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 № 1/20 від 27 серпня 2020р.)

Завідувач кафедри Притула М. М.
_____

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

Львів 2020 р.

Назва	**Моделі та методи дискретної математики**

дисципліни	
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 дискретного аналізу та інтелектуальних систем
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека
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 в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua
Інформація про дисципліну	Моделі та методи дискретної математики є теоретичною основою підготовки з кібербезпеки. Розглядаються такі розділи: теорія чисел і основи криптографії, комбінаторний аналіз, функції алгебри логіки, відношення, теорія графів, дерева та їхні застосування, основи теорії кодування, формальні мови, граматики і автомати, машини Тьюрінга. 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. Висвітюються питання обчислювальної складності.
Коротка анотація дисципліни	Дисципліна "Моделі та методи дискретної математики" є нормативною дисципліною з спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 1-му та 2-му семестрах в обсязі 8-ми кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
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	1. *Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.* Дискретна математика (у серії „Інформатика"). Київ: Видавнича група BHV, 2006, 2007. 2. *Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина.* Дискретна математика (у серії „Комп'ютинг"). Львів: Магнолія-2006, 2009 (1-е видання), 2010 (2-е видання), 2013 (3-є видання), 2016 (4-е видання), 2019 (5-е видання). 3. *Ю.В. Капітонова, С.Л. Кривий, О.А. Летичевський, М.К. Печурін.* Основи дискретної математики. К.: Наукова думка, 2002. 4. *Kenneth H. Rosen.* Discrete Mathematics and Its Applications. Seventh

	Edition. McGraw-Hill, Inc, 2012. 5. *Richard Crandall, Carl Pomerance.* Prime Numbers. A Computational Perspektive. Second Editson. Springer, 2005.
Обсяг курсу	Загальний обсяг: 240 годин. Аудиторних занять: 128 год., з них 64 години лекцій та 64 години лабораторних занять. Самостійної роботи: 112 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; - основні означення та теореми теорії графів; - алгоритми на графах; - дерева та їх застосування в інформатиці; - відношення та їх застосування; - основні поняття теорії кодів; - скінченні автомати та їх застосування у криптографії. Вміти: - розв'язувати типові задачі з множинами; - розв'язувати лінійні конгруенції; - розрізняти симетричні та асиметрична 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 – вилучення; - 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; - знаходити мову за породжувальною граматикою та породжувальну граматику за мовою, розпізнавати типи граматик і мов; - знаходити мову, яка розпізнається скінченним автоматом, та будувати скінченний автомат для подання регулярної мови; - будувати машини Тьюрінга для елементарних прикладів; - використовувати поняття алгоритмічно нерозв'язної проблеми та обчислювальної складності.
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, 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, формальна мова, скінченний автомат, машина Тьюрінга.
Формат курсу	Очний, дистанційний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	**1-й семестр. Математичні основи** 1. Множини. 2. Функції. 3. Подільність і модулярна арифметика. Прості числа. 4. Алгоритм Евкліда. Лінійні конгруенції. 5. Застосування конгруенцій. Класична криптографія. 6. Криптосистеми з відкритим ключем. Криптосистема RSA. 7. Криптографічні протоколи. 8. Основні поняття й теореми комбінаторного аналізу. 9. Генерування комбінаторних об'єктів. Дискретна ймовірність. 10. Розвинута техніка підрахунку. 11. Булеві функції. Реалізація функцій формулами. 12. Алгебри булевих функцій. 13. Повнота й замкненість. 14. Мінімізація булевих функцій. 15. Підсумкова лекція. **2-й семестр. Математичні моделі та алгоритми** 1. Поняття графа. 2. Зв'язність графів. Ейлерів і гамільтонів цикли. 3. Планарність. Розфарбування графів. Незалежність і покриття. 4. Поняття дерева. Рекурсія. Каркаси графів. 5. Застосування дерев в інформаційних технологіях. 6. Відношення та їхні властивості. 7. Замикання відношень. 8. Відношення еквівалентності. Відношення часткового порядку. Застосування відношення часткового порядку в інформаційних технологіях. 9. Алфавітне й рівномірне кодування. 10. Оптимальне кодування. Код Фано. Код Гаффмана. 11. Коди, стійкі до перешкод. Необхідні й достатні умови виявлення та виправлення помилок. Коди Геммінга. 12. Мови і граматики. 13. Скінченні автомати. 14. Машини Тьюрінга. 15. Підсумкова лекція.
Підсумковий контроль, форма	Екзамени у кінці першого і другого семестрів.
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	Презентації, лекції Індивідуальні завдання Групові проекти, менторство

використовувати ся під час викладання курсу	
Необхідне обладнання	Комп'ютер, 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. П**олітика 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.	**1-й семестр.** 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. **2-й семестр.** 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. Скінченні автомати з виходом. Автомати Мілі та Мура. Скінченні автомати без виходу. Детерміновані та недетерміновані скінченні автомати. Застосування скінченних автоматів. Машини Тьюрінга. Уточнення поняття алгоритму на основі машини Тьюрінга: теза Тьюрінга. Алгоритмічно нерозв'язні задачі.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.