Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 5

ДИСКРЕТНА МАТЕМАТИКА

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*II рік підготовки, осінній семестр*
Обсяг дисципліни	*4,5 кредити*
Семестровий контроль / контрольні заходи	*Екзамен / Модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції: Віталій ЦИГАНОК* *Практичні: Василь КУЛІКОВ*
Розміщення курсу	*Google Classroom*

Київ 2022

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента «Дискретна математика» складено відповідно до освітньої програми підготовки бакалаврів «Комп'ютерні системи і технології спеціального зв'язку» спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: (ЗК 1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК 2) Здатність застосовувати знання у практичних ситуаціях; (ЗК 3) Знання та розуміння предметної області та розуміння професійної діяльності; (СК 1) Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування.

Предметом навчальної дисципліни є дискретні структури та способи їх обробки, включаючи: теорію множин, алгебраїчні структури, теорію алгоритмів та алгоритмічні системи, булеву алгебру та предикати, основи теорії автоматів, теорії графів, основи теорії, діофантові рівняння, основи теорії складності, перешкод , математичні основи побудови асиметричних криптоалгоритмів як теоретична основа для об'єктів вивчення та діяльності, передбачених стандартом вищої освіти України щодо спеціальності 122 Комп'ютерні науки рівня бакалавр.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР 2) Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни курсант повинен володіти освітніми компонентами «Аналітична геометрія та лінійна алгебра» та «Математичний аналіз». Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента є необхідними для подальшого вивчення освітніх компонентів «Проектування та аналіз обчислювальних алгоритмів» , «Системний аналіз» та «Теорія прийняття рішень».

3. Зміст навчальної дисципліни

Семестр 3

Семестровий (кредитний) модуль 1. Дискретна математика

Назва теми
Тема 1. Поняття теорії множин. Операції над множинами.
Тема 2. Відношення.
Тема 3. Основні комбінаторні задачі.
Тема 4. Діаграми Венна. Комбінаторні задачі.
Тема 5. Основні положення теорії цілих чисел. Основна теорема арифметики.
Тема 6. Алгоритм Евкліда знаходження найбільшого спільного дільника чисел.
Тема 7. Рішеннння лінійних діофантових рівнянь із двома невідомими.
Тема 8. Прості числа.
Тема 9. Подання чисел у системі залишкових класів.
Тема 10. Тести Ферма та Рабіна – Міллера для простих чисел.
Тема 11. Основи теорії груп. Поля Галуа.
Тема 12. Поля Галуа, засновані на кільцях відрахувань та кільцях многочленів.

Тема 13. Побудова полів Галуа на основі кілець відрахувань та кілець многочленів.
Тема14. Висловлювання та операції над ними.
Тема15. Булеві алгебри та булеві функції.
Тема 16. Поняття про алгебру Жегалкіна.
Тема17. Предикати. Методи перевірки тотожної істинності формул.
Тема 18. Поняття про мінімізацію логічних функцій. МКР (частина 1).
Тема 19. Графи, різновиди графів та операції над ними.
Тема 20. Матриці графів. Списки суміжності та інцидентів.
Тема 21. Побудова матриць і списків суміжності та інциденцій.
Тема 22. Дерева. Шляхи та цикли графа. Основні дерева.
Тема 23. Методи пошуку в ширину і глибину та їх використання для побудови остовного дерева.
Тема 24. Зважені графи. Алгоритми Крускала та Прима побудови остовних дерев мінімальної ваги.
Тема 25. Практичне використання алгоритмів Крускала та Прима для побудови остовних дерев мінімальної ваги.
Тема 26. Пошук мінімального шляху на зважених графах.
Тема 27. Побудова найкоротших шляхів на зважених графах.
Тема 28. . Мережі. Задача про максимальний потік. Поняття про мережі Петрі
Тема 29. Елементи теорії алгоритмів.
Тема 30. Машина Поста та машина Т’юрінга.
Тема 31. Побудова та аналіз роботи машин Т’юрінга.
Тема 32. Формальні граматики та формальні мови.
Тема 33. Основи абстрактної теорії автоматів.
Тема 34. Побудова графів переходів і виходів за заданими таблицями. Універсальний програмний автомат.
Тема 35. Основи завадостійкого кодування. Аналітичне дослідження кодів. Породжуючі матриці.
Тема 36. Основні поняття теорії складності.
Тема 37. Односпрямовані функції. Функції хешування.
Тема 38. Генератори псевдовипадкових чисел.
Тема 39. Криптографічні алгоритми із відкритими ключами. Дискретний логарифм.
Тема 40. Практичні завдання з шифрування на основі дискретного логарифму.

4. Навчальні матеріали та ресурси

Основна література:

1. Новотарський, М. А. Дискретна математика : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 278 с. URL: https://ela.kpi.ua/handle/123456789/37806.

2. Гавриленко, О. В. Навчальний посібник з дисципліни «Дискретна математика». Частина 1 О. В. Гавриленко, О. М. Клименко, Л. В. Рибачук: КПІ ім. Ігоря Сікорського, 2020. 75 с. URL:https://ela.kpi.ua/handle/123456789/38770.

3. Кублій, Л. І. Комп’ютерна дискретна математика (Частина 1) Л. І. Кублій: КПІ ім. Ігоря Сікорського, 2020. – 165 с.

4. Rosen, Kenneth H. Discrete Mathematics and Its Applications: With Combinatorics and Graph Theory / Mathematics. 2. Computer science —Mathematics. I. Title / McGraw-Hill Companies, 2012, - p.843

5. Нікольский Ю.В., Пасічник В.В., Щербина Ю.М. Дискретна математика. – К.: Видавнича група BHV, 2007. – 368с.

6. Вербіцький Вступ до криптології (Серія “Університетська математика: спеціальні курси”). Львів 1998.- 248с.

7. Ю.В. Боднарчук, Б.В. Олійник. Основи дискретної математики. Київ: Києво-

Могилянська академія — 2009, - 160 с.

Додаткова література:

1. В.І. Андрійчук, М.Я. Комарницький, Ю.Б. Іщук. Вступ до дискретної математики. Львів: Видавничий центр ЛНУ імені Івана Франка, 2003.– 254с..

2. Ю.В. Капітонова, С.Л. Кривий,О.А. Летичевський,Г.М. Луцикий, М.К. Песурін. Основи дискретної математики. Київ: "Наукова думка— 2002.

3. Балога С.І. Дискретна математика. Навчальний посібник. – Ужгород: ПП «АУТДОРШАРК», 2021. – 124 с.

4. Новотарський, М. А. Дискретна математика [Електронний ресурс] : навчальний посібник / КПІ ім. Ігоря Сікорського. – 2020. – 278 с.Ван дер Варден Б. Л. Алгебра: Пер.с нем. М.: Изд-во “Наука”, 1976. 648 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Методика опанування навчальної дисципліни (освітнього компонента) передбачає висвітлення інформації за розділами, темами) про всі навчальні заняття (лекції, практичні) та надання рекомендацій щодо їх засвоєння (наприклад, у формі календарного плану чи деталізованого опису кожного заняття та запланованої роботи).

Самостійна робота курсанта містить інформацію про:

Види самостійної роботи (підготовка до аудиторних занять. Проведення розрахунків за первинними даними, отриманими на практичних заняттях, розв’язок задач, тощо).

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (комп’ютерний практикум)	Лабораторні заняття	СР
Розділ 1. *Дискретна математика*						
Тема 1	**Поняття теорії множин. Операції над множинами.**	**2,5**	**2**			**0,5**
Заняття 1/1	Поняття теорії множин. Операції над множинами. 1. Поняття множини. Основні поняття теорії множин. 2. Операції над множинами. 3. Потужність множини. Властивості потужності скінчених та зліченних множини. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 2	**Відношення.**	**2,5**	**2**			**0,5**
Заняття 2/1	Відношення. 1. Поняття відношення. 2. Відношення тотожності. 3. Рефлексивні та іррефлексивні відношення. 4. Симетричні, транзитивні та антисиметричні відношення. 5. Відношення еквівалентності. Замикання відношень. 6. Відображення і операції. Основна література: [1 – 7].	**2,5**	2			0,5

	Додаткова література: [1 – 4]					
Тема 3	**Основні комбінаторні задачі.**	**2,5**	**2**			**0,5**
Заняття 3/1	Основні комбінаторні задачі. 1. Розміщення і комбінації. 2. Перестановки. 3. Біноміальні коефіцієнти. 4. Породжуючі функції. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 4	**Діаграми Венна. Комбінаторні задачі.**	**2,5**		**2**		**0,5**
Заняття 4/1	Діаграми Венна. Комбінаторні задачі. 1. Вирішення практичних завдань з побудови діаграм Венна. 2. Розв'язування комбінаторних задач на розміщення, комбінації, перестановки. 3. Біном Ньютона. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**		2		0,5
Тема 5	**Основні положення теорії цілих чисел. Основна теорема арифметики.**	**2,5**	**2**			**0,5**
Заняття 5/1	Основні положення теорії цілих чисел. Основна теорема арифметики. 1. Прості числа. 2. Основна теорема. арифметики. Доведення першої частини. 3. Ділення з остачею і найбільший спільний дільник (НСД) двох чисел. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 6	**Алгоритм Евкліда знаходження найбільшого спільного дільника чисел.**	**2,5**	**2**			**0,5**
Заняття 6/1	Алгоритм Евкліда знаходження найбільшого спільного дільника чисел. 1. Доведення другої частини основної теореми арифметики. 2. Алгоритм Евкліда знаходження НСД для чисел. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 7	**Рішення лінійних діофантових рівнянь з двома невідомими.**	**3**		**2**		**1**
Заняття 7/1	Рішення лінійних діофантових рівнянь з двома невідомими. 1. Лінійні діофантові рівняння з двома невідомими. 2. Практичне використання алгоритму Евкліда знаходження НСД. 3. Розширений алгоритм Евкліда для знаходження підходящих коефіцієнтів. 4. Знаходження загального розв'язку діофантових рівнянь. 5. Вирішення практичних завдань. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**		2		1
Тема 8	**Прості числа.**	**2,5**	**2**			**0,5**

Заняття 8/1	Прості числа. 1. Генерація малих простих чисел. 2. Великі прості числа. 3. Перевірка того, чи є число простим. 4. Сильні прості числа. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 9	**Подання чисел в системі залишкових класів.**	**3**	**2**			**1**
Заняття 9/1	Подання чисел в системі залишкових класів. 1. Генерація малих простих чисел. 2. Великі прості числа. 3. Перевірка того, чи є число простим. 4. Сильні прості числа. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**	2			1
Тема 10	**Тести Ферма та Рабіна - Міллера для простих чисел.**	**3**		**2**		**1**
Заняття 10/1	Тести Ферма та Рабіна - Міллера для простих чисел. 1. Тест Ферма для простих чисел. 2. Алгоритм дискретного піднесення до степеня. 3. Оцінювання степенів. 4. Тест Рабіна – Міллера. 5. Вирішення практичних завдань. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**		2		1
Тема 11	**Основи теорії груп. Поля Галуа.**	**3**	**2**			**1**
Заняття 11/1	Основи теорії груп. Поля Галуа. 1. Напівгрупи. 2. Групи. 3. Гомоморфні відображення. 4. Кільця. 5. Області цілісності. 6. Поле. 7. Поле Галуа. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**	2			1
Тема 12	**Поля Галуа, засновані на кільцях відрахувань та кільцях многочленів.**	**2,5**	**2**			**0,5**
Заняття 12/ 1	Поля Галуа, засновані на кільцях відрахувань та кільцях многочленів. 1. Поля Галуа, засновані на кільцях відрахувань. 2. Алгебра поліномів в скінченому полі. 3. Залишкові класи многочленів. 4. Поля Галуа, засновані на кільцях многочленів. 5. Обчислення в полях Галуа. 6. Продукуючі елементи. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 13	**Побудова полів Галуа на основі кілець відрахувань та кілець многочленів.**	**3**		**2**		**1**
Заняття 13/1	Побудова полів Галуа на основі кілець відрахувань та кілець многочленів.	**3**		2		1

	1. Елементи кілець відрахував та кілець многочленів, заданих над полем Галуа. 2. Таблиці додавання та множення в кільцях відрахувань та многочленів. 3. Дільники нуля. Цілісність. Визначення обернених елементів. 4. Обернені елементи для операцій додавання та множення на основі їх матриць. 5. Вирішення практичних завдань. Основна література: [1 – 7]. Додаткова література: [1 – 4]					
Тема 14	**Висловлювання та операції над ними.**	**3**	**2**			**1**
Заняття 14/1	Висловлювання та операції над ними. 1. Висловлювання. 2. Операції диз'юнкції, кон'юнк-ції, імплікації та заперечення. 3. Операції над висловлюваннями. 4. Обчислення висловлювань. 5. Повнота логічних операцій. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**	2			1
Тема 15	**Булеві алгебри та булеві функції.**	**3**	**2**			**1**
Заняття 15/1	Булеві алгебри та булеві функції. 1. Булеві алгебри та булеві функції. 2. Повнота і замкненість. 3. Нормальні форми. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**	2			1
Тема 16	**Поняття про алгебру Жегалкіна.**	**3**		**2**		**1**
Заняття 16/1	Поняття про алгебру Жегалкіна. 1. Диз'юнктивна та кон'юнктивна нормальні форми. 2. Категорії алгебри Жегалкіна. 3. Поліноми Жегалкіна. 4. Вирішення практичних завдань з побудови поліномів Жегалкіна за булевими виразами. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**		2		1
Тема 17	**Предикати. Методи перевірки тотожної істинності формул.**	**2,5**	**2**			**0,5**
Заняття 17/1	Предикати. Методи перевірки тотожної істинності формул. 1. Предикати і квантори. 2. Обчислення предикатів. 3. Методи перевірки тотожної істинності формул Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 18	**Поняття про мінімізацію логічних функцій.**	**3**		**2**		**1**
Заняття 18/1	Поняття про мінімізацію логічних функцій. МКР (частина 1). 1. Мінімізація булевих виразів. 2. Бінарне дерево. 3. Спрощення поліномів Жегалкіна. 4. Карти Карно. 5. МКР (частина 1). Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**		2		1

Тема 19	**Графи, різновиди графів та операції над ними.**	**2,5**	**2**			**0,5**
Заняття 19/1	Графи, різновиди графів та операції над ними. 1. Означення, різновиди графів. 2. Операції над графами. 3. Властивості графів. 4. Ізоморфізм графів. 5. Орієнтовані графи. 6. Джерела та стоки. 7. Шляхи. 8. Орієнтовані шляхи. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 20	**Матриці графів. Списки суміжності та інциденцій.**	**2,5**	**2**			**0,5**
Заняття 20/1	Матриці графів. Списки суміжності та інциденцій. 1. Матриці суміжності. 2. Матриці інциденцій. 3. Списки суміжності. 4. Списки інциденцій. 5. Переходи між способами задання для орієнтованих та неорієнтованих графів. 6. Області застосування варіантів подання графів на комп'ютері. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 21	**Побудова матриць і списків суміжності та інциденцій.**	**2,5**		**2**		**0,5**
Заняття 21/1	Побудова матриць і списків суміжності та інциденцій. 1. Матриці та списки суміжності. 2. Матриці та списки інциденцій. 3. Побудови матриць та списків суміжності та інциденцій за заданим графом. 4. Зображення графа за відомим описом на основі матриць і списків суміжності та інциденцій. 5. Вирішення практичних завдань. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**		2		0,5
Тема 22	**Дерева. Шляхи та цикли графа. Остовні дерева.**	**2,5**	**2**			**0,5**
Заняття 22/1	Дерева. Шляхи та цикли графа. Остовні дерева. 1. Дерева. Означення та властивості. 2. Кореневе дерево. 3. Остовні дерева. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 23	**Методи пошуку в ширину і глибину та їх використання для побудови остовного дерева.**	**2,5**		**2**		**0,5**
Заняття 23/1	Методи пошуку в ширину і глибину та їх використання для побудови остовного дерева. 1. Аналіз роботи алгоритму пошуку в ширину. 2. Аналіз роботи алгоритму пошуку в глибину. 3. Гілки – хорди. 4. Побудова остовного дерева за результатом роботи алгоритму пошуку в ширину. 5. Вирішення практичних завдань	**2,5**		2		0,5

	Основна література: [1 – 7]. Додаткова література: [1 – 4]					
Тема 24	**Зважені графи. Алгоритми Крускала та Пріма побудови остовних дерев мінімальної ваги.**	**2,5**	**2**			**0,5**
Заняття 24/1	Зважені графи. Алгоритми Крускала та Пріма побудови остовних дерев мінімальної ваги. 1. Зважені графи. 2. Мінімальні остовні дерева. 3. Алгоритм Крускала та алгоритм Пріма побудови остовних дерев мінімальної ваги Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 25	**Практичне використання алгоритмів Крускала та Пріма для побудови остовних дерев мінімальної ваги.**	**2,5**		**2**		**0,5**
Заняття 25/1	Практичне використання алгоритмів Крускала та Пріма для побудови остовних дерев мінімальної ваги. 1. Аналіз роботи алгоритмів Крускала та Пріма для побудови остовних дерев мінімальної ваги. 2. Практична побудова остовних дерев мінімальної ваги на основі алгоритмів Крускала та Пріма. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**		2		0,5
Тема 26	**Пошук мінімального шляху на зважених графах.**	**2,5**	**2**			**0,5**
Заняття 26/1	Пошук мінімального шляху на зважених графах. 1. Довжина шляху. 2. Метод Флойда. 3. Алгоритм Дейкстри пошуку найкоротшого шляху. 4. Дерево найкоротших шляхів. 5. Метод пошуку в ширину для знаходження найкоротших шляхів Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 27	**Побудова найкоротших шляхів на зважених графах.**	**2,5**		**2**		**0,5**
Заняття 27/1	Побудова найкоротших шляхів на зважених графах. 1. Аналіз роботи алгоритму Дейкстри. 2. Практична побудова найкоротших шляхів на основі алгоритму Дейкстри. 3. Побудова дерева найкоротших шляхів. 4. Метод пошуку в ширину для побудови найкоротших шляхів Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**		2		0,5
Тема 28	**Мережі. Задача про максимальний потік. Поняття про мережі Петрі.**	**2,5**	**2**			**0,5**
Заняття 28/1	Мережі. Задача про максимальний потік. Поняття про мережі Петрі. 1. Мережі. 2. Основні поняття. 3. Задача про максимальний потік. 4. Розмічена мережа.	**2,5**	2			0,5

	5. Основні поняття мережі Петрі. 6. Побудова і аналіз мережі Петрі. Основна література: [1 – 7]. Додаткова література: [1 – 4]					
Тема 29	**Елементи теорії алгоритмів.**	**2,5**	**2**			**0,5**
Заняття 29/1	Елементи теорії алгоритмів. 1. Інтуїтивне поняття алгоритму. 2. Обчислювані і частково рекурсивні функції. 3. Теза Черча. 4. Алгоритмічні проблеми. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 30	**Машина Поста та машина Т'юрінга.**	**2,5**	**2**			**0,5**
Заняття 30/1	Машина Поста та машина Т'юрінга. 1. Машина Поста. 2. Машина Т'юрінга. 3. Словесне представлення машини Т'юрінга. 4. Алгоритмічно розв'язні і нерозв'язні проблеми Основна література**:** [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 31	**Побудова та аналіз роботи машин Т'юрінга.**	**2,5**		**2**		**0,5**
Заняття 31/1	Побудова та аналіз роботи машин Т'юрінга. 1. Аналіз структури машини Т'юрінга. 2. Ілюстрація роботи машини Т'юрінга. 3. Аналіз та словесний опис роботи машини Т'юрінга. 4. Вирішення практичних завдань. Основна література**:** [1 – 7]. Додаткова література: [1 – 4]	**2,5**		2		0,5
Тема 32	**Формальні граматики і формальні мови**	**2,5**	**2**			**0,5**
Заняття 32/1	Формальні граматики і формальні мови. 1. Регулярні граматики і їх властивості. 2. Означення формальної граматики. 3. Класифікація граматик. 4. Мови, семантика формальних мов Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 33	**Основи абстрактної теорії автоматів.**	**2,5**	**2**			**0,5**
Заняття 33/1	Основи абстрактної теорії автоматів. 1. Автомати, як узагальнення машини Т'юрінга. 2. Автомати Мілі. 3. Автомати Мура. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 34	**Побудова графів переходів та виходів за заданими таблицями. Універсальний програмний автомат.**	**2,5**		**2**		**0,5**
Заняття 34/1	Побудова графів переходів та виходів за заданими таблицями. Універсальний програмний автомат. 1. Вузли та гілки (ребра) графів переходів та виходів. 2. Таблиці та графи переходів і виходів. 3. Вирішення практичних задач побудови графів переходів та виходів за заданими таблицями переходів та виходів. 4. Універсальний програмний автомат.	**2,5**		2		0,5

	Основна література: [1 – 7]. Додаткова література: [1 – 4]					
Тема 35	**Основи завадостійкого кодування. Аналітичне дослідження кодів. Породжуючі матриці.**	**2,5**	**2**			**0,5**
Заняття 35/1	Основи завадостійкого кодування. Аналітичне дослідження кодів. Породжуючі матриці. 1. Історія кодування, що контролює помилки. 2. Основні поняття. 3. Найпростіші коди. 4. Структура лінійних блокових кодів. 5. Лінійні коди над GF(2). 6. Матричний опис лінійних блокових кодів. 7. Операції у векторному просторі. 8. Ортогональні матриці і виправлення помилок для кодів Хемінга. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 36	**Основні поняття теорії складності.**	**2,5**	**2**			**0,5**
Заняття 36/1	Основні поняття теорії складності. 1. Складність масових задач. 2. Вимір часу виконання програм. 3. Асимптотичні співвідношення. 4. Обмеженість показника ступеня росту. 5. Поняття складності алгоритму. 6. Класи складності проблем Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 37	**Односпрямовані функції. Функції хешування.**	**2,5**	**2**			**0,5**
Заняття 37/1	Односпрямовані функції. Функції хешування. 1. Поняття про односпрямовані функції. 2. Хеш-функції та їх види. 3. Поняття колізії. 4. Розкриття в день народження проти односпрямованих хеш-функцій. Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 38	**Генератори псевдовипадкових чисел.**	**2,5**	**2**			**0,5**
Заняття 38/1	Генератори псевдовипадкових чисел. 1. Методи генерування псевдовипадкових чисел. 2. Лінійні конгруентні генератори. 3. Регістри зсуву. 4. Потокові шифри Основна література: [1 – 7]. Додаткова література: [1 – 4]	**2,5**	2			0,5
Тема 39	**Криптографічні алгоритми з відкритими ключами. Дискретний логарифм.**	**2,5**	**2**			**0,5**
Заняття 39/1	Криптографічні алгоритми з відкритими ключами. Дискретний логарифм. 1. Алгоритми з відкритими ключами. 2. Шифрування RSA. 3. Апаратні реалізації RSA та швидкість RSA. 4. Безпека RSA. 5. Розкриття загального модуля RSA 6. Розкриття малого показника шифрування та дешифрування RSA. Основна література: [1 – 7].	**2,5**	2			0,5

	Додаткова література: [1 – 4]					
Тема 40	**Практичні завдання з шифрування на основі дискретного логарифму.**	**3**		**2**		**1**
Заняття 40/1	Практичні завдання з шифрування на основі дискретного логарифму. МКР (частина 2). 1. Зашифрування та розшифрування на основі алгоритму RSA. 2. МКР (частина 2). Основна література: [1 – 7]. Додаткова література: [1 – 4]	**3**		2		1
Разом за розділом 1		**105**	**54**	**26**		**25**
Екзамен		30				30
Всього годин		**135**	**54**	**26**		**55**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до екзамену.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1	Тема 1. Поняття теорії множин. Операції над множинами. 1. Поняття множини. Основні поняття теорії множин. 2. Операції над множинами. 3. Потужність множини. Властивості потужності скінчених та зліченних множини. 4. Довести наслідок з теореми 1.6. 5. Навести приклади скінчених, зліченних множин та множин потужності континуум Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
2	Тема 2. Відношення. 1. Поняття відношення. 2. Відношення тотожності. 3. Рефлексивні та іррефлексивні відношення. 4. Симетричні, транзитивні та антисиметричні відношення. 5. Відношення еквівалентності. Замикання відношень. 6. Відображення і операції. 7. Навести приклади відношень тотожності, еквівалентності, рефлексивних та транзитивних відношень. 8. Навести приклади взаємно однозначними відображень та довести, що ці відображення дійсно є взаємно однозначними. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
3	Тема 3. Основні комбінаторні задачі. 1. Розміщення і комбінації 2. Перестановки 3. Біноміальні коефіцієнти 4. Породжуючі функції 5. Принцип включення та виключення. Визначення кількості чисел що не діляться на задане число множників. 6. Означення та властивості чисел Фібоначчі Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5

4	Тема 4. Діаграми Венна. Комбінаторні задачі 1. Вирішення практичних завдань з побудови діаграм Венна 2. Розв'язування комбінаторних задач на розміщення, комбінації, перестановки. 3. Біном Ньютона 4. Властивості біноміальних коефіцієнтів. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
5	Тема 5. Основні положення теорії цілих чисел. Основна теорема арифметики 1. Прості числа 2. Основна теорема арифметики. Доведення першої частини 3. Ділення з остачею і найбільший спільний дільник (НДС) двох чисел Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
6	Тема 6. Алгоритм Евкліда знаходження найбільшого спільного дільника чисел. 1. Доведення другої частини основної теореми арифметики. 2. Алгоритм Евкліда знаходження НСД для чисел. 3. Сформувати загальну структуру (схему) алгоритму знаходження НСД. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
7	Тема 7. Рішення лінійних діофантових рівнянь з двома невідомими. 1. Лінійні діофантові рівняння з двома невідомими. 2. Практичне використання алгоритму Евкліда знаходження НСД. 3. Розширений алгоритм Евкліда для знаходження підходящих коефіцієнтів. 4. Знаходження загального розв'язку діофантових рівнянь. 5. Вирішення практичних завдань. 6. Використання алгоритму Евкліда при дискретному діленні. 7. Поняття про китайську теорему про залишки. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
8	Тема 8. Прості числа. 1. Генерація малих простих чисел. 2. Великі прості числа. 3. Перевірка того, чи є число простим. 4. Сильні прості числа. 5. Сформувати загальну структуру (схему) алгоритму решета Ератосфена знаходження малих простих чисел. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
9	Тема 9. Подання чисел в системі залишкових класів. 1. Модулі. 2. Модулярна арифметика. 3. Використання модульних операцій при вирішенні практичних задач. 4. Тест Ферма простоти чисел. 5. Числа Кармайкла. 6. Сформувати загальну структуру (схему) алгоритму дискретного піднесення до степеня Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
10	Тема 10. Тести Ферма та Рабіна - Міллера для простих чисел 1. Тест Ферма для простих чисел. 2. Алгоритм дискретного піднесення до степеня. 3. Оцінювання степенів. 4. Тест Рабіна – Міллера. 5. Вирішення практичних завдань. 6. Знайти значення виразу $a^b \pmod m$ для вибраних a, b і m. Основна література: [1 – 7].	1

	Додаткова література: [1 – 4]	
11	Тема 11. Основи теорії груп. Поля Галуа. 1. Напівгрупи. 2. Групи. 3. Гомоморфні відображення. 4. Кільця. 5. Області цілісності. 6. Поле. 7. Поле Галуа. 8. Визначити якими алгебраїчними структурами є множина всіх парних чисел та всіх симетричних матриць. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
12	Тема 12. Поля Галуа, засновані на кільцях відрахувань та кільцях многочленів. 1. Поля Галуа, засновані на кільцях відрахувань. 2. Алгебра поліномів в скінченому полі. 3. Залишкові класи многочленів. 4. Поля Галуа, засновані на кільцях многочленів. 5. Обчислення в полях Галуа. 6. Продукуючі елементи. 7. Наявність оберненого елементу в кільцях відрахувань, що не є цілісними. 8. Приклади обернених елементів в кільцях відрахувань та кільцях многочленів, що не є цілісними. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
13	Тема 13. Побудова полів Галуа на основі кілець відрахувань та кілець многочленів. 1. Елементи кілець відрахував та кілець многочленів, заданих над полем Галуа. 2. Таблиці додавання та множення в кільцях відрахувань та многочленів. 3. Дільники нуля. Цілісність. Визначення обернених елементів. 4. Обернені елементи для операцій додавання та множення на основі їх матриць. 5. Вирішення практичних завдань. 6. Вказати елементи кільця многочленів по модулю приведеного многочлена $p(x)=x^3+x^2+1$, заданого над полем GF(2). Побудувати таблицю додавання та множення для елементів кільця. Визначити, чи є дане кільце полем. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
14	Тема 14. Висловлювання та операції над ними. 1. Висловлювання. 2. Операції диз'юнкції, кон'юнкції, імплікації та заперечення 3. Операції над висловлюваннями. 4. Обчислення висловлювань. 5. Повнота логічних операцій. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
15	Тема 15. Булеві алгебри та булеві функції 1. Булеві алгебри та булеві функції. 2. Повнота і замкненість. 3. Нормальні форми 4. Множини та операції над ними як булева алгебра. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
16	Тема 16. Поняття про алгебру Жегалкіна 1. Диз'юнктивна та кон'юнктивна нормальні форми. 2. Категорії алгебри Жегалкіна. 3. Поліноми Жегалкіна.	1

	4. Вирішення практичних завдань з побудови поліномів Жегалкіна за булевими виразами. 5. Функціональна повнота системи операцій алгебри Жегалкіна Основна література: [1 – 7]. Додаткова література: [1 – 4]	
17	Тема 17. Предикати. Методи перевірки тотожної істинності формул 1. Предикати і квантори. 2. Обчислення предикатів. 3. Методи перевірки тотожної істинності формул 4. Методи нескінченого спуску та математичної індукції Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
18	Тема 18. Поняття про мінімізацію логічних функцій. 1. Мінімізація булевих виразів. 2. Бінарне дерево. 3. Спрощення поліномів Жегалкіна. 4. Карти Карно. 5. Повторити аксіоми булевої алгебри та вказати ті із них, на основі яких можливе спрощення булевих виразів. 6. Навести приклад булевого виразу однієї змінної, що містить не менше двох операцій булевої алгебри та спростити його методом Куайна. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
19	Тема 19. Графи, різновиди графів та операції над ними 1. Означення, різновиди графів. 2. Операції над графами. 3. Властивості графів. 4. Ізоморфізм графів. 5. Орієнтовані графи. 6. Джерела та стоки. 7. Шляхи. 8. Орієнтовані шляхи. 9. Нескінчені графи. 10. Повні та повні дводольні графи. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
20	Тема 20. Матриці графів. Списки суміжності та інциденцій. 1. Матриці суміжності. 2. Матриці інциденцій. 3. Списки суміжності. 4. Списки інциденцій. 5. Переходи між способами задання для орієнтованих та неорієнтованих графів. 6. Області застосування варіантів подання графів на комп'ютері. **7.** Побудова матриць суміжності та інциденцій і списків суміжності за списками інциденцій. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
21	Тема 21. Побудова матриць і списків суміжності та інциденцій. 1. Матриці та списки суміжності. 2. Матриці та списки інциденцій. 3. Побудови матриць та списків суміжності та інциденцій за заданим графом. 4. Зображення графа за відомим описом на основі матриць і списків суміжності та інциденцій. 5. Вирішення практичних завдань. 6. Побудова списків суміжності та інциденцій за матрицею суміжності. 7. Побудова матриці суміжності та списків суміжності і інциденцій за матрицею інциденцій.	0,5

	Основна література: [1 – 7]. Додаткова література: [1 – 4]	
22	Тема 22. Дерева. Шляхи та цикли графа. Остовні дерева. 1. Дерева. 2. Означення та властивості. 3. Кореневе дерево. 4. Остовні дерева. 5. Вирішити завдання та вправи, наведені в лекції. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
23	Тема 23. Методи пошуку в ширину і глибину та їх використання для побудови остовного дерева.. 1. Аналіз роботи алгоритму пошуку в ширину. 2. Гілки – хорди. 3. Побудова остовного дерева за результатом роботи алгоритму пошуку в ширину. 4. Вирішення практичних завдань 5. Для заданого графа із заданої вершини методом пошуку в ширину побудувати остовне дерево. Вказати гілки-хорди. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
24	Тема 24. Зважені графи. Алгоритми Крускала та Пріма побудови остовних дерев мінімальної ваги 1. Зважені графи. 2. Мінімальні остовні дерева. 3. Алгоритм Крускала та алгоритм Пріма побудови остовних дерев мінімальної ваги 4. Розробити схеми алгоритмів Крускала та Пріма побудови остовних дерев мінімальної ваги Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
25	Тема 25. Практичне використання алгоритмів Крускала та Пріма для побудови остовних дерев мінімальної ваги. 1. Аналіз роботи алгоритмів Крускала та Пріма для побудови остовних дерев мінімальної ваги. 2. Практична побудова остовних дерев мінімальної ваги на основі алгоритмів Крускала та Пріма. 3. Сформувати загальну структуру (схему) алгоритму методу Пріма побудови остовного дерева мінімальної ваги. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
26	Тема 26. Пошук мінімального шляху на зважених графах. 1. Довжина шляху. 2. Метод Флойда. 3. Алгоритм Дейкстри пошуку найкоротшого шляху. 4. Дерево найкоротших шляхів. 5. Метод пошуку в ширину для знаходження найкоротших шляхів. 6. Сформувати загальну структуру (схему) алгоритму методу Дейкстри пошуку найкоротшого шляху. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
27	Тема 27. Побудова найкоротших шляхів на зважених графах 1. Аналіз роботи алгоритму Дейкстри. 2. Практична побудова найкоротших шляхів на основі алгоритму Дейкстри. 3. Побудова дерева найкоротших шляхів. 4. Метод пошуку в ширину для побудови найкоротших шляхів	0,5

	5. Сформувати загальну структуру (схему) алгоритму методу пошуку в ширину знаходження найкоротших шляхів від заданої вершини до всіх інших вершин. Основна література: [1 – 7]. Додаткова література: [1 – 4]	
28	Тема 28. Мережі. Задача про максимальний потік. Поняття про мережі Петрі 1. Мережі. 2. Основні поняття. 3. Задача про максимальний потік. 4. Розмічена мережа. 5. Основні поняття мережі Петрі. 6. Побудова і аналіз мережі Петрі. 7. Знайти максимальний потік та мінімальний перетин для обраного графа та ваг гілок. 8. Навести приклади наступних мереж Петрі: живої, безпечної, обмеженої, консервативної. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
29	Тема 29. Елементи теорії алгоритмів. 1. Інтуїтивне поняття алгоритму. 2. Обчислювані і частково рекурсивні функції. 3. Теза Черча. 4. Алгоритмічні проблеми. 5. Довести, що функція $f(x,y) = x^2y$ є примітивно рекурсивною. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
30	Тема 30. Машина Поста та машина Т'юрінга. 1. Машина Поста. 2. Машина Т'юрінга. 3. Словесне представлення машини Т'юрінга. 4. Алгоритмічно розв'язні і нерозв'язні проблеми. 5. Визначити, які з типів наказів для машини Поста використовуються в сучасних мовах програмування. 6. Визначити різницю між машинами Поста і машинами Т'юрінга і що для них є спільним. Основна література**:** [1 – 7]. Додаткова література: [1 – 4]	0,5
31	Тема 31. Побудова та аналіз роботи машин Т'юрінга. 1. Аналіз структури машини Т'юрінга. 2. Ілюстрація роботи машини Т'юрінга. 3. Аналіз та словесний опис роботи машини Т'юрінга. 4. Вирішення практичних завдань. 5. Алгоритмічні проблеми. Теза Т'юрінга. 6. Приклади алгоритмічно розв'язних та нерозв'язних проблем. Основна література**:** [1 – 7]. Додаткова література: [1 – 4]	0,5
32	Тема 32. Формальні граматики і формальні мови. 1. Регулярні граматики і їх властивості. 2. Означення формальної граматики. 3. Класифікація граматик. 4. Мови, семантика формальних мов 5. Визначити відмінність між бс-мовою та кв-мовою. 7. Визначити умови, при виконанні яких правильними будуть слова, побудовані на основі граматики, що породжує слова. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
33	Тема 33. Основи абстрактної теорії автоматів. 1. Автомати, як узагальнення машини Т'юрінга.	0,5

	2. Автомати Мілі. 3. Автомати Мура. 4. Визначити спільні характеристики автоматів та машини Т'юрінга. 5. Вказати різницю між автоматами Мілі та автоматами Мура. Основна література: [1 – 7]. Додаткова література: [1 – 4]	
34	Тема 34. Побудова графів переходів та виходів за заданими таблицями. Універсальний програмний автомат. 1. Вузли та гілки (ребра) графів переходів та виходів. 2. Таблиці та графи переходів і виходів. 3. Вирішення практичних задач побудови графів переходів та виходів за заданими таблицями переходів та виходів. 4. Універсальний програмний автомат. 5. Визначити спільні характеристики та відмінності між універсальним програмним автоматом та алгоритмічною системою Поста. 6. Вказати в чому полягає алгоритмічна універсальність будь-якого цифрового автомата. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
35	Тема 35. Основи завадостійкого кодування. Аналітичне дослідження кодів. Породжуючі матриці. 1. Історія кодування, що контролює помилки. 2. Основні поняття. 3. Найпростіші коди. 4. Структура лінійних блокових кодів. 5. Лінійні коди над GF(2). 6. Матричний опис лінійних блокових кодів. 7. Операції у векторному просторі. 8. Ортогональні матриці і виправлення помилок для кодів Хемінга. 9. Сформувати загальну структуру (блок-схему) алгоритму завадостійкого кодування на основі коду Хемінга (7,4). Визначити число операцій додавання, множення, ділення та умовних операторів при кодуванні одного інформаційного блоку. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
36	Тема 36. Основні поняття теорії складності. 1. Складність масових задач. 2. Вимір часу виконання програм. 3. Асимптотичні співвідношення. 4. Обмеженість показника ступеня росту. 5. Поняття складності алгоритму. 6. Класи складності проблем 7. Визначити складність алгоритму методу Крускала знаходження остовного дерева мінімальної ваги. 8. Визначити складність алгоритму сортування методом "бульбашки". Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
37	Тема 37. Односпрямовані функції. Функції хешування 1. Поняття про односпрямовані функції. 2. Хеш-функції та їх види. 3. Поняття колізії. 4. Розкриття в день народження проти односпрямованих хеш-функцій. 5. Стандарти цифрового підпису. Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
38	Тема 38. Генератори псевдовипадкових чисел 1. Методи генерування псевдовипадкових чисел.	0,5

	2. Лінійні конгруентні генератори. 3. Регістри зсуву. 4. Потокові шифри 5. Оцінити обчислювальну складність алгоритму для лінійного конгруентного генератора Основна література: [1 – 7]. Додаткова література: [1 – 4]	
39	Тема 39. Криптографічні алгоритми з відкритими ключами. Дискретний логарифм 1. Алгоритми з відкритими ключами. 2. Шифрування RSA. 3. Апаратні реалізації RSA та швидкість RSA. 4. Безпека RSA. 5. Розкриття загального модуля RSA 6. Розкриття малого показника шифрування та дешифрування RSA. 7. Методи факторизації криптомодуля RSA Основна література: [1 – 7]. Додаткова література: [1 – 4]	0,5
40	Тема 40. Практичні завдання з шифрування на основі дискретного логарифму. 1. Зашифрування та розшифрування на основі алгоритму RSA. Основна література: [1 – 7]. Додаткова література: [1 – 4]	1
	Підготовка до екзамену	30
Всього годин		55

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

У ході навчальних занять використовуються наступні методи навчання:

- усне викладання матеріалу;
- обговорення учбового матеріалу;
- практична робота в класі з застосуванням комп'ютерної техніки;
- самостійна робота під керівництвом викладача.

Відвідування занять є обов'язковим. Відсутність на занять з будь яких причин не вважається поважною причиною невиконання відповідного завдання для самостійного виконання.

Під час занять всі мобільні телефони мають бути переведені на беззвучний режим роботи. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Електронні пристрої, включаючи мобільні телефони та ноутбуки можна використовувати лише за умови виробничої необхідності в них (за погодженням з викладачем).

Всі робочі оголошення та необхідні матеріали курсу будуть розміщуватися на вказаній сторінці. Очікується, що курсанти перевірятимуть свою електронну пошту і сторінку навчальної дисципліни в Google Class та реагуватимуть своєчасно. Результат виконання завдань для самостійного виконання також мають бути викладені на сторінці Google Class у форматі, який буде вказаний викладачем. Також через сторінку Google Class курсанти можуть надіслати у вигляді відкритого чи приватного листа викладачу питання, що виникли під час виконання завдань, або інші питання стосовно курсу, який вивчається.

Завдання для самостійного виконання мають бути виконані і надіслані на перевірку виключно до дати, яка вказана як кінцевий термін її виконання. Завдання надіслані після вказаного строку можуть але не зобов'язані бути перевірені та оцінені викладачем.

Кожний курсант зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства – це плагіат. Використання будь-якої інформації (текст,

фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора. До курсантів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані різні дисциплінарні заходи.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даного кредитного модуля можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальні матеріали та ресурси, зазначена у розділі 4 цієї робочої програми навчальної дисципліни (силабусі) є відкритими, не містять відомостей з обмеженим доступом і можуть бути оприлюднені з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання здобувачів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів (студентів) в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою

Кількість балів Рейтингові бали, RD	Оцінка за університетською шкалою
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше ніж 60	Незадовільно

1. Рейтинг курсанта з навчальної дисципліни “Дискретна математика” визначається балами за:

1) 4 відповіді на практичних заняттях;
2) модульна контрольна робота (2 частини);
3) відповідь на екзамені.

При цьому враховуються заохочувальні (зі знаком “плюс”) та штрафні (зі знаком “мінус”) бали.

2. Критерії нарахування балів.

2.1 Відповіді на практичних заняття оцінюються 5 балами кожне:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації) – 5 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 4 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 3 бали;

– “незадовільно” – відповідь не відповідає вимогам до “задовільно” – 0 балів.

Тобто максимум 4*5 = 20 балів.

2.2 Модульний контроль передбачає 2 частини, кожна з яких складається з 4-х практичних завдань. Кожне завдання оцінюється 5 балами за такими критеріями:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації), хід рішення – правильний, отримано правильний результат, надані відповідні обґрунтування та особистий погляд – 5 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними невідповідностями, допускається помилка в розрахунках, хід рішення – правильний – 4 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 3 бали;

– “незадовільно” – незадовільна відповідь – 0 балів.

Тобто максимум 2*4*5 = 40 балів.

2.3 Відповідь на екзамені оцінюється **40 балами**. Екзаменаційний білет складається з трьох запитань (одне – теоретичне, два – практичних) переліку, що наданий нижче.

Теоретичне питання оцінюється 10 балами за такими критеріями:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 9…10 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними невідповідностями – 8 балів;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 6 - 7 балів;

– “незадовільно” – незадовільна відповідь – 0 балів.

Кожне практичне питання оцінюється 15 балами за такими критеріями:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 14 … 15 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації) з незначними неточностями – 11 … 13 балів;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) з деякими помилками – 9 … 10 балів;

– “незадовільно” – незадовільна відповідь – 0 балів.

2.3. Заохочувальні бали нараховуються за виконання творчих робіт у межах навчальної дисципліни (наприклад, програмна реалізація методів, що вивчаються в рамках дисципліни, оригінальне виконання завдань на практичних заняттях).

Тобто, максимум (+1)*5 **= + 6 балів.**

– штрафні бали нараховуються за несвоєчасне виконання завдань, що виносяться на практичні заняття.

Тобто, загалом (–1)*5 = **– 6 балів.**

$$RD = 100 = \sum_{k} r_K + \sum_{2} r_M + \sum r_E + \sum r_{Ш}$$

3. Календарний контроль (атестація) проводиться згідно Графіка-календаря освітнього процесу ІСЗЗІ КПІ ім. Ігоря Сікорського на навчальний рік.

Умовою атестації є отримання не менше 50% від кількості балів, яку курсант може отримати на час її проведення.

4. Умовою допуску до екзамену є: виконання усіх завдань, що передбачені робочою програмою навчальної дисципліни та отримання рейтингу не менше **36 балів.**

Критерії оцінювання семестрових контрольних заходів

Підсумковий контроль представлений екзаменом. Екзамен проводиться в формі усної або письмової відповіді по білетах. Знання курсантів оцінюються за п’ятибальною системою: “*Відмінно*”, “*Дуже добре*”, “*Добре*”, “*Задовільно*”, “*Незадовільно*” із наступним перерахуванням в бали РСО згідно таблиці:

Критерії оцінювання	$r_{кр}$

Оцінка “Відмінно” ставиться курсанту, який показав глибоке знання предмету, повно і чітко відповів на питання в об'ємі програми, правильно і акуратно оформив відповідь.	38 … 40
Оцінка “Дуже добре” ставиться у тому випадку, коли виповнено всі перелічені вище вимоги, але по деяких показниках мають місце несуттєві недоліки непринципового характеру.	34 … 37
Оцінка “Добре” ставиться у тому випадку, коли відповідь загалом є правильною, але по ряду показників мають місце недоліки непринципового характеру.	30 … 33
Оцінка “Задовільно” ставиться, коли відповідь загалом є правильною і по деяких показниках мають місце недоліки принципового характеру	24 … 29
В інших випадках ставиться оцінка “Незадовільно”	$r_{кр} < 24$

Для отримання курсантом відповідних оцінок його рейтингова оцінка RD переводиться згідно з таблицею:

Рейтингові бали, RD	Оцінка за університетською шкалою
95 – 100	Відмінно
85 – 94	Дуже добре
75 – 84	Добре
65 – 74	Задовільно
60 – 64	Достатньо
Менше ніж 60	Незадовільно

9. Додаткова інформація з навчальної дисципліни

Перелік питань, які виносяться на семестровий контроль (МКР та екзамен).

1. Поняття множини. Основні поняття теорії множин. Операції над множинами. (Теоретичне і практичне).
2. Потужність множини. Властивості потужності скінчених та зліченних множин. (Теоретичне).
3. Поняття відношення. Типи відношень. Відображення. (Теоретичне).
4. Основні комбінаторні задачі: розміщення, перестановки, комбінації. (Теоретичне і практичне).
5. Біном Ньютона. Біноміальні коефіцієнти та їх властивості. (Теоретичне).
6. Основні положення теорії цілих чисел. Прості числа. Теорема Евкліда. (Теоретичне)
7. Основна теорема арифметики. Існування розкладання на прості множники. (Теоретичне).
8. Основна теорема арифметики. Єдиність розкладання на прості множники. (Теоретичне).
9. Ділення з остачею, найбільший спільний дільник (НСД) двох чисел. Взаємно прості числа та їх властивості. (Теоретичне і практичне)
10. Алгоритм Евкліда знаходження найбільшого спільного дільника чисел. (Теоретичне і практичне)
11. Лінійні діофантові рівняння з двома невідомими та їх загальний розв’язок. (Практичне)
12. Розширений алгоритм Евкліда для знаходження підходящих коефіцієнтів. (Практичне)
13. Прості числа. Генерація малих простих чисел. Великі прості числа. Поняття про сильні прості числа. (Теоретичне і практичне).
14. Решето Ератосфена для генерації малих простих чисел. (Теоретичне і практичне)
15. Подання чисел в системі залишкових класів. Модулі. Модулярна арифметика. Модулярні функції. (Теоретичне і практичне).
16. Тест Ферма простоти чисел. Числа Кармайкла. (Теоретичне і практичне).

17. Тест Рабіна - Міллера для простих чисел. (Теоретичне і практичне).
18. Напівгрупи. Групи. (Теоретичне).
19. Кільця. Області цілісності. Поле. Поле Галуа. (Теоретичне).
20. Поля Галуа, засновані на кільцях відрахувань. (Теоретичне).
21. Алгебра поліномів в скінченому полі. (Теоретичне).
22. Поля Галуа, засновані на кільцях многочленів. (Теоретичне).
23. Продукуючі елементи в полях Галуа та їх використання. (Теоретичне і практичне)
24. Таблиці додавання та множення в кільцях відрахувань. Дільники нуля. Цілісність. Визначення обернених елементів. (Практичне).
25. Таблиці додавання та множення в кільцях многочленів. Дільники нуля. Цілісність. Визначення обернених елементів. (Теоретичне і практичне).
26. Висловлювання. Операції над висловлюваннями: диз'юнкція, кон'юнкція, імплікація та заперечення. Обчислення висловлювань. (Теоретичне і практичне).
27. Булеві алгебри та булеві функції. Повнота і замкненість. Нормальні форми. (Теоретичне).
28. Поняття про алгебру Жегалкіна. Категорії алгебри Жегалкіна. Поліноми Жегалкіна. (Теоретичне і практичне).
29. Предикати і квантори. Обчислення предикатів. (Теоретичне і практичне).
30. Методи перевірки тотожної істинності формул. (Теоретичне і практичне).
31. Метод математичної індукції доведення нескінченого числа тверджень. (Теоретичне і практичне).
32. Мінімізація булевих виразів: бінарне дерево, спрощення поліномів Жегалкіна, карти Карно. (Теоретичне і практичне).
33. Графи, різновиди графів та операції над ними. (Теоретичне).
34. Орієнтовані графи. Джерела та стоки. Шляхи. Орієнтовані шляхи. (Теоретичне).
35. Матриці та списки суміжності для графів. (Теоретичне і практичне).
36. Матриці та списки інциденцій для графів. (Теоретичне і практичне).
37. Дерева. Означення та властивості. Кореневе дерево. Остовні дерева. (Теоретичне і практичне).
38. Методи пошуку в ширину та його використання для побудови остовного дерева. (Практичне).
39. Метод пошуку в глибину та його використання для побудови остовного дерева. (Практичне).
40. Зважені графи. Вага дерева. Мінімальне остовне дерево. (Теоретичне).
41. Алгоритми Крускала побудови остовних дерев мінімальної ваги. (Практичне).
42. Алгоритм Пріма побудови остовних дерев мінімальної ваги. (Практичне).
43. Зважені графи. Довжина шляху на зважених графах. Мінімальний шлях. (Теоретичне і практичне).
44. Алгоритм Дейкстри пошуку найкоротшого шляху на зважених графах. Дерево найкоротших шляхів. (Практичне).
45. Метод пошуку в ширину для знаходження найкоротших шляхів на зважених графах. (Теоретичне і практичне).
46. Мережі. Основні поняття. Задача про максимальний потік. (Теоретичне).
47. Розмічена мережа. Основні поняття мережі Петрі. (Теоретичне).
48. Елементи теорії алгоритмів. Інтуїтивне поняття алгоритму. (Теоретичне).
49. Алгоритмічна система на основі обчислювальних та частково рекурсивних функцій. Теза Черча. (Теоретичне).
50. Машина Поста. (Теоретичне і практичне).
51. Машина Т'юрінга. (Теоретичне і практичне).
52. Поняття алгоритмічно розв'язних і нерозв'язних проблем. (Теоретичне).
53. Формальні граматики і формальні мови. (Теоретичне).

54. Автомати, як узагальнення машини Т’юрінга. Автомати Мілі. Автомати Мура. (Теоретичне і практичне).
55. Завадостійке кодування. Основні поняття. Найпростіші коди. (Теоретичне).
56. Кодування, що контролює помилки. Лінійні блокові коди. Суміжні класи. Породжуюча та ортогональна матриці. (Теоретичне і практичне).
57. Коди Хемінга. Виправлення помилок для кодів Хемінга. (Теоретичне).
58. Основні поняття теорії складності. Класи складності проблем. (Теоретичне).
59. Алгоритм дискретного піднесення до степеня і оцінка його складності. (Теоретичне і практичне).
60. Оцінка складності алгоритму Евкліда обчислення НСД. (Теоретичне).
61. Односпрямовані функції. Функції хешування та їх види. (Теоретичне).
62. Хеш-функції. Поняття колізії. Розкриття в день народження проти односпрямованих хеш-функцій. (Теоретичне).
63. Генератори псевдовипадкових чисел. Методи генерування псевдовипадкових чисел. Лінійні конгруентні генератори. Регістри зсуву. (Теоретичне).
64. Квазіодноспрямовані функції. Дискретний логарифм. Зашифрування та розшифрування на основі алгоритму RSA. (Теоретичне і практичне).