

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 Притула М.М.



Силабус з навчальної дисципліни
«Дискретна математика»,
що викладається в межах першого (бакалаврського) рівня
вищої освіти для здобувачів
з спеціальності 113 Прикладна математика

Львів 2023 р.

| | |
|--|---|
| Назва дисципліни | Дискретна математика |
| 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 | 11 Математика та статистика 113 Прикладна математика |
| Викладачі дисципліни | Коковська Ярина Володимирівна, доцентка кафедри дискретного аналізу та інтелектуальних систем (лекції), Кириченко Наталія Володимирівна, асистентка кафедри дискретного аналізу та інтелектуальних систем (лабораторні заняття). |
| Контактна інформація викладачів | yaryna.kokovska@lnu.edu.ua ; https://ami.lnu.edu.ua/employee/kokovska ; nataliia.kyrychenko@lnu.edu.ua ; https://ami.lnu.edu.ua/employee/kvrychenko . 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/course/discrete-mathematics-applied-mathematics |
| Інформація про дисципліну | Дисципліна «Дискретна математика» є нормативною дисципліною з спеціальності 113 Прикладна математика, яка викладається в 1-му та 2-му семестрах в обсязі 9-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| Мета та цілі дисципліни | Метою курсу є строге викладення теоретичних положень зазначених вище розділів з доведенням теорем, формулюванням алгоритмів розв'язування дискретних задач, аналізом та роз'яснення нюансів алгоритмічної реалізації. Компетенції, якими треба оволодіти студентів: виконувати основні операції над множинами, використовуючи комп'ютерне подання множин; формулювати основні положення математичної логіки та застосовувати їх у доведеннях теорем; працювати з графами, зокрема, використовувати основні алгоритми на графах; працювати з деревами; використовувати апарат відношень; розуміти проблематику застосувань теорії кодів в інформатиці та вміти будувати коди Фано, Гаффмана, Геммінга; працювати з апаратом булевих функцій, вміти будувати нормальні форми, мінімальні форми, схеми з функціональних елементів; знати принципи побудови криптографічних алгоритмів, криптографічних стандартів та їх використання в задачах захисту інформації; розуміти основні концепції теорії обчислень; розуміти основні концепції теорії алгоритмів, зокрема, алгоритмічно нерозв'язні проблеми та обчислювальну складність. |

| | |
|--|--|
| <p>Коротка анотація дисципліни</p> | <p>Курс розроблено таким чином, щоб надати студентам знання з таких розділів, як основи математичної логіки, комбінаторного аналізу, теорії графів, відношення, основи теорії кодування, булевих функції, основ теорії формальних граматики і автоматів, теорії алгоритмів</p> <p>Курс дискретної математики має багато призначень. Студенти повинні опанувати значний обсяг математичних фактів та способів їх застосування.</p> <p>Основні знання, що їх повинні набути студенти, стосуються таких розділів: основи теорії множин, комбінаторний аналіз, відношення, теорія графів, математичної логіки, основи теорії кодування, теорія чисел і основи криптографії, булеві функції, основи теорії формальних граматики і автоматів, головні поняття теорії алгоритмів.</p> <p>З кожного розділу розглядаються можливі застосування, в основному до проблем прикладної математики. В усіх розділах приділяється значна увага побудові алгоритмів для розв'язування задач дискретної математики. Поняття, факти, алгоритми, що вивчаються у курсі «Дискретна математика» використовуються у курсах «Основи програмування», «Архітектура комп'ютерних систем», «Алгоритми обчислювальних процесів», «Теорія ймовірностей», «Системи штучного інтелекту», «Методи оптимізації», «Дослідження операцій».</p> |
| <p>Література для вивчення дисципліни</p> | <p style="text-align: center;">Основна література</p> <ol style="list-style-type: none"> 1. <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. 2. <i>Євсєєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В.</i> Кібербезпека: основи кодування та криптографії: навч. посібник. – Харків: ХПІ, 2023. – 658 с. 3. <i>Kenneth H. Rosen.</i> Discrete Mathematics and Its Applications. Eighth Edition. McGraw-Hill, Inc, 2019. – 1118 p. 4. <i>Heba Al-Asady.</i> Introduction to Information Theory and Coding: Probability, Entropy, Channels, and Error Detection and Correction Codes. Lambert academic publ., 2019. – 136 p. 5. Гнатів Б.В., Гладун В.Р., Гнатів Л.Б. Дискретна математика. Навчальний посібник. – Львів: Вид-во Львівської політехніки, 2021. 400 с. 6. Денисова Т.В., Сенчуков В.Ф. Дискретна математика [Електронний ресурс]: навч. посіб. – Харків : ХНЕУ ім. С. Кузнеця, 2019. – 287 с. 7. Якімова Н.А. Дискретна математика. Частина 1. Теорія множин, Теорія графів: курс лекцій. – Одес. нац. ун-т ім. І.І. Мечнікова. – Одеса, 2022. – 101 с. <p style="text-align: center;">Додаткова література</p> <ol style="list-style-type: none"> 8. Нікольський Ю.В., Пасічник В.В., Щербина Ю.М. Дискретна математика (у серії „Комп'ютинг”). Львів, Магнолія-2006, 2009, 2010. 9. Пивоварчик В.М., Яковлева О.М., Болдарєва О.М. Дискретна математика. – Одеса, 2022. – 145 с. 10. Темнікова О.Л. Дискретна математика: конспект лекцій (Частина 1) [Електронний ресурс] : навч. посіб. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 154 с. 11. Трохимчук Р.М., Нікітченко М.С. Дискретна математика у прикладах і задачах; навч. посібник. – Київ: Київський університет, 2017. – 248 с. |

| | |
|---|---|
| Обсяг курсу | Загальний обсяг: 270 годин. Аудиторних занять: 144 год., з них 64 год. лекцій та 80 годин практичних робіт. Самостійної роботи: 126 год. |
| Очікувані результати навчання | <p>Після завершення цього курсу студент буде:</p> <p>знати:</p> <ul style="list-style-type: none"> • основні операції над множинами, використовуючи комп'ютерне подання множин; • головні положення математичної логіки та застосовувати їх у доведеннях теорем; • задачі з графами, зокрема, використовувати основні алгоритми на графах; • розв'язувати задачі з деревами; • основні концепції теорії алгоритмів, зокрема, алгоритмічно нерозв'язні проблеми та обчислювальну складність; • принципи побудови криптографічних алгоритмів, криптографічних стандартів та їх використання в задачах захисту інформації; <p>вміти:</p> <ul style="list-style-type: none"> • використовувати апарат відношень; • застосовувати теорію кодів та вміти будувати коди Фано, Гаффмана, Геммінга; • працювати з апаратом булевих функцій, будувати нормальні форми, мінімальні форми, схеми з функціональних елементів; • використовувати основні концепції теорії обчислень; • 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. <p>Курс забезпечує набуття таких компетентностей: ЗК 06, ФК 01, ФК 02 та програмних результатів навчання: РН 02, РН 03, РН 04.</p> |
| Ключові слова | множини, графи, дерева, булеві функції, кодування, шифрування даних. |
| Формат курсу | Очний Проведення лекцій, лабораторних робіт і консультацій. Ознайомлення з Internet курсами з дискретної математики. |
| Теми | Теми подано нижче у Схемі курсу |
| Підсумковий контроль, форма | 1-й семестр – екзамен, 2-й семестр – екзамен |
| Пререквізити | Для вивчення курсу студенти потребують базових знань середньої освіти. |
| Навчальні методи та техніки, які будуть використовуватися під час викладання курсу | Презентації, лекції Індивідуальні комп'ютерні завдання Групові проекти, менторство |
| Необхідне обладнання | Використання у навчанні додатків для мобільних телефонів, зокрема ресурсів Google, інструментів Microsoft Teams. Друковані та електронні підручники та посібники; Інтернет-технології, вебсервіси. |
| Критерії оцінювання (окремо для кожного виду нав- | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • поточне тестування - максимальна кількість балів 30, 2 тести по 15 балів кожен; |

| | |
|-----------------------------------|---|
| <p>чальної діяльності)</p> | <ul style="list-style-type: none"> • виконання індивідуальних комп'ютерних проєктів, максимальна кількість балів 20, 2 завдання по 10 балів кожне. 10 балів – студент повністю, якісно та вчасно виконує завдання, 5-9 балів – студент не повністю виконав поставлене завдання, 1-4 балів – студент не повністю виконує поставленні перед ним завдання, не виконує завдання вчасно, 0 балів – студент не готовий до заняття, не виконав завдання; • екзамен: 50% семестрової оцінки; максимальна кількість балів 50. <p>Підсумкова максимальна кількість балів 100.</p> <p>Письмові роботи: Очікується, що студенти виконають 2 письмові роботи і звіти про виконання індивідуальних завдань.</p> <p>Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними 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>Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні 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, 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 набрані при поточному тестуванні, за виконання індивідуальних комп'ютерних проєктів та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного 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> | <ol style="list-style-type: none"> 1. Множина. Кортеж. Декартів добуток множин. Операції над множинами. Доведення рівностей з множинами. 2. Відношення. Властивості відношень. Способи подання бінарних відношень. Відношення еквівалентності. Розбиття множини на класи еквівалентності. Конгруентність за модулем m. Відношення часткового порядку. Замикання відношень. Алгоритм Уоршала. 3. Основні правила комбінаторики. Поняття вибірки. Розміщення та сполучення. Перестановки. Задача про цілочислові розв'язки. Розв'язування однорідних рекурентних рівнянь. Розв'язування неоднорідних рекурентних рівнянь. Принцип коробок Діріхле Принцип включення – виключення. 4. Графи, основні означення та властивості. Спеціальні класи простих графів. Способи подання графів. Шляхи та цикли. Зв'язність. Характеристики зв'язності графа, точки з'єднання та мости. Поняття двозв'язного графа. Критерій двочастковості графа. Ізоморфізм графів. Ейлерів цикл у графі. Гамільтонів цикл у графі. Задачі про найкоротші |

| | |
|-------------------|--|
| | <p>шляхи у зважених графах. Алгоритм Дейкстри. Алгоритм Флойда. Обхід графа вглиб та вшир. Планарні графи. Розфарбування графів. Незалежні множини вершин. Кліки. Паросполучення у графах.</p> <p>5. Дерева, основні означення та властивості. Поняття m-арного дерева. Обхід дерев. Бінарне дерево пошуку. Дерево прийняття рішень. Алгоритм ID3. Бектрекінг. Каркаси. Способи побудови каркасів у графах. Алгоритм Краскала для знаходження мінімального (максимального) каркасу.</p> <p>6. Алфавітне й рівномірне кодування. Схеми алфавітного та рівномірного кодування. Достатні умови однозначності декодування. Властивості роздільних кодів. Оптимальне кодування. Код Фано. Код Гаффмана. Коди, стійкі до перешкод.</p> <p>7. Булеві функції. Алгебри булевих функцій. Спеціальні форми подання булевих функцій. Повнота та замкненість. Мінімізація булевих функцій.</p> <p>8. Мови і граматики. Типи граматик. Дерева виведення. Скінченні автомати з виходом. Скінченні автомати без виходу. Детерміновані та недетерміновані скінченні автомати. Регулярні вирази та регулярні множини. Мови, які розпізнаються скінченними автоматами.</p> <p>9. Основи теорії шифрування даних. Класичні симетричні криптосистеми. Сучасні симетричні криптосистеми. Сучасні асиметричні криптосистеми.</p> <p>10. Основи теорії алгоритмів. Поняття про алгоритмічні моделі. Основні вимоги до алгоритмів. Машини Тьюрінга. Обчислення числових функцій на машинах Тьюрінга.</p> |
| Опитування | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу. |

Схема курсу 1 семестр

| Ти ж. | Тема, план, короткі тези | Форма діяльності (заняття) | Літератур а. Ресурси в інтернеті | Завдан ня, год. | Термін виконан ня |
|-------|--|----------------------------|----------------------------------|-----------------|-------------------|
| 1 | Тема 1. Основи теорії множин (Поняття множини і кортежу. Декартів добуток множин. Теоретико-множинні операції. Комп'ютерне подання множин) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 1. Функції (Поняття функції. Способи подання функції. Ін'єкція, сюр'єкція і бієкція. Зростання функцій. Оцінки складності алгоритмів. Приклади) | лаб. | [1-7] | 2 | 1 тиждень |
| 2 | Тема 2. Основи комбінаторного аналізу (Основні правила комбінаторного аналізу: правило суми й правило добутку. Поняття вибірки. Розміщення та сполучення. Перестановки) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 2. Приклади на обчислення розміщень, сполучень та перестановок | лаб. | [1-7] | 2 | 1 тиждень |
| 3 | Тема 3. Біноміальна і поліноміальна теореми. Задача про цілочислові розв'язки. Числа Стірлінга другого роду та числа Белла | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |

| | | | | | |
|---|---|---------------------------|-------|--------|----------------------------------|
| | Тема 3. Приклади на обчислення поліноміальних коефіцієнтів | лаб. | [1-7] | 2 | 1 тиждень |
| 4 | Тема 4. Генерування комбінаторних об'єктів (<i>Генерування перестановок. Генерування сполучень. Генерування розбиттів множини</i>) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 4. Приклади на обчислення комбінаторних об'єктів (<i>Індивідуальний комп'ютерний проект №1</i>) | лаб. | [1-7] | 2 | 1 тиждень під час заняття |
| 5 | Тема 5. Розвинута техніка підрахунку (<i>Метод рекурентних рівнянь. Принцип коробок Діріхле. Принцип включення – виключення. Принцип включення – виключення в альтернативній формі</i>) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 5. Приклади на обчислення рекурентних рівнянь (<i>однорідні і неоднорідні рівняння</i>) | лаб. | [1-7] | 2 | 1 тиждень |
| 6 | Тема 6. Відношення та їх властивості. (<i>Означення бінарного відношення. Способи подання відношень. Відношення еквівалентності. Відношення часткового порядку. Топологічне сортування</i>) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Модульний контроль 1 | лаб. | - | 2 | під час заняття |
| 7 | Тема 7. Операції над відношеннями (<i>Теоретико-множинні операції над відношеннями. Композиція відношень. Замикання відношень. Алгоритм Уоршалла</i>) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 7. Приклади на обчислення композицій відношень та їх замикань. | лаб. | [1-7] | 2 | 1 тиждень |
| 8 | Тема 8. Основні означення теорії графів. Властивості графів. (<i>Означення простого графа, мультиграфа та псевдографа. Теорема про рукостискання. Орієнтовані графи. Спеціальні класи простих графів. Матриця інцидентності. Матриця суміжності. Список пар (список ребер). Списки суміжності</i>) | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 8. Приклади на обчислення матриць інцидентності та суміжності | лаб. | [1-7] | 2 | 1 тиждень |
| 9 | Тема 9. Ізоморфізм графів | лекція, самостійна робота | [1-7] | 2 5 | 1 тиждень |
| | Тема 9. Приклади на способи задання графів на множині вершин многозначного | лаб. | [1-7] | 2 | 1 тиждень |

| | | | | | |
|----|---|---------------------------|-------|--------|----------------------------------|
| | відображення | | | | |
| 10 | Тема 10. Шляхи та цикли. Зв'язність (Головні означення та результати, термінологія. Характеристики зв'язності простого графа. Критерій дводольності графа (теорема Кеніга)) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 10. Приклади на обчислення списків пар та суміжностей | лаб. | [1-7] | 2 | 1 тиждень |
| 11 | Тема 11. Ейлерові та гамільтонові цикли в графах (Ейлерів цикл у зв'язному мультиграфі, необхідна й достатня умова його існування. Алгоритм Флері. Гамільтонів цикл. Теорема Дірака) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 11. Приклади на обчислення ейлерових шляхів та циклів <i>(Індивідуальний комп'ютерний проект №2)</i> | лаб. | [1-7] | 2 | 1 тиждень під час заняття |
| 12 | Тема 12. Зважені графи. (Означення зваженого графа. Формулювання задач про найкоротші шляхи. Алгоритм Дейкстри) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 12. Ейлерів цикл у зв'язному мультиграфі. <i>Розв'язування задач про знаходження довжини найкоротшого циклу, що проходить через кожне ребро принаймні один раз.</i> | лаб. | [1-7] | 2 | 1 тиждень |
| 13 | Тема 13. Обходи графів. (Пошук углиб у простому зв'язному графі. Пошук ушир у простому зв'язному графі) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 13. Приклади на обчислення найкоротших шляхів за алгоритмом Дейкстри | лаб. | [1-7] | 2 | 1 тиждень |
| 14 | Тема 14. Планарність (Плоскі і планарні графи. Грані плоского графа, формула Ейлера. Критерій планарності (теорема Куратовського)) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 14. Приклади на обходи графів пошуком углиб | лаб. | [1-7] | 2 | 1 тиждень |
| 15 | Тема 15. Розфарбування графів. (Розфарбування простого графа. Оцінки хроматичного числа. Хроматичний поліном. Розфарбування планарних графів. Проблема чотирьох фарб) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 15. Приклади на обхід графів пошуком вшир | лаб. | [1-7] | 2 | 1 тиждень |
| 16 | Тема 16. Незалежність і покриття (Незалежні множини і покриття. Кліки. Інтерпретації незалежних множин. Паросполучення. Досконале паросполучення в дводольному графі. Теорема Голла) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |

| | | | | | |
|--|-----------------------------|------|---|---|-----------------|
| | Модульний контроль 2 | лаб. | - | 2 | під час заняття |
|--|-----------------------------|------|---|---|-----------------|

Схема курсу 2 семестр

| Ти ж. | Тема, план, короткі тези | Форма діяльності (заняття) | Література. Ресурси в інтернеті | Завдання, год. | Термін виконання |
|-------|---|----------------------------|---------------------------------|----------------|----------------------------------|
| 1 | Тема 1. Древа та їх застосування (<i>Означення дерева. Властивості дерев. Кореневі дерева</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 1. Вступ у древа (<i>Рекурсивне визначення дерев, приклади</i>) | лаб. | [1-7] | 2 | 1 тиждень |
| 2 | Тема 2. Застосування дерев. (<i>Рекурсія. Обхід дерев. Бінарне дерево пошуку. Дерево рішень. Бектрекінг (пошук із поверненнями). Каркаси. Теорема Келі. Матрична теорема Кірхгофа. Задача про мінімальний каркас. Алгоритм Краскала</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 2. Розрахунки на обхід дерев. Пошук з поверненням. Приклад на алгоритм Краскала | лаб. | [1-7] | 4 | 1 тиждень |
| 3 | Тема 3. Логіка висловлювань. (<i>Означення висловлювання. Формули логіки висловлювань. Виконання, загальнозначуща (тавтологія) та заперечувана формули. Закони логіки висловлювань. Нормальні форми логіки висловлювань (диз'юнктивні та кон'юнктивні)</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 3. Приклади на обчислення бінарного дерева пошуку | лаб. | [1-7] | 2 | 1 тиждень |
| 4 | Тема 4. Логіка першого ступеня (логіка предикатів) (<i>Означення предиката. Формули логіки першого ступеня. Закони логіки першого ступеня. Випереджена нормальна форма</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 4. Приклади на закони логіки висловлень | лаб. | [1-7] | 4 | 1 тиждень |
| 5 | Тема 5. Логічне виведення (<i>Логічне виведення в логіці висловлювань. Застосування правил виведення в логіці висловлювань. Метод резолюцій. Правила виведення в численні предикатів. Методи доведення теорем</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 5. Приклади на закони логіки першого ступеня | лаб. | [1-7] | 2 | 1 тиждень |
| 6 | Тема 6. Вступ у булеві функції (<i>Означення булевої функції. Реалізація функцій формулами. Алгебри булевих функцій. Спеціальні форми подання булевих функцій. Повнота та замкненість</i>) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 6. Приклади на методи резолюцій та доведення теорем. (<i>Індивідуальний комп'ютерний проект №1</i>) | лаб. | [1-7] | 4 | 1 тиждень під час заняття |

| | | | | | |
|----|---|---------------------------------|-------|--------|--------------------|
| 7 | Тема 7. Мінімізація булевих функцій (Теорема про скорочену та мінімальну диз'юнктивні нормальні форми. Методи побудови Скороченої диз'юнктивної нормальної форми. Побудова тупикових диз'юнктивних нормальних форм. Метод карт Карно для побудови мінімальних диз'юнктивних нормальних форм) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 7. Мінімізація булевих функцій. (Приклади на обчислення повноти і замкненості булевих функцій. Приклади на методи побудови скороченої диз'юнктивної нормальної форми.) | лаб. | [1-7] | 2 | 1 тиждень |
| 8 | Тема 8. Схеми з функціональних елементів (Означення функціонального елемента і схеми з функціональних елементів. Реалізація булевих функцій схемами з функціональних елементів) | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 8. Мінімізація булевих функцій. (Приклади на побудову тупикових диз'юнктивних нормальних форм. Метод карт Карно для побудови мінімальних диз'юнктивних нормальних форм) | лаб. | [1-7] | 4 | 1 тиждень |
| 9 | Тема 9. 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 | [1-7] | 2 4 | 1 тиждень |
| | Модульний контроль 1 | лаб. | - | 2 | під час заняття |
| 10 | Тема 10. 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 | [1-7] | 2 4 | 1 тиждень |
| | Тема 10. Подільність і модулярна арифметика. Прості числа. Алгоритм Евкліда. Лінійні конгруенції. (Арифметика за модулем m , Модулярне піднесення до степеня. Пробне ділення. Решето Ератосфена. 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. | [1-7] | 4 | 1 тиждень |
| 11 | Тема 11. Застосування конгруенцій. Класична криптографія. | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |

| | | | | | |
|----|---|---------------------------------|-------|--------|-------------------------------------|
| | <i>(Геш-функції. Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація шифросистем. Шифри перестановки, Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри.)</i> | | | | |
| | Тема 11. Застосування конгруенцій. Класична криптографія. <i>(Генерування псевдовипадкових чисел. Контрольні розряди. Класифікація шифросистем. Шифри перестановки, Шифри зсуву й афінні шифри. Криптоаналіз. Поліалфавітні шифри)</i> | лаб. | [1-7] | 2 | 1 тиждень |
| 12 | Тема 12. Криптосистеми з відкритим ключем. Криптографічні протоколи. <i>(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)</i> | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 12. Криптосистеми з відкритим ключем. Криптографічні протоколи. <i>(Симетричні й асиметричні криптосистеми. Система шифрування RSA. Приклади. Обмін ключем. Цифрове підписання. Приклади.)</i> | лаб. | [1-7] | 4 | 1 тиждень |
| 13 | Тема 13. Мови і граматики. Скінченні автомати з виходом. <i>(Означення формальної мови. Породжувальні граматики. Типи граматик. Дерева виведення. Форми Бекуса–Наура. Означення та способи подання скінченного автомата з виходом. Автомати Мілі та Мура)</i> | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Тема 12. Мови і граматики. Скінченні автомати з виходом. <i>(Індивідуальний комп'ютерний проєкт №2)</i> | лаб. | [1-7] | 2 | 1 тиждень під час заняття |
| 14 | Тема 14. Скінченні автомати без виходу <i>(Означення та способи подання. Детерміновані та недетерміновані скінченні автомати)</i> | лекція, самостійна робота | [1-7] | 2 3 | 1 тиждень |
| | Тема 14. Приклади на побудову скінченних автоматів з виходом та без виходу. | лаб. | [1-7] | 4 | 1 тиждень |
| 15 | Тема 15. Подання мов. Поняття про алгоритмічні моделі. <i>(Регулярні вирази та регулярні множини. Теорема Кліні. Мови, які розпізнаються скінченними автоматами. Лема про накачування для регулярних мов. Лема про накачування для контекстно вільних мов. Основні вимоги до алгоритмів. Машина Тьюрінга. Обчислення числових функцій на машинах Тьюрінга)</i> | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |

| | | | | | |
|----|---|---------------------------------|-------|--------|--------------------|
| | Тема 15. Поняття про алгоритмічні моделі. (Мови, які розпізнаються скінченними автоматами. Машина Тьюрінга. Обчислення числових функцій на машинах Тьюрінга) | лаб. | [1-7] | 4 | 1 тиждень |
| 16 | Тема 16. Поняття про алгоритмічні моделі (Основні вимоги до алгоритмів. Машина Тьюрінга. Обчислення числових функцій на машинах Тьюрінга) | лекція, самостійна робота | [1-7] | 2 4 | 1 тиждень |
| | Модульний контроль 2 | лаб. | - | 2 | під час заняття |