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 "Застосування 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	**Застосування 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 "Застосування дискретної математики" є нормативною дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 2-му семестрі першого (бакалаврського) рівня освіти в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Застосування дискретної математики є важливою складовою підготовки з кібербезпеки. Розглядаються такі розділи: теорія графів, дерева та їхні застосування, відношення, теорія кодів. 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 "Застосування 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. Додаткова література: 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: 120 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 години лабораторних занять. Самостійної роботи: 56 годин.
Очікувані результати навчання	Після завершення цього курсу студент буде Знати: - основні означення та теореми теорії графів; - алгоритми на графах; - застосування графів; - дерева та їх застосування в інформатиці; - відношення та їх застосування; - основні поняття теорії кодів. Вміти: - використовувати графові моделі для розв'язування задач; - використовувати властивості дерев для розв'язування типових задач; - здійснювати обхід кореневих дерев, формувати польський запис виразів, будувати бінарне дерево пошуку; - виявляти відношення еквівалентності й відношення часткового порядку та розв'язувати типові задачі; - будувати коди Фано і Гаффмана; - будувати коди Геммінга; **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 2, КФ 10, КФ 12; та програмних результатів навчання: ПРН 2-6, ПРН 10-12, ПРН 28, ПРН 47, ПРН 48, ПРН 53.**
Ключові слова	Граф, ізоморфізм графів, найкоротший шлях у графі, алгоритм Дейкстри, алгоритм Флойда, мінімальний каркас, алгоритм Краскала, дерево, польський запис, дерево рішень, відношення, алгоритм Воршалла, алфавітне кодування, рівномірне кодування, код Фано, код Гаффмана, код Геммінга.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.

Теми	1. Поняття графа. Способи подання графів. Ізоморфізм. 2. Шляхи й цикли. Зв'язність графів. 3. Ейлерів і гамільтонів цикли. 4. Планарність. Розфарбування. Незалежність. Паросполучення, теорема Голла. 5. Задача про найкоротший шлях. Алгоритм Дейкстри. Задача комівояжера (лише формулювання). 6. Поняття дерева. Рекурсія. Обхід дерев. Польська нотація. 7. Застосування дерев в інформаційних технологіях. 8. Відношення та їхні властивості. 9. Замикання відношень. 10. Відношення еквівалентності. 11. Відношення часткового порядку. Застосування відношення часткового порядку в інформаційних технологіях. 12. Алфавітне й рівномірне кодування. Роздільні коди. 13. Оптимальне кодування. Код Фано. 14. Оптимальне кодування (закінчення). Код Гаффмана. Стиснення даних: алгоритм Лемпеля – Зіва. 15. Коди, стійкі до перешкод. Необхідні й достатні умови виявлення та виправлення помилок. 16. Коди Геммінга.
Підсумковий контроль, форма	Екзамен у кінці другого семестру.
Пререквізити	Для вивчення курсу студенти потребують базові знання з математики в обсязі середньої школи, а також дисциплін: "Моделі та методи дискретної математики", "Основи кібербезпеки".
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 екзаменів.	**2-й семестр.** Поняття графа. Способи подання графів. Шляхи та цикли. Зв'язність. Ізоморфізм графів. Ейлерів і гамільтонів цикли в неорієнтованих графах. Планарні графи. Теорема Куратовського. Розфарбування графів. Незалежні множини вершин і кліки. Паросполучення у двочастковому графі. Теорема Голла. Дерева, основні властивості. Кореневі дерева. Обхід дерев, польська нотація. Дерево рішень. Бінарні відношення. Композиція відношень. Транзитивне замикання відношення, алгоритм Воршалла. Відношення еквівалентності. Відношення часткового порядку. Діаграма Гассе. Решітка. Схеми алфавітного та рівномірного кодування. Оптимальне кодування. Код Гаффмана. Коди, стійкі до перешкод. Коди Геммінга.
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. Поняття графа. Способи подання графів. Ізоморфізм.** (Основні означення та властивості. Деякі спеціальні класи простих графів. Способи подання графів: матриця інцидентності, матриця суміжності. Ізоморфізм графів)	лекція, самостійна робота	[1, 4, 6-8]	2 6	1 тиждень
	Тема 1. Поняття графа. Способи подання графів. Ізоморфізм. (Основні означення та властивості. Спеціальні класи простих графів. Подання графів матрицею інцидентності та матрицею суміжності. Визначення ізоморфізму графів)	лаб	[1, 4, 6-8]	2	
2	**Тема 2.Шляхи й цикли. Зв'язність графів.** (Шляхи й цикли. Зв'язність. Термінологія. Шляхи в графах та ізоморфізм. Оцінка кількості ребер простого графа. Критерій двочастковості графа.)	лекція, самостійна робота	[1, 4, 6-8]	2 6	1 тиждень
	Тема 2.Шляхи й цикли. Зв'язність графів. (Шлях та цикл, варіанти термінології. Шляхи та ізоморфізм. Оцінки кількості ребер простого графа. Критерій двочастковості графа.)	лаб.	[1, 4, 6-8]	2	
3	**Тема 3. Ейлерів і гамільтонів цикли.** (Ейлерів цикл у графі, задача про кенігсбергські мости. Критерій наявності ейлеревого циклу в неорієнтованому графі. Алгоритм Флері. Гамільтонів цикл у неорієнтованому графі, теореми Дірака та Оре)	лекція, самостійна робота	[1, 4, 6-8]	2 6	1 тиждень
	Тема 3. Ейлерів і гамільтонів цикли. (Побудова ейлеревого циклу за алгоритмом об'єднання циклів і за алгоритмом Флері. Гамільтонів цикл у неорієнтованому графі, Приклади застосування теорем Дірака та Оре)	лаб	[1, 4, 6-8]	2	
4	**Тема 4. Планарність. Розфарбування. Незалежність. Паросполучення, теорема Голла.** (Означення плоского та планарного графів. Теорема Ейлера про плоскі графи та наслідки з неї. Розфарбування графа, хроматичне число. Незалежні множини вершин. Кліки)	лекція, самостійна робота	[1, 4, 6-8]		
	Тема 4. Планарність. Розфарбування. Незалежність. Паросполучення, теорема Голла. (Означення плоского та планарного графів. Теорема Ейлера про плоскі графи та наслідки з неї. Критерії планарності: теореми Куратовського та Вагнера /без доведення/. Розфарбування графа,	лаб.	[1, 4, 6-8]		

	Практичні задачі, які зводяться до розфарбування графів. хроматичне число. Незалежні множини вершин. Кліки. Паросполучення, теорема Голла та її застосування)				
5	**Тема 5. Задача про найкоротший шлях. Алгоритм Дейкстри. Задача комівояжера.** (Різні формулювання задач про найкоротший шлях. Алгоритм Дейкстри та його реалізація. Задача комівояжера, складність її розв'язання)		[1, 4, 6-8]	2 6	1 тиждень
	Тема 5. Задача про найкоротший шлях. Алгоритм Дейкстри. Задача комівояжера. (Різні формулювання задач про найкоротший шлях. Реалізація алгоритму Дейкстри. Алгоритм Дейкстри належить дл жадібних алгоритмів)		[1, 4, 6-8]	2	
6	**Тема 6. Дерева та їхні застосування.** (Поняття дерева, основні означення та властивості. Рекурсія. Обхід дерев. Польська нотація)	лекція, самостійна робота	[1, 4, 6-8]	2 6	1 тиждень
	Тема 6. Дерева та їхні застосування. (Поняття дерева, основні означення та властивості. Рекурсія. Обхід дерев. Подання виразів у польській та зворотній польській нотаціях)	лаб.	[1, 4, 6-8]	2	
7	**Тема 7. Застосування дерев в інформаційних технологіях.** (Код Прюфера для дерев, теорема Келі, бінарне дерево пошуку, АВЛ-дерево, червоно-чорне дерево, дерево рішень, бектрекінг, каркаси, задача про мінімальний каркас: алгоритм Краскала)	лекція, самостійна робота	[1, 4, 6-8]	2 6	1 тиждень
	Тема 7. Застосування дерев в інформаційних технологіях. (Код Прюфера для дерев, теорема Келі, бінарне дерево пошуку: алгоритми додавання об'єкта в дерево і пошуку об'єкта, АВЛ-дерево, червоно-чорне дерево, дерево рішень, бектрекінг, каркаси, задача про мінімальний каркас: алгоритм Краскала)	лаб.	[1, 4, 6-8]	2	
8	**Тема 8. Відношення та їхні властивості.** (Означення відношення, функції як відношення, подання відношень матрицями та орієнтованими графами, властивості бінарних відношень на множині, теоретико-множинні операції над відношеннями, композиція відношень, теорема про властивість степеня транзитивного відношення. Операції над булевими матрицями, операції над відношеннями через матриці відношень)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 8. Відношення та їхні властивості. (Означення відношення, функції як відношення, подання відношень матрицями	лаб.	[1, 4, 7, 8]	2	

	та орієнтованими графами, властивості бінарних відношень на множині, теоретико-множинні операції над відношеннями, композиція відношень, теорема про властивість степеня транзитивного відношення. Операції над булевими матрицями, операції над відношеннями через матриці відношень)				
9	**Тема 9 Замикання відношень.** **(**Рефлексивне, симетричне та транзитивне замикання відношення. Алгоритм Воршалла**)**	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 9. Замикання відношень. **(**Рефлексивне, симетричне та транзитивне замикання відношення. Алгоритм Воршалла, його реалізація.**)**	лаб.	[1, 4, 7, 8]	2	
10	**Тема 10. Відношення еквівалентності.** **(**Приклади відношень еквівалентності. Теореми про зв'язок між відношенням еквівалентності та розбиттям множини**)**	лекція, самостійна робота	[1, 4, 7, 8]	2 7	1 тиждень
	Тема 10. Відношення еквівалентності. (Наведення прикладів відношень еквівалентності. Побудова розбиття множини за відношенням еквівалентності та відношення еквівалентності за розбиттям множини**)**	лаб.	[1, 4, 7, 8]	2	
11	**Тема 11. Відношення часткового порядку. Застосування відношення часткового порядку в інформаційних технологіях.** (Означення відношення часткового порядку. Діаграма Гассе. Максимальні та мінімальні елементи. Решітки. Решіткова модель інформаційного потоку. Топологічне сортування)	лекція, самостійна робота	[1, 4, 7, 8]	2 6	1 тиждень
	Тема 11. Відношення часткового порядку. Застосування відношення часткового порядку в інформаційних технологіях. (Означення відношення часткового порядку. Побудова діаграми Гассе. Максимальні та мінімальні елементи. Решітки. Решіткова модель інформаційного потоку. Топологічне сортування)	лаб.	[1, 4, 7, 8]	2	1 тиждень
12	**Тема 12. Алфавітне й рівномірне кодування. Роздільні коди.** (Означення алфавітного та рівномірного кодувань. Достатні умови однозначності алфавітного декодування. Властивості роздільних кодів. Префіксна схема. Нерівність Мак-Міллана та пов’язані з нею результати)	лекція, самостійна робота	[1, 3-5, 7]	2 6	1 тиждень
	Тема 12. Алфавітне й рівномірне кодування. Роздільні коди. (Означення алфавітного та рівномірного кодувань. Достатні умови однозначності алфавітного декодування. Властивості роздільних кодів. Префіксна схема. Нерівність Мак-Міллана та пов’язані з нею результати)	лаб.	[1, 3-5, 7]	2	

13	**Тема 13. Оптимальне кодування. Код Фано.** (Середня довжина кодування. Коди з мінімальною надлишковістю, або оптимальні коди. Код Фано – код, близький до оптимального. Кодове дерево)	лекція, самостійна робота	[1, 3-5, 7]	2 7	1 тиждень
	Тема 13. Оптимальне кодування. Код Фано. (Середня довжина кодування. Коди з мінімальною надлишковістю, або оптимальні коди. Побудова коду Фано)	лаб.	[1, 3-5, 7]	2	
14	**Тема 14. Оптимальне кодування (закінчення). Код Гаффмана. Стиснення даних: алгоритм Лемпеля – Зіва.** (Оптимальне кодування. Код Гаффмана – оптимальний код. Поняття про алгоритм Лемпеля – Зіва для стиснення даних)	лекція, самостійна робота	[1, 3-5, 7]	2 7	1 тиждень
	Тема 14. Оптимальне кодування (закінчення). Код Гаффмана. Стиснення даних: алгоритм Лемпеля – Зіва. (Оптимальне кодування. Побудова коду Гаффмана за таблицею та за деревом Гаффмана. Алгоритм Гаффмана належить до жадібних алгоритмів.)	лаб.	[1, 3-5, 7]	2	
15	**Тема 15. Коди, стійкі до перешкод. Необхідні й достатні умови виявлення та виправлення помилок.** (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, 3-5, 7]	2 7	1 тиждень
	Тема 15. Коди, стійкі до перешкод. Необхідні й достатні умови виявлення та виправлення помилок. (Віддаль Гемінга, аксіоми метрики. Умови надійності кодування в разі адитивних помилок: умова виявлення і умова виправлення помилок)	лаб.	[1, 3-5, 7]	2	
16	**Тема 16. Коди Геммінга** (Лінійні або групові коди. Теорема про кодову віддаль лінійного коду. Коди Геммінга. Задання коду Геммінга за допомогою перевірочної матриці. (7,4,3)- та (15,11,3)-коди Геммінга. Виявлення двох та виправлення однієї помилки: (8,4,4)- та (16,11,4)-коди Геммінга)	лекція, самостійна робота	[1, 3-5, 7]	2 7	1 тиждень
	Тема 16. Коди Геммінга Побудова (7,4,3)- та (15,11,3)-кодів Геммінга. Виявлення двох та виправлення однієї помилки у (8,4,4)- та (16,11,4)-кодах Геммінга)	лаб.	[1, 3-5, 7]	2	