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 2»

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 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	90	
Кількість кредитів ECTS	3	
Кількість змістових модулів	2	
Курсовий проект (робота) (за наявності)	Курсовий проект	
Форма контролю	*іспит*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	3	-
Семестр	6	-
Лекційні заняття	*30 год.*	*год.*
Практичні, семінарські заняття	*год.*	*год.*
Лабораторні заняття	*30 год.*	*год.*
Самостійна робота	*30 год.*	*год.*
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 2» є ознайомлення з математичними основами асиметричних криптографічних перетворень, принципами створення та функціонування односторонніх (геш-) функцій, стандартами криптографічних асиметричних схем протоколів та алгоритмів. Вивчаються принципи роботи та конструювання стеганографічних методів та засобів захисту інформації.

Набуття компетентностей:

інтегральна компетентність (ІК): здатність застосовувати набуті знання з асиметричної криптографії у практичних ситуаціях захисту інформації, використовуючи абстрактне та системне мислення для аналізу криптографічних моделей, сучасні методи інформаційної безпеки та інформаційно-комунікаційні технології, а також проєктувати та впроваджувати апаратні, алгоритмічні й програмні компоненти систем криптографічного захисту.
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; 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. Асиметричні криптосистеми та алгоритми													
Тема 1. Асиметрична криптографія. Основні поняття та властивості асиметричних криптосхем. Теоретична та практична криптостійкість асиметричних криптоалгоритмів.	1	4	2		-		2						
Тема 2. Односторонні криптоперетворення. Геш-функції та їх параметри. Принципи конструювання геш-функцій.	2	8	2		4		2						

Тема 3. Криптосхема RSA. Реалізації RSA та алгоритму Ель Гамаля (EG).	3	10	2		4		2						
Тема 4. Асиметричні криптосистеми. Алгоритм DSA.	5	6	2		2		2						
Тема 5. Протоколи обміну ключами. Алгоритм Діфі-Хелмана та його модифікації.	6	6	2		-		4						
Тема 6. Еліптичні криві (ЕК). Математичні основи ЕК. Схеми ЕЦП на базі математичного апарату еліптичних кривих.	7	10	4		4		2						
Разом за модулем 1		**44**	**14**		**14**		**14**						
Змістовий модуль 2. Стеганографічні методи захисту інформації													
Тема 6. Розвиток і значення науки стеганографії. Основні терміни, означення в стеганографії. Задачі приховування інформації для стеганографічних перетворень.	9	6	4		-		2						
Тема 7. Стеганографічні методи приховування форматуванням тексту. Модель стеганосистеми. Вимоги до стеганосистем.	10	16	4		6		6						
Тема 8. Стеганографічні контейнери та цифрові водяні знаки (Watermark). Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації.	12	12	4		6		4						
Тема 9. Принципи дискретних перетворень аналогових сигналів в стеганографії. Приховування інформації в звукових файлах.	14	12	4		4		4						
Разом за модулем 2		**46**	**16**		**16**		**16**						
Усього годин за курс		**90**	**30**		**30**		**30**						
Курсовий проект (робота) з Основ криптографічного та стеганографічного захисту інформації – частина 2				**30**									

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Асиметрична криптографія. Основні поняття та властивості асиметричних криптосхем. Теоретична та практична криптостійкість асиметричних криптоалгоритмів.	2
2	Односторонні криптоперетворення. Геш-функції та їх параметри. Принципи	2

	конструювання геш-функцій.	
3	Криптосхема RSA. Реалізації алгоритму RSA	2
4	Асиметричні криптосистеми. Алгоритм DSA	2
5	Протоколи обміну ключами. Алгоритм Діфі-Хелмана та Ель-Гамаля (EG)	2
6	Еліптичні криві та їх застосування в схемах ЕЦП. Еліптичні криві та їх застосування в схемах ЕЦП на прикладах	4
7	Розвиток і значення науки стеганографії. Основні терміни, означення в стеганографії. Задачі приховування інформації для стеганографічних перетворень	4
8	Стеганографічні методи приховування форматуванням тексту. Модель стеганосистеми. Вимоги до стеганосистем	4
9	Стеганографічні контейнери та цифрові водяні знаки (Watermark). Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації	4
10	Принципи дискретних перетворень аналогових сигналів в стеганографії. Приховування інформації в звукових файлах.	4

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Односторонні криптоперетворення. Хеш-функції.	4
2	Реалізації алгоритму ЕЦП RSA	4
3	Асиметричні криптосистеми. Криптоалгоритм DSA	2
4	Протокол обміну ключами Діфі-Хелмана та El-Gamal	4
5	Стеганографічні методи приховування форматуванням тексту	6
6	Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації	6
7	Стеганографічне приховування інформації в звукових файлах	4

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Якість геш-функцій. Колізії в односторонніх геш-функціях	4
2	Існуючі алгоритми цифрового підпису. Умови безпечності захисту цілісності з використанням геш-функцій. RSA та DSA алгоритми	6
3	Математичні операції з еліптичними кривими.	2
4	Еліптичні криві в схемах ЕЦП в схемах DSA та RSA	6
5	Методи приховування інформації в зображеннях та відео. Поняття, функції та вимоги то стеганоконтейнера	8
6	Дискретні перетворення та їх види при вбудовуванні інформації в звукові контейнери.	4

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. Асиметричні криптосистеми та алгоритми		
Лабораторна робота 1 - Односторонні криптоперетворення. Хеш-функції.	знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації.	5
Лабораторна робота 2 - Реалізації алгоритму ЕЦП RSA	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	5
Лабораторна робота 3 - Асиметричні криптосистеми. Криптоалгоритм DSA		5
Лабораторна робота 4 - Протокол обміну ключами Діфі-Хелмана та El-Gamal		6
Самостійна робота 1 - Якість геш-функцій. Колізії в односторонніх геш-функціях	знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації.	2
Самостійна робота 2 - Існуючі алгоритми цифрового підпису. Умови безпечності захисту цілісності з використанням геш-функцій. RSA та DSA алгоритми.	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	3
Самостійна робота 3 - Математичні операції з еліптичними кривими	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	3
Самостійна робота 4 - Еліптичні криві в схемах ЕЦП в схемах DSA та RSA		3
Модульна контрольна робота 1	Контроль засвоєння матеріалу	**7**
Всього за модулем 1		**39**
Змістовий модуль 2. Стеганографічні методи захисту інформації		
Лабораторна робота 5 - Стеганографічні методи приховування форматуванням тексту	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних	6

Лабораторна робота 6 - Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації	системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;	6
Лабораторна робота 7 - Стеганографічне приховування інформації в звукових файлах		6
Самостійна робота 5 - Методи приховування інформації в зображеннях та відео. Поняття, функції та вимоги то стеганоконтейнера	знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації.	3
Самостійна робота 6 - Дискретні перетворення та їх види при вбудовуванні інформації в звукові контейнери.		3
Модульна контрольна робота 2	Контроль засвоєння матеріалу	**7**
Всього за модулем 2		**31**
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=4670), 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

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.