Національний технічний університет України «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»	Навчально-науковий фізико-технічний інститут Кафедра математичних методів захисту інформації

ДИСКРЕТНА МАТЕМАТИКА. ЧАСТИНА 2 (ЗО 12.2)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Обов'язкова (нормативна) (цикл загальної підготовки)*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 курс, весняний семестр*
Обсяг дисципліни	*Загальна кількість: 3 кредити ЄКТС / 90 годин* *Лекційних занять: 36 годин* *Практичних занять: 18 годин* *Самостійна робота студентів: 36 годин*
Семестровий контроль/ контрольні заходи	*залік, МКР*
Розклад занять	*http://rozklad.kpi.ua* *http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: доцент Яковлєв Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua)* *Практичні: ас. Грубіян Євген Олександрович, ас. Столович Михайло Вадимович, ас. Якимчук Олексій Петрович*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

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

Дискретна математика є тією частиною математичних знань, яка пов'язана з дослідженням, проектуванням, розробкою та побудовою складних систем, зокрема комп'ютерів, а також систем комп'ютерної обробки та подання різного роду інформації.

Дискретна математика є однією зі складових, що утворюють основу математичного апарату, який використовують спеціалісти з комп'ютерних наук та розробники методів захисту інформації. Розробка та успішна експлуатація систем баз даних, комп'ютерної графіки, комп'ютерної алгебри, засобів інформаційної безпеки тощо вимагають від спеціаліста ґрунтовних знань багатьох розділів дискретної математики.

Метою вивчення дискретної математики є засвоєння основних дискретних конструкцій, таких, як відношення, відображення, граф, алгебра, а також сучасних методів побудови та перетворення таких конструкцій. Апарат дискретної математики використовується для конструювання моделей реальних об'єктів та процесів їх функціонування, побудови методів розв'язання задач, а також для розробки засобів подання та обробки інформації в комп'ютерах.

При викладенні матеріалу курсу виділяються такі аспекти:

- основні теоретичні поняття;
- математичні моделі та обчислювальні алгоритми, що базуються на вивчених поняттях;
- застосування розглянутих моделей та алгоритмів у сучасних інформаційних технологіях.

У результаті вивчення курсу студент повинен:

а) знати математичні основи, які складають фундамент курсу, основні моделі обчислень, методи перетворень дискретних об'єктів та прикладні аспекти математичних основ та моделей;

б) вміти оперувати основними сучасними поняттями, будувати власні моделі обчислень, мати змогу розібратися в наявних моделях.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями

ЗК 3 – Здатність генерувати нові ідеї (креативність)

ЗК 4 – Здатність бути критичним і самокритичним

ЗК 6 – Здатність до абстрактного мислення, аналізу та синтезу

ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел

ЗК 8 – Знання та розуміння предметної області та розуміння професійної діяльності

Фахові компетентності

ФК 1 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем

ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі

ФК3 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень

ФК 14 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних

ФК 18 – Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем

Програмні результати навчання

РН 1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці

РН 2 – Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами

РН 4 – Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів

РН 6 – Володіти основними методами розробки дискретних і неперервних математичних моделей об'єктів та процесів, аналітичного дослідження цих моделей на предмет існування та єдиності їх розв'язку

РН 7 – Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач

РН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу

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

Для засвоєння матеріалу курсу «Дискретна математика» студент повинен знати курс математики в рамках шкільної програми та успішно і вчасно опановувати курси «Математичний аналіз» та «Алгебра та геометрія», які вивчаються паралельно.

Отримані практичні навички та засвоєнні знання необхідні для опанування таких дисциплін як «Математична логіка та теорія алгоритмів», «Комбінаторний аналіз», «Прикладна алгебра»; також вони сприяють глибшому розумінню таких дисциплін як «Програмування», «Алгоритми та структури даних», «Математичне моделювання» тощо.

3. Зміст навчальної дисципліни

Розділ 6. Основи теорії чисел

Тема 6.1. Властивості натуральних чисел

Тема 6.2. Порівняння за модулем та їх властивості

Розділ 7. Вступ до абстрактної алгебри

Тема 7.1. Алгебраїчні системи з однією операцією

Тема 7.2. Алгебраїчні системи з двома операціями

4. Навчальні матеріали та ресурси

1. Кривий, Сергій Лук'янович. Дискретна математика : підручник для студентів вищих навчальних закладів / С.Л. Кривий ; Міністерство освіти і науки України, Київський національний університет імені Тараса Шевченка, Хмельницький національний університет. - Київ ; – Чернівці : Букрек, 2017. – 567 с.

2. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцький Г.М., Печурін М.К. Основи дискретної математики. – К.: Наукова думка, 2002. – 580 с.

3. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов’язаних з інформаційними технологіями та захистом інформації. Частина 1. Множини та відношення. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2006. – 68 с.

4. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов’язаних з інформаційними технологіями та захистом інформації. Частина 3. Основні поняття теорії графів. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2012. – 87 с.

5. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов’язаних з інформаційними технологіями та захистом інформації. Частина 5. Булеві функції. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2016. – 48 с.

6. Темнікова, О. Л. Дискретна математика. Конспект лекцій. Частина 1 [Електронний ресурс] : навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» / О. Л. Темнікова – Київ : КПІ ім. Ігоря Сікорського, 2021. – 154 с. – https://ela.kpi.ua/handle/123456789/42839

7. Темнікова, О. Л. Дискретна математика. Конспект лекцій. Частина 2 [Електронний ресурс] : навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» / О. Л. Темнікова – Київ : КПІ ім. Ігоря Сікорського, 2019. – 128 с. – https://ela.kpi.ua/handle/123456789/42842

8. Базилевич, Лідія Євгенівна. Дискретна математика у прикладах і задачах : підручник / Л.Є. Базилевич. – Львів : І.Е. Чижиков, 2013. – 486 с.

9. Кривий, Сергій Лук'янович. Збірник задач з дискретної математики : навчальний посібник для студентів вищих навчальних закладів / С.Л. Кривий ; Міністерство освіти і науки України, Київський національний університет імені Тараса Шевченка. – Київ ; – Чернівці : Букрек, 2018. – 455 с.

Відеозаписи лекцій по розділу 6 викладено на Youtube-каналі кафедри ММЗІ та доступне за посиланням https://www.youtube.com/playlist?list=PLhCN8H4P5LvjLac2rY_M_0CvnKATDbPoV

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються такі методи навчання: для лекційних занять – пояснювально-ілюстративний метод та метод проблемного викладу; для практичних занять – пояснювально-ілюстративний метод, репродуктивний метод та метод проблемного викладу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
Розділ 6. Основи теорії чисел	
1	Подільність чисел. Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне.
2	Евклідові послідовності. Розширений алгоритм Евкліда, лема Безу. Лінійні діофантові рівняння.
3	Прості числа. Розподіл простих чисел. Основна теорема арифметики.
4	Мультиплікативні функції, функції кількості та суми дільників числа, їх властивості. Досконалі числа. Функція Мебіуса.
5	Порівняння за модулем, лишки. Степені за модулем. Обернені елементи за модулем.
6	Китайська теорема про остачі. Функція Ойлера. Теорема Ойлера, мала теорема Ферма.
7	Системи числення. Ознака подільності Паскаля. Подільність біноміальних коефіцієнтів, теорема Люка.
8	Лінійні порівняння. Загальна теорія розв'язку порівнянь. Розклад Тейлора для поліномів. Поліноміальні порівняння за простим модулем.
9	Квадратичні лишки, критерій Ойлера, критерій Гаусса. Символ Лежандра та його властивості. Символ Якобі та його властивості.
10	Обчислення квадратних коренів за модулем.
11	Порядок лишку за модулем. Генератори за простими модулями.
12	Функція Кармайкла. Циклічність зведених систем лишків за модулем. Порівняння вищих степенів, теорема Ойлера, задача дискретного логарифмування.
Розділ 7. Вступ до абстрактної алгебри	
13	Алгебраїчні системи з однією операцією: напівгрупи, моноїди, групи, абелеві групи. Властивості елементів моноїдів, циклічні моноїди.
14	Властивості елементів груп; циклічні групи. Порядок групи, порядок елементу групи, підгрупи. Класи суміжності. Теорема Лагранжа, наслідки з неї.
15	Властивості циклічних груп та їх елементів; генератори груп. Структура циклічної групи. Нормальні підгрупи, критерій нормальності. Фактор-групи, теорема про фактор-групи.
16	Морфізми алгебраїчних структур. Гомоморфізми, ядро та образ гомоморфізму. Теорема про гомоморфізм груп Алгебраїчні системи з двома операціями: напівкільця, кільця, поля. Оборотні елементи та дільники нуля.

17	Види кілець. Підкільця, ідеали. Головні ідеали. Фактор-кільця. Теорема про гомоморфізм кілець
18	Напіврешітки, відношення подільності. Решітки, часткове впорядкування на решітках та його властивості. Узагальнена формула включень та виключень

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Властивості подільності, алгоритм Евкліда та розширений алгоритм Евкліда
2	Застосування розширеного алгоритму Евкліда. Властивості простих чисел, основна теорема арифметики
3	Мультиплікативні функції та доведення їх властивостей. Обчислення обернених за модулем
4	Застосування китайської теореми про лишки. Функція Ойлера, теорема Ойлера та мала теорема Ферма МКР, частина 1.
5	Розв'язування лінійних порівнянь. Розв'язування поліноміальних порівнянь. Символи Лежандра та Якобі.
6	Розв'язування квадратичних порівнянь. МКР, частина 2.
7	Класифікація алгебраїчних систем. Властивості напівгруп, моноїдів та груп
8	Фактор-групи, побудова класів суміжності. Властивості гомоморфізмів. МКР, частина 3.
9	Залік

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до самостійних та модульних контрольних робіт.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Календарний рубіжний контроль

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Календарний контроль базується на поточній рейтинговій оцінці.

Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Оголошення результатів контрольних заходів

Результати виконання домашніх завдань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження.

Результати модульної контрольної роботи та письмової частини залікової контрольної роботи вказуються на відповідних бланках (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа, рейтингової системи оцінювання та/або зауважень.

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

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	4	1	≥ 4	16
2.	Написання конспектів лекцій	12	1	1	12
3.	Модульна контрольна робота	52	1	1	52
4.	Тест з теоретичного матеріалу	10	1	2	20
	Усього				100

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестра. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Рейтингова оцінка складається з результатів роботи в семестрі. Якщо семестровий рейтинг складає не менше 60 балів, студенту виставляється відповідна оцінка, окрім випадку, коли студент не погоджується із нею.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їх семестровий рейтинг складає не менше 10 балів), та студенти, які не погоджуються із такою оцінкою, на останньому практичному занятті виконують залікову контрольну роботу. При цьому їх семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової контрольної роботи. Залікова контрольна робота включає в себе тест з теоретичного матеріалу (20 балів) та практичну частину (8 задач, 80 балів).

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням **замість** складання залікової контрольної роботи можуть пройти усну співбесіду із викладачем за матеріалами курсу. На співбесіді, відповідаючи на теоретичні питання (до десяти питань, одне питання = один бал), студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки.

Студенти, які не одержали позитивної оцінки за результатами заліку, йдуть на перескладання дисципліни. Перескладання проводиться у такій само формі, як і залікова контрольна робота. На перескладанні семестровий рейтинг та результати виконання залікової роботи анулюються, а рейтингова оцінка виставляється за результатами виконання роботи на перескладанні.

Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізованій атестаційній комісії. Формат повторного перескладання визначається комісією.

Студенти, які протягом семестру одержали менше 10 балів, не допускаються до складання семестрової атестації та рекомендуються кафедрі на відрахування або повторне проходження дисципліни.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):
Склав: доцент кафедри ММЗІ, к.т.н. Яковлєв Сергій Володимирович
Ухвалено кафедрою математичних методів захисту інформації (протокол №6 від 22.06.2022 р.).
Затверджено Методичною комісією НН ФТІ (протокол № 6 від 30.06.2022 року)