МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра теорії оптимальних процесів

Затверджено
На засіданні кафедри теорії оптимал
процесів факультету прикла
математики та інформатики
Львівського національного універси
імені Івана Франка
(протокол №_1_ від __18.08.2025_ р.)

Завідувач кафедри Шахно С.М.

Силабус з навчальної дисципліни
"Основи криптології та захисту інформації",
що викладається в межах ОПП
«Системний аналіз і управління. Інтелектуальний аналіз дани
першого (бакалаврського) рівня вищої освіти для здобувачів
зі спеціальності 124 – системний аналіз

Львів 2025 р.

Назва дисципліни	Основи криптології та захисту інформації
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра теорії оптимальних процесів
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 124 – системний аналіз
Викладачі дисципліни	Голуб Богдан Михайлович, доцент кафедри теорії оптимальних процесів Шунькін Юрій Валерійович, асистент кафедри теорії оптимальних процесів
Контактна інформація викладачів	bohdan.holub@lnu.edu.ua; https://ami.lnu.edu.ua/employee/holub; yuriy.shunkin@lnu.edu.ua; https://ami.lnu.edu.ua/employee/shunkin-yu-v; Головний корпус ЛНУ ім. І. Франка, каб. 269. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/osnovy-kryptolohii-124-systemnyy-analiz
Інформація про дисципліну	Дисципліна “Основи криптології та захисту інформації” є нормативною дисципліною зі спеціальності 124 – системний аналіз для освітньої програми Системний аналіз і управління. Інтелектуальний аналіз даних, яка викладається у 4-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс розроблено таким чином, щоб надати учасникам знання основних методів захисту інформації від несанкціоновоного доступу, застосування симетричних та асиметричних алгоритмів криптографії, алгоритмів генерування ключів, цифрового підпису, розподілу таємниці.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни “Основи криптології” є освоєння студентами теоретичних і практичних основ криптології, криптографії та принципів розробки програмного забезпечення для їх реалізації на робочих станціях і кластерах.
Література для вивчення дисципліни	1. Вербіцький О.В. Вступ до криптології. – Львів, ВНТА, 1998. – 248с. 2. Берегуляк І.Я. Класичні методи криптування. – Львів, в-во Львів. ун-ту, 1997. 3. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів, БаК, 2003. – 148с. 4. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с 5. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. 6. Б.М.Голуб. Системи захисту інформації. Текст лекцій. – Львів, 2025. Електронна версія. Introduction to Cryptology.docx

	7. Overview of encryption, digital signatures, and hash algorithms in .NET https://learn.microsoft.com/en-us/dotnet/standard/security/cryptographic-services
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 години лабораторних робіт. Самостійної роботи: 56 год.
Очікувані результати навчання	Після завершення цього курсу студент буде : Знати: - класичні криптологічні методи: шифр простої заміни, частотний аналіз, гомофонний шифр заміни, поліграмні шифри, поліалфавітні шифри, шифри перестановок - шифри з використанням булевої алгебри. - криптосистему DES. - математичні основи криптографії: конгруенції, кільце лишків, символ Якобі, розподіл і пошук простих чисел, псевдопрості числа. - асиметричні криптосистеми: RSA, Ель-Гамаля, Рабіна, ймовірнісні алгоритми, алгоритми на основі еліптичних кривих - генератори псевдовипадкових бітів, важкооборотні функції, геш-функції. - архітектуру та методи цифрового підпису, поняття сертифікатів, криптокласи бібліотеки .NET Framework - адміністрування ключами: обмін ключами, розподіл таємниці. - основи стеганографії Вміти: - програмно реалізовувати симетричні та асиметричні криптосистеми - використовувати навички криптоаналізу - утворювати системи цифрового підпису - реалізовувати протоколи обміну ключами та розподілу таємниці **Загальні компетентності (ІК) і фахові компетентності (К):** ІК01. Здатність розв'язувати складні задачі та практичні проблеми системного аналізу у професійній діяльності або у процесі навчання, що передбачає проведення досліджень із застосуванням теорії та методів системного аналізу, які характеризуються невизначеністю умов і вимог. К01. Здатність до абстрактного мислення, аналізу та синтезу.К22. Здатність до комп'ютерної реалізації математичних моделей реальних систем і процесів; проектувати, застосовувати і супроводжувати програмні засоби моделювання, прийняття рішень, оптимізації, обробки інформації, інтелектуального аналізу даних **Програмні результати навчання (ПРН):** ПР13. Проектувати, реалізовувати, тестувати, впроваджувати, супроводжувати, експлуатувати програмні засоби роботи з даними і знаннями в комп'ютерних системах і мережах.
Ключові слова	Криптологія, криптографія, криптоаналіз, симетричні криптосистеми, асиметричні криптосистеми, цифровий підпис.
Формат курсу	Очний, дистанційний Проведення лекцій, лабораторних робіт і консультацій.
Теми	1. Категорії інформаційної безпеки. Основні способи несанкціонованого доступу до інформації 2. Принципи дії вірусних програм та їх категорії. Антивірусні системи

<table>
<tr><td></td><td>3. Елементарна криптологія. Класичні криптологічні методи
4. Шифри з використанням булевої алгебри
5. Математичні основи криптографії.
6. Афінні шифри.
7. Арифметичні задачі та алгоритми
8. Факторизація. Розпізнавання квадратичності і добування квадратних коренів
9. Криптосистеми з відкритим ключем
10. Криптосистеми на основі еліптичних кривих та теорії ґраток
11. Основи квантових алгоритмів
12. Генератори псевдовипадкових бітів.
13. Важкооборотні функції.
14. Цифровий підпис
15. Адміністрування ключами. Розподіл таємниці
16. Модель криптографії .NET Framework</td></tr>
<tr><td>Підсумковий контроль, форма</td><td>Залік у кінці семестру</td></tr>
<tr><td>Пререквізити</td><td>Для вивчення курсу студенти потребують базових знань з
- Програмування, лінійна алгебра, математичний аналіз;</td></tr>
<tr><td>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</td><td>Презентації, лекції
Індивідуальні завдання
Групові проекти, менторство</td></tr>
<tr><td>Необхідне обладнання</td><td>Комп’ютер та Internet-доступ до хмарного середовища (Amazon/Windows Asure/Google (App Engine)).</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>Оцінювання проводиться за 100-бальною шкалою.
<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Оцінка в балах</th><th colspan="3">Оцінка за національною шкалою</th></tr>
<tr><th colspan="2">Екзамен, диференційований залік</th><th>Залік</th></tr>
<tr><td>A</td><td>90-100</td><td>5</td><td>відмінно</td><td rowspan="6">зараховано</td></tr>
<tr><td>B</td><td>81-89</td><td rowspan="2">4</td><td>дуже добре</td></tr>
<tr><td>C</td><td>71-80</td><td>добре</td></tr>
<tr><td>D</td><td>61-70</td><td rowspan="2">3</td><td>задовільно</td></tr>
<tr><td>E</td><td>51-60</td><td>достатньо</td></tr>
<tr><td>FX</td><td>21-50</td><td>2</td><td>незадовільно</td><td>не зараховано</td></tr>
<tr><td>F</td><td>0-20</td><td>2</td><td>незадовільно (без права перездачі)</td><td>не зараховано (без права перездачі)</td></tr>
</table>
Впродовж семестру студент може отримати 100 балів. З них:</td></tr>
</table>

- **за роботу на лабораторних заняттях:** максимальна кількість – 70 балів (10 програм (індивідуальні завдання) по 7 балів); для кожного завдання встановлено терміни здачі. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (кожне лабораторне заняття на 10% балів менше).
- залікова **контрольна робота**: максимальна кількість – 30 балів (3 теоретичних завдання по 10 б.).

Підсумкова максимальна кількість балів 100.

Поточне тестування та самостійна робота			Контр. робота	Залік	Сума
Індивідуальне завдання №1	...	Індивідуальне завдання №10	30		100
7	...	7			

Критерії оцінювання індивідуальних завдань:

7 балів – студент повністю виконав умови завдання, алгоритми реалізовано правильно, відповідає на всі запитання, пов'язані з тематикою завдання, проводить чіткий аналіз та порівняння отриманих результатів, пропонує інші підходи до вирішення поставленого завдання;

6 балів – студент повністю виконав умови завдання, алгоритм реалізовано правильно, на деякі запитання, пов'язані з тематикою завдання, відповідає з незначними неточностями, проводить аналіз отриманих результатів з незначними неточностями;

4-5 балів – студент виконав завдання з незначними помилками, але самостійно їх виправляє, якщо на них вкаже викладач, на деякі запитання, пов'язані з тематикою завдання, відповідає з неточностями, проводить аналіз отриманих результатів з неточностями;

3 бали – студент виконав завдання частково, алгоритм реалізовано з помилками, які частково може виправити, якщо на них вкаже викладач, на запитання відповідає з помилками, проводить аналіз отриманих результатів з помилками;

2 бали – студент виконав завдання частково, алгоритми реалізовано з помилками, які самостійно не може виправити, переважно не відповідає на запитання;

1 бал – студент виконав завдання частково з грубими помилками, які самостійно не може виправити, демонструє незнання матеріалу;

0 балів – студент не виконав завдання.

1-2 завдання: Відповідні бали цієї таблиці подвоюються.

Академічна доброчесність:

Відвідування лекцій та лабораторних завдань обов'язкове.

Жодні форми порушення академічної доброчесності не толеруються.

Питання до заліку чи екзамену.	Наведені у розділі "Теми".
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу “Основи криптології та захисту інформації”

Тиждень	Тема, план, короткі тези	Форма діяльності (заняття)	Література, ресурси в інтернеті	Завдання, год.	Термін виконання
1	**Тема 1. Категорії інформаційної безпеки. Основні способи несанкціонованого доступу до інформації**: *Категорії інформаційної безпеки. Абстрактні моделі захисту інформації. Технічний захист інформації. Слабка ланка, спам, фішинг, способи крадіжки паролів*	лекція (2 год)	[6]		
	Тема 1. Міжмережеві екрани (Firewall)	лабораторне (2 год)		Функціональність міжмережевих екранів (Firewall) (2 год.)	Під час заняття
2	**Тема 2. Принципи дії вірусних програм та їх категорії. Антивірусні системи**: *Структура віруса, симптоми зараження, шляхи проникнення, середовище існування, макровіруси, трояни, мережеві віруси. Антивіруси: монітори, сканери, евристичне сканування, ревізори, блокувальники.*	лекція (2 год)	[6,10,11]		
	Тема 2. Функціональність антивірусних програм	лабораторне (2 год)		Аналіз лабораторної антивірусної системи (2 год.)	Під час заняття
3	**Тема 3. Елементарна криптологія. Класичні криптологічні методи**: *Термінологія та позначення, історичний огляд. Шифри простої заміни, Гауса, поліграмні, поліалфавітні, перестановок. Частотний аналіз.*	лекція (2 год)	[1,6]		
	Тема 3. (Інд. Завдання №1) Розрахунок таблиць частот англійської та української абеток	лабораторне (2 год)		Розробка програми розрахунку частот	Під час заняття

				(2 год.)	
4	**Тема 4. Шифри з використанням булевої алгебри**: *Шифр одноразового блокнота, композиція шифрів, криптосистеми DES та AES. Модифікації блокових шифрів.*	лекція (2 год)	[2,6]		
	Тема 3. (Інд. Завдання №2) Програмна реалізація шифру простої заміни	лабораторне (2 год)		Програмна реалізація шифру простої заміни (2 год.)	Під час заняття
5	**Тема 5. Математичні основи криптографії**: *Термінологія. Дешифрування ітераціями. Алгоритм Евкліда. Конгруенції. Кільце лишків. Кільце матриць.* **Тема 6. Афінні шифри**: *Афінний шифр 1-го порядку. Шифри вищих порядків.*	лекція (2 год)	[1,3,6]		
	Тема 3. (Інд. Завдання №3) Дешифрування криптотексту частотним аналізом	лабораторне (2 год)		Програмна реалізація функціональності частотного криптоаналізу (2 год.)	Під час заняття
6	**Тема 7. Арифметичні задачі та алгоритми**: *Бінарний метод піднесення до степеня. Випадковий вибір. Первісні корені. Квадратичні лишки. Символ Якобі.*	лекція (2 год)	[1,6]		
	Тема 3. (Інд. Завдання №3) Дешифрування криптотексту частотним аналізом	лабораторне (2 год)		Дешифрування криптотексту частотним аналізом (2 год.)	Під час заняття
7	**Тема 7. Арифметичні задачі та алгоритми**: *Розподіл простих чисел. Тестування простоти. Ймовірносні тести Соловея-Штрассена та Міллера-Рабіна.*	лекція (2 год)	[1,6]		
	Тема 3. (Інд. Завдання №4) Програмна реалізація шифру Віженера	лабораторне (2 год)		Програмна реалізація шифру Віженера (2 год.)	Під час заняття

8	**Тема 8. Факторизація. Розпізнавання квадратичності і добування квадратних коренів**: *Добування квадратного кореня за простим модулем. Знаходження квадратичного нелишка за простим модулем. Добування квадратного кореня за модулем* $n = p \cdot q$	лекція (2 год)	[1,6]		
	Тема 4. (Інд. Завдання №5) Програмна реалізація шифру одноразового блокноту	лабораторне (2 год)		Програмна реалізація шифру одноразового блокноту (2 год.)	Під час заняття
9	**Тема 9. Криптосистеми з відкритим ключем**: *Криптосистеми RSA, Рабіна, Ель-Гамаля. Ймовірносне криптування.*	лекція (2 год)	[1,6]		
	Тема 5. (Інд. Завдання №6) Програмна реалізація розширеного алгоритму Евкліда, піднесення до степеня, вибору випадкових елементів	лабораторне (2 год)		Програмна реалізація розширеного алгоритму Евкліда, піднесення до степеня (2 год.)	Під час заняття
10	**Тема 10. Криптосистеми на основі еліптичних кривих та теорії ґраток**: *Еліптичні криві. Алгоритм Діффі-Гелмана. Ґратки. Криптосистема GGH.*	лекція (2 год)	[3,6]		
	Тема 7. (Інд. Завдання №6) Програмна реалізація розширеного алгоритму Евкліда, піднесення до степеня, вибору випадкових елементів	лабораторне (2 год)		Програмна реалізація вибору випадкових елементів (2 год.)	Під час заняття
11	**Тема 11. Основи квантових алгоритмів**: *Базові принципи. Квантові вентилі. Стан системи. Спрощений алгоритм Гровера. Алгоритм Шора.*	лекція (2 год)	[6]		
	Тема 7. (Інд. Завдання №7) Програмна реалізація алгоритму обчислення символу Якобі і тестування числа на простоту	лабораторне (2 год)		Програмна реалізація алгоритму обчислення символу Якобі (2 год.)	Під час заняття
12	**Тема 12. Генератори псевдовипадкових бітів**: *Генератори BBS, Блюма-*	лекція (2 год)	[6]		

	Мікалі. Потокове шифрування. Алгоритм Блюма-Гольдвассера.				
	Тема 7. (Інд. Завдання №7) Програмна реалізація алгоритму обчислення символу Якобі і тестування числа на простоту	лабораторне (2 год)		Програмна реалізація алгоритму Соловея-Штрассена (2 год.)	Під час заняття
13	**Тема 13. Важкооборотні функції**: *Функції RSA, Рабіна, експоненційна. Ядро важкооборотної функції. Предикат із секретом і ймовірносне криптування. Геш-функції.*	лекція (2 год)	[1,6]		
	Тема 9. (Інд. Завдання №8) Програмна реалізація криптосистеми RSA	лабораторне (2 год)		Програмна реалізація криптосистеми RSA (2 год.)	Під час заняття
14	**Тема 14. Цифровий підпис**: *Підпис у системі RSA. Загальна схема цифрового підпису. Системи цифрового підпису Ель-Гамаля, Шнорра, DSA.*	лекція (1 год)	[1,6]		
	Тема 14. (Інд. Завдання №9) Програмна реалізація цифрового підпису у системі RSA	лабораторне (2 год)		Програмна реалізація генерування цифрового підпису (2 год.)	Під час заняття
15	**Тема 15. Адміністрування ключами. Розподіл таємниці**: *Практика адміністрування ключами. Експоненційний обмін ключами. Протокол Аді Шаміра поділу таємниці.*	лекція (2 год)	[1,6]		
	Тема 14. (Інд. Завдання №9) Програмна реалізація цифрового підпису у системі RSA	лабораторне (2 год)		Програмна реалізація перевірки цифрового підпису (2 год.)	Під час заняття
16	**Тема 16. Модель криптографії .NET Framework**: *Ієрархія класів, потоко-орієнтований підхід, криптографічна конфігурація, вибір алгоритмів.*	лекція (2 год)	[6,7]		
	Тема 16. (Інд. Завдання №10) Програмна реалізація	лабораторне (2 год)		Програмна реалізація протоколу Аді	Під час заняття

	протоколу Аді Шаміра поділу таємниці			Шаміра поділу таємниці (2 год.)	