



ДИСКРЕТНА МАТЕМАТИКА. ЧАСТИНА 2 (ПО 05.2)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>F Інформаційні технології</i>
Спеціальність	<i>F1 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Обов'язкова (нормативна) (цикл загальної підготовки)</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 3 кредити ЄКТС / 90 годин Лекційних занять: 30 годин Практичних занять: 16 годин Самостійна робота студентів: 44 годин</i>
Семестровий контроль/ контрольні заходи	<i>залік, МКР</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: доцент Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua) Практичні: ас. Грубіян Євген Олександрович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення 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:

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

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

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

ПРН 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

ПРН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів

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

ПРН 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

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

ПРН 14 – Виявляти здатність до самонавчання та продовження професійного розвитку

ПРН 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 опанувати 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 та методи оптимізації» тощо.

3. Зміст навчальної дисципліни

Розділ 5. Основи теорії чисел

Тема 6.1. Властивості натуральних чисел

Тема 6.2. Порівняння за модулем та їх властивості

Розділ 6. 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

Рекомендована література

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 4. Елементи загальної алгебри. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2015. – 81 с.

4. Клесов, Олег Іванович. Елементарна теорія чисел та елементи криптографії : підручник для студентів вищих навчальних закладів, які навчаються за спеціальністю "Математика та статистика" / О.І. Клесов. – Київ : ТВіМС, 2016. – 393 с.

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

6. 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 викладено на Youtube-каналі кафедри ММЗІ та доступні за такими посиланнями:

- розділ 6: https://www.youtube.com/playlist?list=PLhCN8H4P5LvJLac2rY_M_0CvnKATDbPoV
- розділ 7: <https://www.youtube.com/playlist?list=PLhCN8H4P5LvJZDr1DgDRKScCpAmh0N-dE>

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. Захист розрахункової роботи передбачає використання дискусійного методу.

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	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.
8	Лінійні порівняння. Загальна теорія розв'язку порівнянь. Розклад Тейлора для поліномів. Поліноміальні порівняння за простим модулем.
9	Квадратичні лишки, критерій Ойлера. Символ Лежандра та його властивості. Символ Якобі та його властивості. Обчислення квадратних коренів за модулем.
10	Порядок лишку за модулем. Генератори за простими модулями.
Розділ 7. Вступ до абстрактної алгебри	
11	Алгебраїчні системи з однією операцією: напівгрупи, моноїди, групи, абелеві групи. Властивості елементів моноїдів, циклічні моноїди.
12	Властивості елементів груп; циклічні групи. Порядок групи, порядок елемента групи, підгрупи. Класи суміжності. Теорема Лагранжа, наслідки з неї.
13	Властивості циклічних груп та їх елементів; генератори груп. Структура циклічної групи. Нормальні підгрупи, критерій нормальності. Фактор-групи, теорема про фактор-групи.
14	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.
15	Види кілець. Підкільця, ідеали. Головні ідеали. Фактор-кільця. Теорема про гомоморфізм кілець

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.

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.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу	16
2.	Підготовка до практичних занять, виконання домашніх завдань	16
4.	Підготовка до виконання модульної контрольної роботи	6
6.	Підготовка до заліку	6
	Усього	44

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 необхідні навички. 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 опанувати самостійно.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), підтверджених відповідними документами, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Пропущений залік (за необхідності його складати) не зараховується незалежно від причин пропуску; у такому випадку студент отримує оцінку, сформовану на основі його семестрового рейтингу, та повинен складати залік на додатковій сесії.

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 вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Результати письмової частини заліку вказуються на бланках для письмової екзаменаційної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини іспиту/заліку оголошуються наприкінці її проходження.

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>.

У разі виявлення порушень норм академічної доброчесності під час виконання контрольного заходу студент одержує за цей захід нуль балів без можливості повторного виконання.

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 (PCO)

№	Контрольний захід	Макс бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	4	≥ 3	12
2.	Модульна контрольна робота	58	1	58
3.	Тест з теоретичного матеріалу	15	2	30
	Усього			100

Критерії оцінювання контрольних заходів

1) Виконання домашніх завдань

Домашні завдання перевіряються вибірково та випадковим чином, однак у кожного студента буде не менше трьох перевірянь домашніх завдань протягом семестру. Одне домашнє завдання оцінюється у 4 рейтингових бали.

Критерії оцінювання одного домашнього завдання:

- | | |
|---|---------------|
| • Правильне повне виконання усіх завдань | 100% оцінки |
| • Виконання з деякими неточностями | 75-99% оцінки |
| • Виконання не менш ніж 50% усіх завдань | 50-74% оцінки |
| • Наявність окремих правильно виконаних завдань | 25-49% оцінки |
| • Усі завдання повністю неправильні | 0 балів |
| • Домашнє завдання не здано | 0 балів |

Здача домашнього завдання після назначеного терміну виконання без поважної причини приводить до зниження оцінки за нього на 0,1 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 0,8 бали. Домашнє завдання, яке не було здано або було здано більш ніж через вісім днів після дедлайну, вважається невиконаним і автоматично оцінюється у 0 балів.

Максимальна кількість балів, яку можна одержати за домашні завдання, дорівнює 12. Загальна кількість балів, яку студент одержує за домашні завдання, дорівнює сумі балів за кожне перевірене домашнє завдання.

2) Модульна контрольна робота

Модульна контрольна робота (МКР) складається з декількох частин, які проводяться протягом семестру по мірі опанування теоретичного та практичного матеріалу. Кількість задач та їх вартість у балах визначається викладачами в залежності від складності самої задачі та об'єму винесеного на дану частину МКР матеріалу.

Критерії оцінювання однієї задачі МКР:

- | | |
|---|---------------|
| • Правильне повне розв'язання без помилок | 100% оцінки |
| • Розв'язання з несуттєвими помилками та/або описками | 90-99% оцінки |
| • Розв'язання з деякими неточностями | 70-89% оцінки |
| • Розв'язання із правильною ідеєю, але грубими помилками | 50-69% оцінки |
| • Наявність правильної ідеї розв'язку з неправильним її застосуванням або незакінченим розв'язком | 30-49% оцінки |
| • Розв'язок повністю неправильний або відсутній | 0% оцінки |

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Виконання частини МКР, пропущеної з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за модульну контрольну роботу, дорівнює 58. Загальна кількість балів, яку студент одержує за одну частину модульної контрольної, дорівнює сумі балів за кожне завдання у відповідності до їх вартості та наведених критеріїв оцінювання. Загальна кількість балів, яку студент одержує за модульну контрольну роботу, дорівнює сумі балів за виконання усіх її частин.

3) Тести з теоретичного матеріалу

Протягом семестру по мірі опанування теоретичного матеріалу студенти пишуть два тести. Тести складаються із відкритих питань та питань із мультिवибором відповіді. Кількість питань та їх вартість у балах визначається викладачами.

Критерії оцінювання одного тестового питання:

- | | |
|---|-------------|
| • Правильна відповідь | 100% оцінки |
| • Обрано не усі правильні відповіді | 50% оцінки |
| • Відкрита відповідь містить суттєві неточності | 50% оцінки |
| • Обрана хоча б одна неправильна відповідь | 0% оцінки |

- Відкрита відповідь є неправильною 0% оцінки

Студент, який без поважних причин пропустив тест, одержує за нього нуль балів без можливості перескладання. Виконання тесту, пропущеного з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за один тест, дорівнює 15 балів. Загальна кількість балів, яку студент одержує за один тест, дорівнює сумі балів за кожне тестове питання у відповідності до їх вартості та наведених критеріїв оцінювання.

Заохочувальні бали

Модульна контрольна робота може включати в себе додаткові задачі, правильне розв'язання яких оцінюється бонусними (заохочувальними) балами поза шкалою семестрового рейтингу.

На практичних заняттях проводиться регулярне бліц-опитування теоретичних знань (означення, формулювання теорем тощо). Студенти, які правильно відповідають на таких бліц-опитуваннях, можуть одержати за семестр додатково до 3-х бонусних балів.

Студенти, які стали переможцями етапу університетської олімпіади з математики або аналогічного за змістом та статусом заходу (олімпіади інших університетів, математичні бої, конкурси наукових робіт з математики тощо), одержують 10 заохочувальних балів за перше місце, 8 – за друге місце, 6 – за третє місце.

Загальна кількість заохочувальних балів, які можна одержати за дисципліну: 10 балів.

Умови одержання проміжної атестації

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях семестру. 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.

Умови одержання семестрової оцінки

Необхідною умовою одержання семестрової оцінки є семестровий рейтинг не менше 60 балів.

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, виконують залікову роботу. При цьому їх семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової роботи.

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням замість написання залікової 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 протягом семестру одержали менше 10 балів, вважаються такими, що не виконали умови одержання семестрової оцінки, та рекомендуються кафедрі на відрахування або повторне переслуховування дисципліни.

Умови проведення залікової роботи

Право писати залікову роботу мають:

- а) студенти, семестровий рейтинг яких складає 10-59 балів;
- б) студенти, семестровий рейтинг яких складає 60-100 балів, але які не згодні з одержаною семестровою оцінкою.

Студентам, які пишуть залікову роботу, анулюється семестровий рейтинг. Оцінка, яку вони одержують за дисципліну, формується за результатами складання залікової роботи.

Залікова робота проводиться на заліковому тижні в кінці семестру.

Залікова робота включає в себе:

- практичну частину (8 задач, 80 балів);
- теоретичний тест (20 питань, 20 балів).

Критерії оцінювання задач практичної частини співпадають з критеріями оцінювання задач МКР. Критерії оцінювання тестових питань співпадають із критеріями для тестів з теоретичного матеріалу.

Під час виконання залікової роботи забороняється використання будь-яких додаткових довідкових матеріалів.

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і залікова робота. Для допуску до перескладання студент повинен одержати не менше 10 рейтингових балів (з урахуванням складання залікової роботи). Рейтингова оцінка студента визначається результатами перескладання.

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

Підсумкова оцінка з дисципліни

Рейтингова оцінка складається з результатів виконання семестрових контрольних заходів (включно з заохочувальними) або за результатами виконання залікової роботи чи перескладання. Оцінка за стобальною шкалою переводиться до університетської шкали оцінок за наведеною таблицею відповідності.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
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 №6/2 від 25.06.2025 р.).

Затверджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2025 року)