НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
02 червня 2025 р

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи криптографічного та стеганографічного захисту інформації – частина 1»

Галузь знань _____12 Інформаційні технологі

Спеціальність ___125 Кібербезпека_____

Освітня програма _____«Кібербезпека»_____

Факультет (ННІ)_____інформаційних технологій_____

Розробники: _____доцент, к.т.н., доцент, Сагун А.В._____

(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни

Дисципліна вивчає математичні основи та алгоритми криптографічних перетворень, основні поняттями симетричної криптографії, стандарти криптографічних схем, алгоритмів та протоколів.

Розглядаються основи спеціальних розділів математики для задач криптографічного захисту інформації (модулярна арифметика, операції в числових полях тощо). Розглядаються основи побудови та використання симетричної криптографії та методів захисту інформації на основі мереж Файстеля, sp-мереж, підстановочних, перестановочних шифрів, шифрів заміни та потокових шифрів.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*125 – Кібербезпека*	
Освітня програма	*Кібербезпека*	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*залік*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	3	-
Семестр	5	-
Лекційні заняття	*30 год.*	*г*
Практичні, семінарські заняття	*год.*	*г*
Лабораторні заняття	*30 год.*	*г*
Самостійна робота	*60 год.*	*г*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*4 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни «Основи криптографічного та стеганографічного захисту інформації – частина 1» є ознайомлення з математичними основами симетричних криптографічних перетворень (модулярна арифметика, операціїі в скінченних числових полях), основними поняттями симетричної криптографії, симетричними криптопротоколами та алгоритмами блокової криптографії та потоковими шифрами.

Набуття компетентностей:

інтегральна компетентність (ІК): здатність на основі системного і логічного мислення ефективно застосовувати теоретичні знання з симетричної криптографії та математичних основ криптографії у практичних завданнях захисту інформації, використовуючи сучасні інформаційно-комунікаційні технології, моделі, методи та засоби криптографічного і технічного захисту даних, а також розробляти елементи програмного та апаратного забезпечення інформаційної безпеки.

загальні компетентності (ЗК): здатність застосовувати знання у практичних ситуаціях; здатність до абстрактного і системного мислення, аналізу та синтезу.

спеціальні (фахові) компетентності (СК): здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності; здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

Програмні результати навчання (ПРН): вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації.

2. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин**												
	денна форма							**заочна форма**					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Змістовий модуль 1. Спеціальні розділи математики в крипотографії													
Тема 1. Основні складові криптографічних систем. Задачі криптології та стеганографії в кібербезпеці.	1	4	2		-		2						
Тема 2. Поняття шифрування. Шифри, ключі. Симетричні та	2	6	2		-		4						

асиметричні шифри та їх основні параметри.													
Тема 3. Модулярна арифметика для задач криптографії. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера та Ферма. Обчислення у скінченних полях.	3	14	4		4		6						
Тема 4. Операції в кільцях. Криптоперетворення XOR-шифруванням. Гамування. Композиційні шифри. Шифр Вернама.	5	10	2		4		4						
Тема 5. Прості симетричні криптосистеми та шифри. Моно та поліалфавітні шифри (шифри Віженера/Цезаря).	6	12	2		6		6						
Тема 6. Великі числа та довга арифметика в криптографічних задачах.	8	6	2		-		4						
Разом за модулем 1		**54**	**14**		**14**		**28**						
Змістовий модуль 2. Симетричні криптосистеми та алгоритми шифрування													
Тема 7. Шифри підстановок та перестановок, заміни (квадрат Полібія). Афінні криптоперетворення.	9	12	2		4		4						
Тема 8. Симетричні блокові криптоалгоритми на базі мережі Фейстеля. Конструювання симетричних шифрів на базі мереж Фейстеля, їх теоретичниа криптостійкість.	10	14	4		4		6						
Тема 9. Шифри DES, 3-DES, ДСТУ ГОСТ 28147-2009, алгоритм RC5.	11	10	4		2		8						
Тема 10. Симетричні блочні криптосистеми на базі SP-боксів: AES, ДСТУ 7624:2014	13	14	2		2		8						
Тема 11. Потокові шифри. Математичні основи побудови потокових шифрів A5, RC4, «СТРУМОК» (примітивні незвідні поліноми). Лінійний регістр зсуву.	14	14	4		4		6						
Разом за модулем 2		**66**	**16**		**16**		**32**						
Усього годин		**120**	**30**		**30**		**60**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Лекція 1 - Основні терміни і поняття криптографії та стеганографії	2
	Лекція 2 - Поняття шифрування. Шифри, ключі. Симетричні та асиметричні	

	шифри та їх основні параметри	2
2	Лекція 3 - Спеціальні розділі математики в криптографії.	2
	Лекція 4 - Мала теорема Ферма. Теорема Ейлера. Алгоритм Евкліда. Поняття числових полів в криптографії.	4
3	Лекція 5 - Застосування модулярної арифметики в криптографії. Афінні шифри.	2
4	Лекція 6 - Прості симетричні криптосистеми: шифри Цезарі, Віженера, квадрат Полібія.	2
5	Лекція 7-Гамування. Гама шифри, XOR-шифрування	2
6	Лекція 6 - Композиційні симетричні шифри. Блочні шифри: вимоги та параметри блочних шифрів; S та P-таблиці	2
7	Лекція 7 - Симетричні блокові криптосистеми. Мережа Фейстеля.	2
8	Лекція 8 - Симетричні блочні криптосистеми. DES-шифрування. 3-DES-шифрування. Шифр ДСТУ ГОСТ 28147-2009, алгоритм RC5.	4
9	Лекція 9 - Симетричні блочні криптосистеми. AES-шифрування. Шифри ДСТУ 7624:2014. Апаратна реалізація AES-криптоперетворень	2
10	Лекція 8 - потокові шифри. Математичні основи побудови потокових шифрів A5, RC4, «СТРУМОК» (примітивні незвідні поліноми). Лінійний регістр зсуву.	4

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Лабораторна робота 1 - Основи криптографічних перетворень. Прості шифри перестановки та заміни	
2	Лабораторна робота 2 - Теорія чисел та її прикладне застосування в криптографії. Модулярна арифметика та числові поля, теорія лишків, конгруентності.	
3	Лабораторна робота 2 - Теорія чисел та її прикладне застосування в криптографії. Теорема Ферма, алгоритм Евкліда.	
4	Лабораторна робота 4 - Симетричні криптосистеми. Шифри гамування. Композиційні шифри	
5	Лабораторна робота 5 - Симетричні криптосистеми. Шифри на базі мереж Фейстеля. Блоковий шифр RC5	
6	Лабораторна робота 6- Шифр DES. Шифр 3-DES	
7	Лабораторна робота 7 - Симетричний криптоалгоритм AES	
8	Лабораторна робота 8 - Потокові шифри. Шифр A5. Криптоалгоритм "Струмок" ДСТУ 8845:2019	

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Обчислення в скінченних полях. Використання малої теореми Ферма в симетричній криптографії	6
2	Шифри простої заміни. Квадрат Полібія	6
3	Парний шифр	6
4	Матричне шифрування	4
5	Нелінійні перетворення в SP-шифрах та їх характеристики	4
6	Варіації блокового шифру RC5	8
7	Абсолютно стійкі шифри. Шифр Вернама (одноразовий блокнот)	6
8	Шифри Фейстеля і Фейстель-сумісні (DES)	14

9	Створення моделі потокового шифру	6

6. Методи та засоби діагностики результатів навчання:

(вибрати необхідне чи доповнити)

- усне або письмове опитування;
- співбесіда;
- тестування;
- захист лабораторних робіт;
- пірінгове оцінювання, самооцінювання.

7. Методи навчання *(вибрати необхідне чи доповнити):*

- метод проблемного навчання;
- метод практико-орієнтованого навчання;
- метод командної роботи, мозкового штурму
- метод гейміфікованого навчання.

8. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Змістовий модуль 1. Спеціальні розділи математики в крипотографії		
Лабораторна робота 1 - Основи криптографічних перетворень. Прості шифри перестановки та заміни	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;	5
Лабораторна робота 2 - Теорія чисел та її прикладне застосування в криптографії. Модулярна арифметика та числові поля, теорія лишків, конгруентності.	знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації;	6
Лабораторна робота 2 - Теорія чисел та її прикладне застосування в криптографії. Теорема Ферма, алгоритм Евкліда.		6
Самостійна робота 1	використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій	2
Самостійна робота 2	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	2
Самостійна робота 3		2
Модульна контрольна робота 1	Контроль засвоєння матеріалу	**5**

Всього за модулем 1		**28**
Змістовий модуль 2. Симетричні криптосистеми та алгоритми шифрування		
Лабораторна робота 4 - Симетричні криптосистеми. Шифри гамування. Композиційні шифри	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	6
Лабораторна робота 5 - Симетричні криптосистеми. Шифри на базі мереж Фейстеля. Блоковий шифр RC5	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.	6
Лабораторна робота 6- Шифр DES. Шифр 3-DES		6
Лабораторна робота 7 - Симетричний криптоалгоритм AES	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;	6
Лабораторна робота 8 - Потокові шифри. Шифр А5. Криптоалгоритм "Струмок" ДСТУ 8845:2019		7
Самостійна робота 4	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень	2
Самостійна робота 5		3
Самостійна робота 6		2
Модульна контрольна робота 2	Контроль засвоєння матеріалу	**4**
Всього за модулем 2		**42**
Навчальна робота		**(М1 + М2)*0,7 ≤ 70**
Екзамен		**30**
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. Політика оцінювання

Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (пропорційно інтервалів пропущеної дати складання). Перескладання модульних контрольних та тестів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Лабораторні роботи мають бути виконані виключна за індивідуальними завданнями варіантів.

Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (хвороба, участь в заходах від кафедри або факультету, міжнародне стажування). В узгоджених офіційно випадках навчання може відбуватись індивідуально (в он-лайн формі)

9. Навчально-методичне забезпечення:

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=4163), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання лабораторних та самостійних завдань;
- модульних контрольних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної дисципліни.

10. Рекомендовані джерела інформації

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=4668), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання лабораторних та самостійних завдань;
- модульних контрольних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної дисципліни.

11.Рекомендовані джерела інформації

1. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. – К.: НПУ імені М.П. Драгоманова, 2012. – 120 с. Режим доступу: https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf

2. Основи криптографічного та стеганографічного захисту інформації. Криптографічний захист інформації: навчальний посібник. Сагун А.В., Кулініч О.М., Хайдуров В.В. – Київ : НУБіП України, 2023. – 285.