



ПРИКЛАДНА АЛГЕБРА.

Частина 2. (ПО 15.2)

Робоча програма навчальної дисципліни (Силабус)

• Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>11 Математика і статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Нормативна (цикл професійної підготовки)</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>2-й курс, весінній семестр</i>
Обсяг дисципліни	Загальна кількість: (5 кр.) 150 год. Лекційних занять: 36 год. Практичних занять: 36 год. Самостійна робота студентів: 78 год.
Семестровий контроль/ контрольні заходи	<i>Екзамен, поточний контроль, модульна контрольна робота Розрахункова робота</i>
Розклад занять	<i>http://ipt.kpi.ua/navchalnij-protses</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	Лектор: д.т.н., професор, Ковальчук Людмила Василівна (lusi.kovalchuk@gmail.com) Практичні: д.т.н., професор, Ковальчук Людмила Василівна
Розміщення курсу	

• Програма навчальної дисципліни

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

Навчальна дисципліна «Прикладна алгебра» складається з двох частин: «Прикладна алгебра-I» та «Прикладна алгебра-II». Вона є необхідною для формування навичок абстрактного мислення та побудови строгих, з математичної точки зору, доведень для різних тверджень. *Метою* вивчення дисципліни «Прикладна алгебра II» є засвоєння студентами основних алгебраїчних систем та їх властивостей. *Предметом* вивчення є такі поняття як алгебраїчні системи з однією та двома операціями, відображення таких систем, їх властивості, обчислення у таких системах, основні теореми абстрактної алгебри та теорії чисел.

Математичні об'єкти, що вивчаються в цьому курсі, та їх властивості суттєво використовуються при побудові та аналізі будь-яких сучасних криптографічних систем. Так, вони є необхідними для побудови блокових та потокових алгоритмів шифрування та для обґрунтування їх стійкості (теорія груп, обчислення у скінченних полях), для побудови класичних асиметричних систем (теорія чисел) та сучасних асиметричних систем (скінченні поля). Проте роль цієї дисципліни не обмежується лише криптологією, її можна вважати центральною та базовою для вивчення будь-яких інших розділів як фундаментальної, так і прикладної математики.

Для успішного засвоєння дисципліни необхідні знання перш за все з математичного аналізу, алгебра та геометрія, дискретної математики, математична логіка та теорія алгоритмів, комбінаторий аналіз, теорія складності. Матеріал другої частини курсу суттєво спирається на визначення та методи, вивчені у частині I.

Для закріплення та поглибленого розуміння означень, теоретичних положень та методів прикладної алгебри передбачено проведення практичних занять. *Основна мета практичних занять* – сформувані у студентів навички використання теоретичних знань, які викладаються на лекціях з даної дисципліни. Для цього доцільно на практичних заняттях з прикладної алгебри:

- а) перевіряти знання студентів теоретичного матеріалу з теми, що вивчається;
- б) розв'язувати задачі різноманітних типів з теми, що вивчається, в першу чергу – задачі на доведення, демонструючи при цьому різні можливі способи їх розв'язання;
- в) перевіряти виконання студентами домашніх завдань (шляхом усних або письмових опитувань);
- г) здійснювати підсумкові перевірки засвоєння вивченої теми (в усній та письмовій формах).

За курсом відповідно до навчального плану передбачено проведення поточного контролю у вигляді виконання модульної контрольної роботи (МКР), розрахункової роботи (РР).

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

знання: впевнено володіти основними поняттями абстрактної алгебри; математично коректно формулювати постановки задач, пов'язаних із алгебраїчними системами; будувати строгі доведення тверджень, знаходити логічні та інші помилки в таких доведеннях;

уміння: будувати моделі об'єктів, які за своєю суттю можна описати алгебраїчними системами; визначати, який саме метод доцільно використовувати для розв'язання тієї чи іншої задачі; вміти правильно вибирати алгебраїчну систему, щоб побудувати відповідну модель та розв'язати задачу; використовувати властивості алгебраїчних систем та їх елементів для розв'язку задач; доводити, що даний об'єкт є або не є певною алгебраїчною системою; вміти використовувати алгебраїчні методи для розв'язку задач теорії чисел; вміти будувати скінченні поля за заданими параметрами або доводити, що такого поля не існує; вміти виконувати обчислення у групах, кільцях та скінченних полях, обчислювати різні числові характеристики груп, кілець, полів та їх елементів; будувати відображення між різними алгебраїчними системами та визначати характеристики цих відображень;

досвід: навички практичного використання засвоєних знань, методів абстрактної алгебри, теорії чисел та теорії скінченних полів у подальшому навчанні та професійній діяльності.

Згідно з вимогами освітньо-наукової програми студенти після засвоєння навчальної дисципліни «Прикладна алгебра II» мають продемонструвати такі результати навчання:

Загальні компетентності СВО

ЗК1	Здатність вчитися і оволодівати сучасними знаннями.
ЗК3	Здатність генерувати нові ідеї (креативність).
ЗК4	Здатність бути критичним і самокритичним.
ЗК6	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК8	Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК 7	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності СВО

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.
ФК14	Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.
ФК18	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 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 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.
ПРН 19	Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми
ПРН 21	Вміти формулювати та розв'язувати алгебраїчні та комбінаторні задачі, будувати та реалізовувати комбінаторні алгоритми та алгоритми прикладної алгебри, аналізувати теоретичну та практичну складність таких алгоритмів

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

Для засвоєння матеріалу курсу «Прикладна алгебра-II» студентам необхідні знання в рамках шкільного курсу алгебри та геометрії, а також вони повинні засвоїти основні поняття та методи курсів:

- 1) прикладна алгебра-I;
- 2) математичний аналіз;
- 3) методи комбінаторики;
- 4) алгебра;
- 5) дискретна математика.

Отримані практичні навички та засвоєнні теоретичні знання під час вивчення навчальної дисципліни «Прикладна алгебра» можна використовувати в подальшому в таких навчальних дисциплінах:

1. статистична фізика;
2. статистична радіотехніка;
3. математичні методи захисту інформації;
4. математична теорія надійності;
5. теорія масового обслуговування;
6. спеціальні розділи обчислювальної математики;
7. симетрична криптографія;
8. асиметричні криптосистеми та протоколи;
9. теорія інформації та кодування;
10. методи криптоаналізу 1,2;
11. методи реалізації криптографічних механізмів;
12. сучасні алгебраїчні системи і організаційні аспекти криптографії;
13. квантове обчислення та квантова криптографія;
14. проектування, розробка та реалізація криптографічних систем;
15. розділи сучасної криптології 2.

3. Зміст навчальної дисципліни

4. Навчальні матеріали та ресурси

Для опанування дисципліни «Прикладна алгебра II» рекомендується наступна

– *Базова література*

1. Конспект лекцій з рекомендованими задачами за курсом “Прикладна алгебра I”.
2. *Вербицький О. В.* Вступ до криптології / О.В. Вербицький– Львів: Видавництво науково-технічної літератури, 1998. – 247 с.
3. *Ковальчук Л.В., Яремчук Ю.Є.* Прикладна алгебра. Частина 1. Основи абстрактної алгебри: навчальний посібник / Л.В. Ковальчук, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2015. – 99 с.
4. *Ковальчук Л.В., Яремчук Ю.Є.* Прикладна алгебра. Частина 2. Теорія чисел: навчальний посібник / Л.В. Ковальчук, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2020. – 129 с.

– *Додаткова література*

1. *Ван Тилборг Х.К.А.* Основы криптологии / Х.К.А. Ван Тилборг. - Пер. с англ. – М.: Мир, 2006. – 471 с.
2. *Коблиц Н.* Курс теории чисел и криптографии / Н. Коблиц – М.: Научное изд-во ТВП, 2001. – 254 с.

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студента для засвоєння студентами матеріалу та розвитку у них практичних навичок. Для проведення занять застосовується практичний метод. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання, для проведення лабораторних робіт використовується частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами проблему, і ті вирішують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, підбираючи для цього необхідні джерела інформації, методи, підходи тощо.

Лекційні заняття

Розділ 1. Елементи теорії чисел.

Тема 1.1. Конгруенції та їх властивості. Системи конгруенцій.

1. Означення конгруенції, її властивості.
2. Системи конгруенцій. Китайські теореми про лишки (проста та узагальнена).
3. Застосування Китайської теореми – задача про розподіл секрету.

Тема 1.2. Структура мультиплікативної групи скінченного поля.

1. Теорема про структуру мультиплікативної групи скінченного поля.
2. Критерій генератора групи.
3. Алгоритм пошуку генераторів групи.

Тема 1.3. Квадратичні лишки та нелишки.

1. Означення квадратичного лишка та нелишка. Властивості.
2. Символ Лежандра, символ Якобі. Властивості.
3. Відмінність між символом Якобі та символом Лежандра.

Тема 1.4. Добування квадратного кореня за модулем.

1. Добування квадратичного кореня за простим модулем (3 випадки).
2. Добування квадратичного кореня за складеним модулем.

Тема 1.5. Псевдопрості числа.

1. Означення та властивості псевдопростих Ферма. Числа Кармайкла.
2. Означення та властивості псевдопростих Ойлера.
3. Означення та властивості сильно псевдопростих чисел.

Тема 1.6. Генерація простих чисел.

1. "Наївні" алгоритми генерації простих чисел.
2. Алгоритм Соловея-Штрассена та його характеристики.
3. Алгоритм Міллера-Рабіна та його характеристики.

Розділ 2. Скінченні поля.

Тема 2.1. Розширення полів.

1. Означення розширення, типи розширень.
2. Означення мінімального поліному.

3. Властивості мінімального поліному.

Тема 2.2. Поле як векторний простір над підполем.

1. Поле як векторний простір.
2. Степінь розширення. Скінченні розширення.
3. Зв'язок між простими, алгебраїчними та скінченними розширеннями.

Тема 2.3. Властивості простого розширення. Поле розкладу.

1. Прості розширення, їх побудова та властивості.
2. Поле розкладу полінома.
3. Існування та єдність поля розкладу.

Тема 2.4. Головна характеристична теорема скінченних полів. Критерій підполя.

1. Допоміжні леми.
2. Головна характеристична теорема скінченних полів.
3. Критерій підполя.

Тема 2.5. Примітивні елементи поля.

1. Примітивні елементи поля.
2. Скінченне поле як просте розширення.
3. Існування незвідних поліномів.

Тема 2.6. Корені незвідних поліномів.

1. Корені незвідних поліномів.
2. Властивості коренів незвідних поліномів.
3. Автоморфізми поля над підполем.

Тема 2.7. Слід та норма елемента поля.

1. Означення та властивості характеристичного поліному.
2. Означення сліду та норми.
3. Властивості сліду та норми.
4. Теорема про лінійні відображення поля над підполем.

Тема 2.8. Базиси поля над підполем.

1. Типи базисів поля над підполем.
2. Критерії базису.
3. Існування нормального базису.

Тема 2.9. Порядки поліномів.

1. Означення порядку полінома. Коректність означення.
2. Порядки незвідних поліномів.
3. Обчислення порядку полінома.

Тема 2.10. Примітивні поліноми.

1. Примітивні поліноми.
2. Критерій примітивності.
3. Кількість примітивних поліномів над полем.

Тема 2.11. Критерії незвідності та примітивності полінома, алгоритми перевірки незвідності та примітивності.

1. Критерії незвідності та примітивності полінома.
2. Алгоритми перевірки незвідності та примітивності.

Тема 2.12. Функція Мебіуса. Обчислення кількості незвідних поліномів.

1. Рекурентна формула обчислення кількості незвідних поліномів над полем.
2. Означення функції Мебіуса. Формула обернення.
3. Формула обчислення кількості незвідних поліномів з використанням функції Мебіуса.

•

Практичні заняття

Метою проведення практичних занять є закріплення знань, надбаних на лекційних заняттях та практичне оволодіння математичними методами та прикладами їх застосування.

Необхідний матеріал, для підготовки до практичних занять можна знайти, зокрема, у посібниках [1-4], які містить основні означення, твердження та формули, необхідні для розв'язування задач, та приклади розв'язання найбільш типових задач.

Розділ 1. Елементи теорії чисел.

Заняття 1. Конгруенції та їх властивості. Системи конгруенцій.

1. Розв'язок задач на визначення та властивості конгруенцій та систем конгруенцій.
2. Розв'язок задач на знаходження генераторів мультиплікативної групи.

СРС: [1-4].

Заняття 2. Квадратичні лишки та нелишки.

1. Розв'язок задач на визначення та властивості квадратичних лишків та нелишків та їх властивості.
2. Розв'язок задач на добування квадратичних коренів за простим та складеним модулем.

СРС: [1-4].

Заняття 3. Псевдопрості числа.

1. Розв'язок задач на визначення та властивості псевдопростих чисел.
2. Розв'язок задач на використання алгоритмів перевірки простоти числа.

СРС: [1-4].

Розділ 2. Скінченні поля.

Заняття 4. Розширення полів.

Розв'язок задач на визначення та властивості розширень скінченних та нескінченних полів.

СРС: [1-4].

Заняття 5. Властивості простого розширення. Поле розкладу. ГХТ скінченних полів.

1. Розв'язок задач на визначення та властивості простих розширень полів.
2. Розв'язок задач на побудову полів за заданими параметрами та визначення їх підполів.

СРС: [1-4].

Заняття 6. Примітивні елементи поля. Корені незвідних поліномів.

1. Розв'язок задач на визначення примітивних елементів поля та їх мінімальних поліномів.

2. Розв'язок задач на визначення коренів незвідних поліномів та перевірку їх властивостей.

СРС: [1-4].

Заняття 7. Слід та норма елемента поля. Базиси поля над підполем.

1. Розв'язок задач на обчислення сліду та норми елементів та на побудову лінійних відображень поля над підполем.

2. Розв'язок задач на побудову базисів різних типів та на використання критеріїв базису.

СРС: [1-4].

Заняття 8. Порядки поліномів. Примітивні поліноми.

1. Розв'язок задач на обчислення порядків поліномів.

2. Розв'язок задач на перевірку примітивності поліному та обчислення їх кількості.

СРС: [1-4].

Заняття 9. Критерії незвідності та примітивності полінома, алгоритми перевірки незвідності та примітивності. Функція Мебіуса. Обчислення кількості незвідних поліномів.

Розв'язок задач на перевірку незвідності та примітивності поліномів.

1. Рекурентна формула обчислення кількості незвідних поліномів над полем.

2. Означення функції Мебіуса. Формула обернення.

3. Формула обчислення кількості незвідних поліномів з використанням функції Мебіуса.

4. Розв'язок задач на визначення та властивості алгебраїчної системи.

СРС: [1-4].

6. Самостійна робота студента/аспіранта

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.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу за темою «Основи теорії графів». Для підготовки до виконання розрахункової роботи слід скористатися рекомендованою літературою, конспектом та/або відеозаписами лекцій. Студенту надається не менше двох тижнів на виконання розрахункової роботи, після чого в узгоджений із викладачем час студент повинен захистити виконану роботу.

Для кращого закріплення теоретичного матеріалу першого семестру студент повинен здати колоквиум; підготовка до колоквиуму вимагає ретельного повторення теоретичного матеріалу відповідних лекцій у години самостійної роботи.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу, підготовка до колоквиуму	18
2.	Підготовка до практичних занять	18
4.	Підготовка до виконання модульної контрольної роботи	2
5.	Виконання індивідуального завдання	10
6.	Підготовка та складання іспиту	30
	Усього	78

• 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.

Студент, який без поважних причин пропустив колоквиум або захист розрахункової роботи, не допускається до складання іспиту. Якщо пропуск стався з поважної причини, складання колоквиуму або захист розрахункової роботи, дозволяється виконання цих заходів у інший узгоджений із викладачем час.

Пропущений іспит не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен скласти іспит 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.

Захист виконаної та оформленої розрахункової роботи проводиться у формі співбесіди з викладачем. Під час захисту студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач. Результати виконаної та повністю оформленої РР у встановлений викладачем термін кожен студент захищає індивідуально. Результати захисту оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок.

Колоквіум проходить в усній формі в режимі діалогу, в якому відповіді та зауваження на свої відповіді студент одержує безпосередньо під час спілкування. Оцінка за колоквіум оголошується наприкінці його проходження.

Результати письмової частини іспиту 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	Бал	Кількість	Всього
1	Модульна контрольна робота	24	1	24
2	Домашні завдання	2	5	10
3	РР	5	1	5
4	Колоквіум	15	1	15
5	Конспекти	0.5	12	6
6	Екзамен	40	1	40
	Всього			100

Критерії оцінювання контрольних заходів

1) Виконання домашніх завдань

Домашні завдання перевіряються вибірково та випадковим чином, однак у кожного студента буде не менше п'яти перевірянь домашніх завдань протягом семестру. Одне домашнє завдання оцінюється у 2 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 0,05 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 0,4 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 10. Загальна кількість балів, яку студент одержує за домашні завдання, дорівнює сумі балів за кожне перевірене домашнє завдання. Якщо одержана сума перевищує 10 балів, вона встановлюється у 10 балів.

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 24. 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) Розрахункова робота

Розрахункова робота (РР) складається з декількох завдань. Кожен студент одержує своє індивідуальне завдання для виконання. Кількість задач та їх вартість у балах визначається викладачами та наводиться у завданні на РР. Оцінювання РР складається з двох етапів: безпосереднього виконання студентом індивідуального завдання та його захист у викладача; кожна частина дає до 50% від оцінки за кожну задачу РР.

Критерії оцінювання одного завдання РР:

- | | |
|--|---------------|
| • Повне розв'язання без помилок, правильна відповідь | 50% оцінки |
| • Правильне розв'язання із неправильною відповіддю через неточності та арифметичні помилки | 25-49% оцінки |
| • Розв'язання із правильною ідеєю, але грубими помилками | 10-24% оцінки |
| • Розв'язок повністю неправильний або відсутній | 0% оцінки |

Критерії оцінювання захисту одного завдання РР:

- Студент демонструє вичерпне розуміння наведеного

- | | |
|---|---------------------|
| розв'язку та відповідного теоретичного матеріалу | 50% оцінки |
| • Студент відповідає з неточностями та помилками | 30-49% оцінки |
| • Відповідь студента містить окремі вірні положення | 10-29% оцінки |
| • Студент демонструє повне нерозуміння теоретичного матеріалу та наведеного розв'язку | 0 балів за завдання |

Максимальна кількість балів, яку можна одержати за виконання та захист РР, дорівнює 5.

Здача РР після призначеного терміну виконання без поважної причини приводить до зниження оцінки за неї на 0,25 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 2 бали. АЛЕ: якщо РР була здана через вісім днів після призначеного терміну, вона автоматично оцінюється у 0 балів.

Виконання та захист РР (навіть на 0 балів) є обов'язковою умовою допуску до іспиту.

4) Колоквіум

Протягом семестру кожен студент повинен скласти колоквіум – фронтальне усне опитування теоретичного матеріалу першого змістовного модуля курсу. Колоквіуми здаються викладачу у позааудиторний час за узгодженим графіком.

Максимальна кількість балів, яку можна одержати за складання колоквіуму, дорівнює 15.

Критерії оцінювання колоквіуму:

- | | |
|--|-------------|
| • Студент демонструє вичерпне розуміння теоретичного матеріалу | 15 балів |
| • Студент відповідає з незначними неточностями | 12-14 балів |
| • Студент відповідає з суттєвими неточностями | 8-11 балів |
| • Відповіді студента лише частково вірні | 5-7 балів |
| • Відповіді студента містять лише окремі вірні положення | 1-5 балів |
| • Студент демонструє повне нерозуміння теоретичного матеріалу | 0 балів |

Графік складання колоквіумів узгоджується між викладачем та студентами заздалегідь. Студент, який без поважних причин пропустив колоквіум, вважається таким, який не склав колоквіум. Студенту, який пропустив колоквіум з поважних причин, в індивідуальному порядку надається можливість скласти його в інший час, узгоджений із викладачем.

Складання колоквіуму є обов'язковою умовою допуску до іспиту.

5) Конспекти

Конспект, який є повним та деталізованим (містить всі означення, приклади, теореми, леми та основні тези доведень) оцінюється в 0.5 балів. Конспект, який є фрагментарним, оцінюється в 0.25 балів. Незданий конспект оцінюється в 0 балів.

За конспект, зданий після дедлайну, оцінка знижується на 0.2 бали. Конспект, незданий протягом 2-х тижнів після дедлайну, автоматично вважається незданим і оцінюється в 0 балів.

б) Семестрова атестація (іспит)

Семестрова атестація (іспит) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Іспит включає в себе

- практичну частину на 10 балів (2 задачі, по 5 балів кожна);
- теоретичну частину на 30 балів (2 теоретичних питання із розгорнутою відповіддю, 10 балів кожне, та два питання на формулювання означень або теорем або прикладів, по 5 балів кожне).

Критерії оцінювання задач практичної частини співпадають з критеріями оцінювання задач МКР. Критерії оцінювання теоретичного питання із розгорнутою відповіддю:

- Студент демонструє вичерпне розуміння теоретичного матеріалу 100% оцінки
- Студент відповідає з незначними неточностями 90-99% оцінки
- Студент відповідає з суттєвими неточностями 60-89% оцінки
- Відповіді студента лише частково вірні 30-59% оцінки
- Відповіді студента містять лише окремі вірні положення 10-29% оцінки
- Студент демонструє повне нерозуміння теоретичного матеріалу 0 балів

Під час іспиту забороняється використання будь-яких додаткових довідкових матеріалів.

Заохочувальні бали

На практичних заняттях за кожну самостійно розв'язану біля дошки задачу дається по 1-3 бали. Конструктивна ідея або вірна відповідь з «місця»: 1 бал. Можливі і інші варіанти оцінки роботи на розсуд викладача, що веде практику, проте прикінцевий максимальний бал становить не більше 10. З огляду на обмежену кількість виходів до дошки студенти зацікавлені у активній участі в роботі на практичних заняттях.

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 допуску до семестрової атестації

Необхідною умовою допуску до семестрової атестації є

- семестровий рейтинг не менше 25 балів;
- зданий колоквіум;
- виконана та здана розрахункова робота.

Студенти, які протягом семестру отримали від 10 до 25 балів, не допускаються до складання іспиту. Замість іспиту такі студенти виконують письмову допускну роботу (10 задач, 20 балів), результати якої додають до семестрового рейтингу; якщо після виконання допускну роботи семестровий рейтинг стає більшим 30 балів (і виконані усі інші умови допуску), студент допускається до семестрової атестації на перескладанні, а його семестровий рейтинг вважається таким, що дорівнює 30 балів; в іншому випадку результати допускну роботи анулюються, а на перескладанні студент повторно виконує допускну роботу.

Студенти, які не виконали розрахункову роботу та/або не здали колоквіум, не допускаються до складання іспиту. Таким студентам буде надана можливість здати та захистити розрахункову роботу та/або здати колоквіум перед додатковою сесією, щоб одержати допуск до перескладання дисципліни.

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

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і іспит. Для допуску до перескладання студент повинен одержати не менше 30 рейтингових балів (з урахуванням першої спроби складання іспиту або допускної роботи), виконати і захистити розрахункову роботу та здати колоквиум. На перескладанні результати основного іспиту анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів 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) та результатів усного іспиту або його 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: професор кафедри ММЗІ, д.т.н., професор Ковальчук Людмила Василівна.

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)