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 № 24/23 від 30 серпня 2023 р.)

Завідувач кафедри Микола ПРИТУЛА

Силабус з навчальної дисципліни "Моделі та методи дискретної математики", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів зі спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Моделі та методи дискретної математики**
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра дискретного аналізу та інтелектуальних систем
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Щербина Юрій Миколайович, професор кафедри дискретного аналізу та інтелектуальних систем, лауреат Державної премії України в галузі науки і техніки. Кириченко Наталія Володимирівна, асистент кафедри дискретного аналізу та інтелектуальних систем.
Контактна інформація викладачів	yuriy.shcherbyna@lnu.edu.ua; https://ami.lnu.edu.ua/employee/scherbyna nataliia.kyrychenko@lnu.edu.ua; https://swr.abtollc.com/ReportList Головний корпус ЛНУ ім. І. Франка, каб. 360. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua
Інформація про дисципліну	Дисципліна “Моделі та методи дискретної математики” є нормативною дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 1-му семестрі першого (бакалаврського) рівня освіти в обсязі 5-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Моделі та методи дискретної математики є теоретичною основою підготовки з кібербезпеки. Розглядаються такі розділи: множини і функції, теорія чисел і основи криптографії, комбінаторний аналіз, функції алгебри логіки. З кожного розділу розглядаються можливі застосування, в основному до проблем кібербезпеки. 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 “Моделі та методи дискретної математики” є систематичне викладення 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, зокрема, у криптографії.
Література для вивчення дисципліни	Основна література: 1. *Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.* Дискретна математика (у серії „Комп’ютинг”), видання 7-ме, виправлене та доповнене Львів: Магнолія 2006 та ЛНУ ім. Івана Франка, 2023. 2. *Ю.М. Щербина, Н.М. Колос, О.Я. Прядко.* Математична логіка для комп’ютерних наук. Львів: ЛНУ ім. Івана Франка, 2023. 3. *Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В.* Кібербезпека: основи кодування та криптографії: навч. посібник. – Харків: ХПІ, 2023. – 658 с. 4. *Kenneth H. Rosen.* Discrete Mathematics and Its Applications. Eighth Edition. McGraw-Hill, Inc, 2019. – 1118 p.

	5. *Heba Al-Asady.* Introduction to Information Theory and Coding: Probability, Entropy, Channels, and Error Detection and Correction Codes. Lambert academic publ., 2019. – 136 p. <u>Додаткова література:</u> 6. *Leigh Metcalf, William Casey.* Cybersecurity and Applied Mathematics. Syngress, 2016. – 240 p. 7. *Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.* Дискретна математика (у серії „Інформатика"). Київ: Видавнича група BHV, 2006, 2007. 8. *Ю.В. Капітонова, С.Л. Кривий, О.А. Летичевський, М.К. Печурін.* Основи дискретної математики. К.: Наукова думка, 2002.
Обсяг курсу	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 години лабораторних занять. Самостійної роботи: 86 годин.
Очікувані результати навчання	Після завершення цього курсу студент буде Знати: - основні поняття теорії множин; - основні поняття класичної криптографії; - основні поняття теорії чисел; - застосування теорії чисел у криптографії; - основні поняття й методи комбінаторного аналізу; - булеві функції та їх застосування. Вміти: - розв'язувати типові задачі з множинами; - розв'язувати лінійні конгруенції; - розрізняти симетричні та асиметричні криптосистеми; - розв'язувати задачу побудови шифру RSA для невеликих простих чисел p і q. - використовувати криптографічні протоколи. - будувати кон'юнктивні, диз'юнктивні нормальні форми та поліном Жегалкіна для булевих функцій; - обчислювати кількість комбінаторних об'єктів; - розв'язувати рекурентні рівняння та застосовувати принцип коробок Діріхле й принцип включення – виключення. **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 2, КФ 3, КФ 5, КФ 10, КФ 12; та програмних результатів навчання: ПРН 2-6, ПРН 10-12, ПРН 22, ПРН 27-28, ПРН 31, ПРН 47, ПРН 48, ПРН 53.**
Ключові слова	Подільність, просте число, конгруенція, китайська теорема про остачі, шифросистема RSA, шифр зсуву, шифр заміни, вибірка, розміщення, сполучення, перестановка, дискретна ймовірність, рекурентне рівняння, булева функція, повнота, мінімізація.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.

Теми	1. Множини. Поняття відношення. 2. Відношення еквівалентності. 3. Функції. 4. Подільність і модулярна арифметика. Прості числа. 5. Алгоритм Евкліда. Лінійні конгруенції. 6. Застосування конгруенцій. Класична криптографія. 7. Класична криптографія (закінчення). 8. Криптосистеми з відкритим ключем. Криптосистема RSA. Криптографічні протоколи. 9. Основні поняття й теореми комбінаторного аналізу. 10. Генерування комбінаторних об'єктів. Дискретна ймовірність. 11. Розвинута техніка підрахунку. 12. Булеві функції. Реалізація функцій формулами. 13. Алгебри булевих функцій. 14. Повнота системи булевих функцій. 15. Мінімізація булевих функцій. 16. Поняття про схеми з функціональних елементів.
Підсумковий контроль, форма	Екзамен у кінці першого 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. Робота в групах. Групові проєкти.
Необхідне обладнання	Проектор, дошка, комп'ютер, Moodle, Internet.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • поточне тестування: 40% семестрової оцінки; максимальна кількість балів 40; • індивідуальне завдання: 10% семестрової оцінки; максимальна кількість балів 10; • екзамен: 50% семестрової оцінки; максимальна кількість балів 50. Підсумкова максимальна кількість балів 100. **Письмові роботи:** Очікується, що студенти виконають вісім письмових робіт і звіт про виконання індивідуального завдання. **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. **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. **Література.** Уся література, яку студенти не зможуть знайти самостійно, 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. **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 запізнень 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. Жодні форми порушення академічної доброчесності не толеруються.
Питання до екзамену	Множина. Кортеж. Декартів добуток множин. Поняття відношення. Модулярна арифметика. Найбільші спільні дільники як лінійні комбінації. Теорема Безу. Лінійні конгруенції. Китайська теорема про остачі. Мала теорема Ферма. Первісні корені та дискретні логарифми. Класична криптографія. Шифри зсуву і шифри заміни. Криптосистеми з відкритим ключем. Система RSA. Криптографічні протоколи. Правило суми і правило добутку в комбінаториці. Вибірка. Розміщення, перестановки, сполучення. Принцип коробок Діріхле, принцип включення-вилучення. Розв'язування рекурентних рівнянь. Означення булевої функції, алгебри булевих функцій. Теорема Поста про повноту системи булевих функції. Мінімізація булевих функцій.
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. Множини. Поняття відношення** (Поняття множини й кортежу. Декартів добуток. Булева алгебра множин. Доведення рівностей з множинами. Поняття відношення на множині)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 1. Множини. Поняття відношення. (Булева алгебра множин. Доведення рівностей з множинами. Відношення на множині)	лаб	[1, 4, 7, 8]	2	
2	**Тема 2. Відношення еквівалентності.** (Властивості бінарних відношень на множині. Відношення еквівалентності. Конгруентність за модулем *m*. Класи еквівалентності)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 2. Відношення еквівалентності. (Відношення еквівалентності. Конгруентність за модулем *m*. Класи еквівалентності)	лаб.	[1, 4, 7, 8]	2	
3	**Тема 3. Функції.** (Означення й приклади функцій, термінологія. Зростання функції. Оцінки складності алгоритмів)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 3. Функції. (Приклади функцій, термінологія. Зростання функції. Оцінки складності алгоритмів)	лаб	[1, 4, 7, 8]	2	
4	**Тема 4. 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	[3, 4, 6]	2 6	1 тиждень
	Тема 3. Подільність і модулярна арифметика. Прості числа. (Арифметика за модулем *m*, Модулярне піднесення до степеня. Пробне ділення. Решето Ератосфена)	лаб.	[3, 4, 6]	2	
5	**Тема 5. 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	[3, 4, 6]	2 6	1 тиждень
	Тема 5. Алгоритм Евкліда. Лінійні	лаб.	[3, 4, 6]	2	

	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)				
6	**Тема 6. Застосування конгруенцій. Класична криптографія.** (Геш-функції. Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація шифросистем. Шифри перестановки)	лекція, самостійна робота	[3, 4, 6]	2 6	1 тиждень
	Тема 6. Застосування конгруенцій. Класична криптографія. (Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація шифросистем. Шифри перестановки)	лаб.	[3, 4, 6]	2	
7	**Тема 7. Класична криптографія (закінчення).** (Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри. Що таке криптосистема? Історична довідка)	лекція, самостійна робота	[3, 4, 6]	2 6	1 тиждень
	Тема 7. Класична криптографія (закінчення). (Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри)	лаб.	[3, 4, 6]	2	
8	**Тема 8. Криптосистеми з відкритим ключем. 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	[3, 4, 6]	2 6	1 тиждень
	Тема 8. Криптосистеми з відкритим ключем. Криптографічні протоколи. **(**Симетричні й асиметричні криптосистеми. Система шифрування *RSA*. Приклади. Обмін ключем. Цифрове підписання. Приклади.**)**	лаб.	[3, 4, 6]	2	
9	**Тема 9. Основні правила комбінаторного аналізу. Розміщення та сполучення.** **(**Правило суми та правило добутку. Поняття вибірки. Основні комбінаторні об'єкти: розміщення та сполучення. Обчислення кількості розміщень і сполучень. Перестановки. Біном Ньютона. Поліноміальна теорема. Задача про цілочислові розв'язки.)	лекція, самостійна робота	[1, 4, 7, 8]	2 7	1 тиждень
	Тема 9. Основні правила комбінаторного аналізу. Розміщення та сполучення. **(**Обчислення кількості розміщень і сполучень. Перестановки. Біном Ньютона. Поліноміальна теорема. Задача про цілочислові розв'язки.)	лаб.	[1, 4, 7, 8]	2	
10	**Тема 10. Числа Стірлінга другого**	лекція,	[1, 4, 7, 8]	2	1 тиждень

	роду та числа Белла. Генерування комбінаторних об'єктів. Дискретна ймовірність. (Задача підрахунку кількості розбиттів множини на непорожні частини. Числа Стірлінга другого роду та числа Белла, їх обчислення. Генерування перестановок, сполучень, розміщень. Генерування розбиттів множини. Дискретна ймовірність: означення та приклади)	самостійна робота		6	
	Тема 10. Числа Стірлінга другого роду та числа Белла. Генерування комбінаторних об'єктів. Дискретна ймовірність. (Підрахунок кількості розбиттів множини на непорожні частини. Числа Стірлінга другого роду та числа Белла, їх обчислення. Генерування перестановок, сполучень, розміщень. Генерування розбиттів множини. Дискретна ймовірність, приклади)	лаб.	[1, 4, 7, 8]	2	1 тиждень
11	**Тема 11. Розвинута техніка підрахунку.** (Рекурентні рівняння, числа Фібоначчі, розв'язування лінійних однорідних і неоднорідних рекурентних рівнянь. Принцип коробок Діріхле, Принцип включення – виключення, принцип включення – виключення в альтернативній формі)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 11. Розвинута техніка підрахунку. (Розв'язування лінійних однорідних і неоднорідних рекурентних рівнянь. Принцип коробок Діріхле, Принцип включення – виключення, принцип включення – виключення в альтернативній формі)	лаб.	[1, 4, 7, 8]	2	
12	**Тема 12. Булеві функції.** (Означення булевої функції, реалізація функцій формулами. Еквівалентність формул. Двоїстість)	лекція, самостійна робота	[1, 4, 7]	2 6	1 тиждень
	Тема 12. Булеві функції. (Табличне задання булевої функції. Реалізація функцій формулами. Еквівалентність формул. Двоїстість)	лаб.	[1, 4, 7]	2	
13	**Тема 13. Алгебри булевих функцій.** (Алгебра Буля, алгебра Жегалкіна. Диз'юнктивні й кон'юнктивні нормальні форми. Поліном Жегалкіна)	лекція, самостійна робота	[1, 4, 7]	2 7	1 тиждень
	Тема 13. Алгебри булевих функцій. (Побудова диз'юнктивних, кон'юнктивних нормальних форм і полінома Жегалкіна)	лаб.	[1, 4, 7]	2	
14	**Тема 14. Повнота системи булевих функцій.** (Функціонально повні системи. Замкнені класи. Критерій функціональної повноти системи булевих функцій. Джордж Буль. Аугустус де Морган)	лекція, самостійна робота	[1, 4, 7]	2 7	1 тиждень
	Тема 14. Повнота системи булевих	лаб.	[1, 4, 7]	2	

	функцій. (Функціонально повні системи. Замкнені класи. Критерій функціональної повноти системи булевих функцій)				
15	**Тема 15. Мінімізація булевих функцій.** (Мінімальні диз'юнктивні нормальні форми. Скорочена диз'юнктивна нормальна форма. Алгоритм Квайна. Алгоритм Мак-Класкі. Тупикові диз'юнктивні нормальні форми та імплікантна таблиця. Алгоритм Петріка знаходження всіх тупикових диз'юнктивних нормальних форм)	лекція, самостійна робота	[1, 4, 7]	2 7	1 тиждень
	Тема 15. Мінімізація булевих функцій. (Мінімальні диз'юнктивні нормальні форми. Скорочена диз'юнктивна нормальна форма. Алгоритм Квайна. Алгоритм Мак-Класкі. Тупикові диз'юнктивні нормальні форми та імплікантна таблиця. Алгоритм Петріка знаходження всіх тупикових диз'юнктивних нормальних форм)	лаб.	[1, 4, 7]	2	
16	**Тема 16. Метод карт Карно. Поняття про схеми з функціональних елементів.** (Метод карт Карно побудови мінімальних диз'юнктивних нормальних форм. Застосування до булевих функцій від трьох та чотирьох змінних. Означення схеми з функціональних елементів)	лекція, самостійна робота	[1, 4, 7]	2 7	1 тиждень
	Тема 16. Метод карт Карно. Поняття про схеми з функціональних елементів. (Метод карт Карно побудови мінімальних диз'юнктивних нормальних форм: застосування до булевих функцій від трьох та чотирьох змінних. Приклади схем з функціональних елементів)	лаб.	[1, 4, 7]	2	