шифрами. Класичні шифри: Цезаря, Віженера, шифр з автоключем, книжковий шифр з бігучим рядком, шифр Вернама (одноразовий блокнот).
7. Правило Керкгоффса. Ієрархія типів атак на криптосистему за рівнем доступної криптоаналітику інформації. Підходи до криптоаналізу класичних шифрів.
8. Поняття ентропії, властивості ентропії, сумісна та умовної ентропія, взаємна інформація. Джерела дискретних сигналів, ентропія на символ джерела, надлишковість.
9. Основні поняття криптографії та криптоаналізу. Поняття стійкості, теоретична і практична стійкість за Шенноном. Загальна схема секретного зв'язку. Математична модель Шеннона симетричного шифру.
10. Цілком таємна криптосистема. Необхідні і достатні умови цілковита таємності. Межа Шеннона. Цілковита таємність шифру Вернама.
11. Функція ненадійності ВТ і ключа. Відстань однозначності: визначення, доведення формули, інтерпретація, застосування. Принципи Шеннона: розсіювання і перемішування. Підхід до побудови стійких криптосистем, запропонований Шенноном. Класифікація класичних і сучасних криптосистем.
12. Одновимірні та багатовимірні булеві функції. Способи представлення булевих функцій: таблиця істинності, поліном Жегалкіна (АНФ) та алгебраїчний степінь булевої функції.
13. Спектральні представлення булевих функцій: розклад Фур’є та коефіцієнти Уолша.
14. Криптографічні властивості булевих функцій. Невиродженість, відсутність заборон, збалансованість, згладжування.
15. Кореляційний імунітет булевих функцій: різні визначення, зв’язок із коефіцієнтами Уолша Лавинні ефекти булевих функцій.
16. Симетричні блокові шифри: визначення, загальні властивості. Принципи побудови сучасних блокових шифрів. Схема Фейстеля, властивості.

17. Стандарт шифрування DES: схема роботи, характеристики, недоліки. Модифікації алгоритму DES.
18. Стандарт шифрування ДСТУ ГОСТ 28147:2009: схема роботи, характеристики.
19. Стандарт шифрування AES: схема роботи, структура, характеристики. Стандарт шифрування ДСТУ 7624:2014 «Калина». Основні характеристики.
20. Режими роботи блокових шифрів, основні характеристики. Вплив спотворень у шифротекстах на відкриті тексти у різних режимах роботи.
21. Потокові шифри: визначення, загальна модель. Типи генераторів гами. Внесення нелінійності у схеми на основі регістрів зсуву із лінійним зворотним зв'язком.
22. Потокові шифри A5/1, A5/2. Потоковий шифр RC4. Конкурс eSTREAM.

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"ютерна криптологія. – 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. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. - М.: Издательство ТРИУМФ, 2003. - 816 с.
8. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. - М.: Мир, 2006. – 471с.
9. Menezes A., P. van Oorschot, S.Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.