

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет
імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра дискретного аналізу та інтелектуальних систем

Затверджено

на засіданні кафедри дискретного аналізу
та інтелектуальних систем
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(протокол № 1/23 від 28 серпня 2023 р.)

Завідувач кафедри проф. Притула М. М.



Силабус навчальної дисципліни
“Дискретна математика. Частина 2”,
що викладається в межах
ОПП «Середня освіта (Інформатика)»
для здобувачів першого (бакалаврського) рівня вищої освіти
з предметної спеціальності **014.09 Середня освіта (Інформатика)**
галузі знань **01 Освіта/Педагогіка**

Львів 2023 р.

Назва дисципліни	Дискретна математика. Частина 2
Адреса викладання дисципліни	Головний корпус ЛНУ ім. Івана Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра дискретного аналізу та інтелектуальних систем
Галузь знань, шифр та назва спеціальності	Галузь знань 01 Освіта/Педагогіка Предметна спеціальність 014.09 Середня освіта (Інформатика)
Викладачі дисципліни	Щербина Юрій Миколайович, професор кафедри дискретного аналізу та інтелектуальних систем, лауреат Державної премії України в галузі науки і техніки. Прядко Ольга Ярославівна, асистент кафедри дискретного аналізу та інтелектуальних систем.
Контактна інформація викладачів	yuriy.shcherbyna@lnu.edu.ua ; https://ami.lnu.edu.ua/employee/scherbyna olha.pryadko@lnu.edu.ua ; https://ami.lnu.edu.ua/employee/priadko-2 Головний корпус ЛНУ ім. І. Франка, каб. 360. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/dyskretna-matematyka-122-komp-iuterni-nauky
Інформація про дисципліну	Курс “Дискретна математика. Частина 2” є нормативною дисципліною з освітньо-професійної програми «Середня освіта (Інформатика)» першого (бакалаврського) рівня вищої освіти з предметної спеціальності 014.09 Середня освіта (Інформатика), його викладають у 2-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Дискретна математика є теоретичною основою комп’ютерних наук. Розглядаються такі розділи: функції алгебри логіки, множини і відношення, комбінаторний аналіз, теорія графів, дерева та їхні застосування, основи теорії кодування, теорія чисел і основи криптографії, формальні мови, граматики і автомати, машини Тьюрінга. З кожного розділу розглядаються можливі застосування, в основному до проблем інформатики. В усіх розділах значна увага приділяється доведенню теорем, опису алгоритмів розв’язування дискретних задач. Висвітлюються питання обчислювальної складності.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни “Дискретна математика” є систематичне викладання засобів дискретної математики як інструментарію для подання та обробки інформації в комп’ютерах. Цілями дисципліни є вивчення дискретних математичних моделей та алгоритмів із прикладами застосувань.

<p>Література для вивчення дисципліни</p>	<p>Основна</p> <ol style="list-style-type: none"> 1. <i>Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.</i> Дискретна математика (у серії „Інформатика”). Київ: Видавнича група ВНУ, 2006, 2007. 2. <i>Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.</i> Дискретна математика (у серії „Комп’ютинг”), видання 7-ме, виправлене та доповнене Львів: Магнолія 2006 та ЛНУ ім. Івана Франка, 2023. 3. <i>Ю.М. Щербина, Н.М. Колос, О.Я. Прядко.</i> Математична логіка для комп’ютерних наук. Львів: ЛНУ ім. Івана Франка, 2023. <p>Додаткова</p> <ol style="list-style-type: none"> 4. <i>Ю.В. Капітонова, С.Л. Кривий, О.А. Лещевський, М.К. Печурін.</i> Основи дискретної математики. К.: Наукова думка, 2002. 5. <i>Kenneth H. Rosen.</i> Discrete Mathematics and Its Applications. Eighth Edition. McGraw-Hill, Inc, 2019.
	<ol style="list-style-type: none"> 6. <i>Richard Crandall, Carl Pomerance.</i> Prime Numbers. A Computational Perspective. Second Editson. Springer, 2005.
<p>Обсяг курсу</p>	<p>4 кредити ЄКТС – 120 годин. З них 32 години лекцій, 32 години лабораторних занять та 56 годин самостійної роботи</p>
<p>Очікувані результати навчання</p>	<p>Після завершення цього курсу студент буде :</p> <p>Знати:</p> <ul style="list-style-type: none"> - дерева та їх застосування в інформатиці; - відношення та їх застосування; - основні поняття теорії кодів; - основні поняття теорії чисел; - застосування теорії чисел у криптографії; - моделі обчислень. <p>Вміти:</p> <ul style="list-style-type: none"> - використовувати властивості дерев для розв’язування типових задач; - уміти здійснювати обхід кореневих дерев, формувати польський запис виразів, будувати бінарне дерево пошуку; - виявляти відношення еквівалентності й відношення часткового порядку та розв’язувати типові задачі; - застосовувати схеми алфавітного й рівномірного кодування, використовувати достатні умови однозначності декодування та властивості роздільних кодів; - будувати коди Фано і Гаффмана; - будувати коди Геммінга; - знаходити мову за породжувальною граматикою та породжувальну граматикою за мовою, розпізнавати типи граматик імов; - знаходити мову, яка розпізнається скінченним автоматом, та будувати скінченний автомат для подання регулярної мови; будувати машини Тьюрінга для елементарних прикладів.
<p>Компетентності</p>	<p>курс забезпечує набуття таких компетентностей:</p> <p>ЗК1. Здатність до абстрактного мислення, аналізу та синтезу, до застосування знань у практичних ситуаціях</p> <p>ФК1. Здатність перенесення системи наукових знань у професійну діяльність та в площину навчального предмету.</p> <p>ПК1. Здатність використовувати знання наукових фактів, концепцій, теорій, принципів і методів сучасної інформатики у практиці навчання інформатики.</p> <p>ПК2. Володіння методами інформаційного моделювання; здатність реалізовувати інформаційну модель засобами інформаційнокомунікаційних технологій; проводити комп’ютерний експеримент, інтерпретувати, аналізувати та узагальнювати його результати</p> <p>ПК6. Здатність розв’язувати задачі шкільного курсу інформатики різного рівня складності, аналізувати та оцінювати ефективність розв’язку та формувати відповідні вміння у учнів</p>

Програмні результати навчання	та програмних результатів навчання: ПРН7. Демонструє знання основ фундаментальних і прикладних наук інформатики та програмування, оперує базовими категоріями та поняттями предметної області спеціальності ПРН14. Знає та розуміє фізичні, логічні та математичні основи інформаційних технологій; пояснює та застосовує способи двійкового кодування текстової, числової, графічної, звукової та відеоінформації.
Ключові слова	Булева функція, повнота, мінімізація, відношення, алгоритм Воршалла, вибірка, розміщення, сполучення, перестановка, дискретна ймовірність, рекурентне рівняння, граф, ізоморфізм графів, найкоротший шлях у графі, алгоритм Дейкстри, алгоритм Флойда, мінімальний каркас, алгоритм Краскала, дерево, польський запис, дерево рішень, червоно- чорне дерево, подільність, просте число, конгруенція, китайська теорема про остачі, шифросистема RSA, алфавітне кодування, рівномірне кодування, код Фано, код Гаффмана, код Геммінга, формальна мова,скінченний автомат, машина Тьюрінга, алгоритмічно нерозв'язна проблема.
Формат курсу	Очний.
Теми	<ol style="list-style-type: none"> 1. Вступ у дерева. 2. Рекурсія. Застосування дерев в інформаційних технологіях. 3. Каркаси графів. Теорема Келі. Алгоритм Краскала. 4. Алфавітне й рівномірне кодування. 5. Оптимальне кодування. Код Фано. Код Гаффмана. 6. Коди, стійкі до перешкод. Необхідні й достатні умови виявлення та виправлення помилок. Коди Геммінга. 7. Подільність і модулярна арифметика. Прості числа. 8. Алгоритм Евкліда. Лінійні конгруенції. 9. Застосування конгруенцій. Класична криптографія. 10. Криптосистеми з відкритим ключем, система RSA. Криптографічні протоколи. 11. Мови й граматики. 12. Скінченні автомати. 13. Машина Тьюрінга. 14. Алгоритмічно нерозв'язні задачі. 15. Поняття про обчислювальну складність. <p style="text-align: right;"><i>Докладну схему курсу подано нижче</i></p>
Підсумковий контроль, форма	Екзамени у кінці другого семестру.
Пререквізити	Для вивчення курсу студенти потребують базові знання з математики в обсязі середньої школи, достатні для сприйняття категоріального апарату моделей і методів дискретної математики.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Індивідуальні завдання Групові проекти
Необхідне обладнання	Комп'ютер, Internet.

<p>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</p>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховують за наступним співвідношенням:</p> <ul style="list-style-type: none"> • поточне тестування: 40% семестрової оцінки; всього чотири тестування по 10 балів, максимальна кількість балів 40; • індивідуальні завдання: 10% семестрової оцінки; два завдання по 5 балів, максимальна кількість балів 10; • екзамен: 50% семестрової оцінки; максимальна кількість балів 50. <p>Підсумкова максимальна кількість балів 100.</p> <p>Академічна доброчесність: Очікується, що роботи студентів будуть їх самостійними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p>Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів, визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.</p> <p>Література. Уся література, яку студенти не зможуть знайти самостійно,</p>
	<p>буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p>Політика виставлення балів. Враховуються бали, отримані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнь на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях, не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p>
<p>Питання до екзамену.</p>	<p>Дерева, основні властивості. Кореневі дерева. Обхід дерев, польська нотація. Дерево рішень.</p> <p>Схеми алфавітного та рівномірного кодування.</p> <p>Оптимальне кодування. Код Гаффмана.</p> <p>Коди, стійкі до перешкод. Коди Геммінга.</p> <p>Модулярна арифметика.</p> <p>Найбільші спільні дільники як лінійні комбінації. Теорема Безу.</p> <p>Лінійні конгруенції.</p> <p>Китайська теорема про остачі. Мала теорема Ферма. Первісні корені та дискретні логарифми.</p> <p>Класична криптографія. Шифри зсуву і шифри заміни.</p> <p>Криптосистеми з відкритим ключем. Система RSA. Криптографічні протоколи.</p> <p>Означення та способи подання скінченного автомата з виходом.</p> <p>Автомати Мілі та Мура.</p> <p>Скінченні автомати без виходу.</p> <p>Детерміновані та недетерміновані скінченні автомати.</p> <p>Мови, які розпізнаються скінченними автоматами.</p> <p>Машини Тьюрінга. Уточнення поняття алгоритму на основі машини Тьюрінга: теза Тьюрінга.</p> <p>Алгоритмічно нерозв'язні задачі.</p>

Опитування

Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	Тема 1. Вступ у дерева. (Дерева. Основні означення та властивості)	лекція, самостійна робота	[1,2,4,5]	2 3	1 тиждень
	Тема 1. Вступ у дерева. (Дерева. Основні означення та властивості)	лаб	[1,2,4,5]	2	
2	Тема 2. Рекурсія. Застосування дерев в інформаційних технологіях. (Рекурсія. Обхід дерев. Польська нотація. Бінарне дерево пошуку. Червоно-чорне дерево. Дерево рішень. Бектрекінг)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 2. Рекурсія. Застосування дерев в інформаційних технологіях. (Рекурсія. Обхід дерев. Польська нотація. Бінарне дерево пошуку. Дерево рішень. Бектрекінг)	лаб.	[1,2,4,5]	2	
3	Тема 3. Каркаси графів. Код Прюфера. Теорема Келі. (Каркаси графів. Код Прюфера для дерев. Теорема Келі. Задача про мінімальний каркас. Алгоритм Краскала)	лекція, самостійна робота	[1,2,4,5]	2 3	1 тиждень
	Тема 3. Каркаси графів. Код Прюфера. Теорема Келі. (Каркаси графів. Код Прюфера для дерев. Теорема Келі. Задача про мінімальний каркас. Алгоритм Краскала)	лаб	[1,2,4,5]	2	
4	Тема 4. Алфавітне й рівномірне кодування. (Алфавітне й рівномірне кодування. Достатні умови однозначності декодування. Властивості роздільних кодів)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 4. Алфавітне й рівномірне кодування. (Алфавітне й рівномірне кодування. Достатні умови однозначності декодування. Властивості роздільних кодів)	лаб	[1,2,4,5]	2	
5	Тема 5. Оптимальне кодування. Код Фано. Код Гаффмана. (Код Фано – код, близький до оптимального. Код Гаффмана – оптимальний код. Приклад НЕ алфавітного кодування – стиснення даних: алгоритм Лемпеля – Зіва)	лекція, самостійна робота	[1,2,4,5]	2 3	1 тиждень
	Тема 5. Оптимальне кодування. Код Фано. Код Гаффмана. (Код Фано – код, близький до оптимального. Код Гаффмана – оптимальний код.)	лаб	[1,2,4,5]	2	
6	Тема 6. Коди, стійкі до перешкод. Коди Геммінга. (Необхідні й достатні умови виявлення та виправлення помилок. Коди Геммінга)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 6. Коди, стійкі до перешкод. Коди Геммінга. (Необхідні й достатні умови виявлення та виправлення помилок. Коди Геммінга)	лаб	[1,2,4,5]	2	

7	Тема 7. Подільність і модулярна арифметика. Прості числа. (Ділення, модулярна арифметика, арифметика за модулем m , Абелева група. Комутативне кільце з одиницею. Модулярне піднесення до степеня. Означення простого числа, властивості простих чисел. Відкриті проблеми щодо простих чисел. Пробне ділення. Решето Ератосфена)	лекція, самостійна робота	[5-6]	2 4	1 тиждень
	Тема 7. Подільність і модулярна арифметика. Прості числа. (Арифметика за модулем m , Модулярне піднесення до степеня. Пробне ділення. Решето Ератосфена)	лаб.	[5-6]	2	
8	Тема 8. Алгоритм Евкліда. Лінійні конгруенції. (Опис алгоритму Евкліда. Найбільші спільні дільники як лінійні комбінації. Розширений алгоритм Евкліда. Розв'язування лінійних конгруенцій. Китайська теорема про остачі. Мала теорема Ферма. Первісні корені й дискретні логарифми)	лекція, самостійна робота	[5-6]	2 3	1 тиждень
	Тема 8. Алгоритм Евкліда. Лінійні конгруенції. (Опис алгоритму Евкліда. Найбільші спільні дільники як лінійні комбінації. Розширений алгоритм Евкліда. Розв'язування лінійних конгруенцій. Китайська теорема про остачі. Мала теорема Ферма, приклади застосування)	лаб.	[5-6]	2	
9	Тема 9. Застосування конгруенцій. Класична криптографія. (Геш-функції. Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація	лекція, самостійна робота	[5-6]	2 4	1 тиждень
	шифросистем. Шифри перестановки Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри. Що таке шифросистема? Історична довідка)				
	Тема 9. Застосування конгруенцій. Класична криптографія. (Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація шифросистем. Шифри перестановки. Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри. Що таке шифросистема? Історична довідка)	лаб.	[5-6]	2	
10	Тема 10. Криптосистеми з відкритим ключем. Система RSA. Криптографічні протоколи. (Симетричні й асиметричні криптосистеми. Система шифрування RSA . Обґрунтування коректності системи RSA . Чому система RSA підходить для криптографії з відкритим ключем? Обмін ключем. Цифрове підписання. Довідка про сучасні симетричні криптосистеми)	лекція, самостійна робота	[1,2,4-6]	2 3	1 тиждень
	Тема 10. Криптосистеми з відкритим ключем. Система RSA. Криптографічні протоколи. (Симетричні й асиметричні криптосистеми. Система шифрування RSA . Приклади. Обмін ключем. Цифрове підписання. Приклади.)	лаб.	[1,2,4-6]	2	
	Тема 11. Мови й граматики. (Означення формальної мови. Породжувальні граматики. Типи граматик: ієрархія Хомського. Деревя виведення. Форми Бекуса – Наура)	лекція, самостійна робота	[1,2,4]	2 4	

11	Тема 11. Мови й граматики. (Означення формальної мови. Породжувальні граматики. Типи граматик: ієрархія Хомського. Дерева виведення. Форми Бекуса – Наура)	лаб.	[1,2,4]	2	1 тиждень
12	Тема 12. Скінченні автомати. (Скінченні автомати з виходом і без виходу. Подання мов скінченними автоматами. Мова чи проблема? Леми про накачування для регулярних і для контекстно вільних мов)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 12. Скінченні автомати. (Скінченні автомати з виходом і без виходу. Подання мов скінченними автоматами. Леми про накачування для регулярних і для контекстно вільних мов)	лаб.	[1,2,4,5]	2	
13	Тема 13. Машини Тьюрінга. (Основні вимоги до алгоритмів. Означення машини Тьюрінга. Обчислення числових функцій на машинах Тьюрінга)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 13. Машини Тьюрінга. (Основні вимоги до алгоритмів. Означення машини Тьюрінга. Обчислення числових функцій на машинах Тьюрінга)	лаб.	[1,2,4,5]	2	
14	Тема 14. Алгоритмічне нерозв'язні задачі. (Теза Тьюрінга. Приклади алгоритмічно нерозв'язних проблем)	лекція, самостійна робота	[1,2,4,5]	2 4	1 тиждень
	Тема 14. Алгоритмічне нерозв'язні задачі. (Теза Тьюрінга. Приклади алгоритмічно нерозв'язних проблем)	лаб.	[1,2,4,5]	2	
15- 16	Тема 15. Поняття про обчислювальну складність. (Складність алгоритмів. Поліноміальні та експоненціальні алгоритми. Класи задач P та NP . Теорема Кука. Приклади NP - повних задач)	лекція, самостійна робота	[1,2,4,5]	4 5	2 тижні
	Тема 15. Поняття про обчислювальну складність. (Поліноміальні та експоненціальні алгоритми. Класи задач P та NP . Приклади NP - повних задач)	лаб.	[1,2,4,5]	4	