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

ПРИКЛАДНА АЛГЕБРА. ЧАСТИНА 2 (ПО 1.2)

Робоча програма навчальної дисципліни (Силабус)

• Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	***11 Математика і статистика***
Спеціальність	***113 Прикладна математика***
Освітня програма	***Математичні методи криптографічного захисту інформації***
Статус дисципліни	***Нормативна (цикл професійної підготовки)***
Форма навчання	***Очна (денна)***
Рік підготовки, семестр	***2-й курс, весінній семестр***
Обсяг дисципліни	**Загальна кількість: (4 кр.) 120 год.** **Лекційних занять: 36 год.** **Практичних занять: 18 год.** **Самостійна робота студентів: 66 год.**
Семестровий контроль/ контрольні заходи	***Екзамен, поточний контроль,*** ***модульна контрольна робота*** ***Розрахункова робота***
Розклад занять	***http://ipt.kpi.ua/navchalnij-protses***
Мова викладання	***Українська***
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 вивчання та результати навчання

Навчальна дисципліна «Прикладна алгебра» складається з двох частин: «Прикладна алгебра. Частина 1» та «Прикладна алгебра. Частина 2». Вона є необхідною для формування навичок абстрактного мислення та побудови строгих, з математичної точки зору, доведень для різних тверджень. *Метою* вивчення дисципліни «Прикладна алгебра. Частина 2» 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, комбінаторний аналіз, теорія складності. Матеріал другої частини курсу суттєво спирається на визначення та методи, вивчені у частині І.

Для закріплення та поглибленого розуміння означень, теоретичних положень та методів прикладної алгебри передбачено проведення практичних занять. *Основна мета практичних занять* – сформувати 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 вимог освітньої програми, студенти після засвоєння навчальної дисципліни «Прикладна алгебра. Частина 1» мають продемонструвати такі результати навчання:

Загальні компетентності СВО

ЗК1 Здатність учитися і оволодівати сучасними знаннями.

ЗК3 Здатність генерувати нові ідеї (креативність).

ЗК4 Здатність бути критичним і самокритичним.

ЗК6 Здатність до абстрактного мислення, аналізу та синтезу.

ЗК7 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК8 Знання та розуміння предметної області та розуміння професійної діяльності.

Фахові компетентності СВО

ФК1 Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

ФК2 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

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

РН 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.

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

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

РН 14 Виявляти здатність до самонавчання та продовження професійного розвитку.

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

РН 19 Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

РН 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 студентам необхідні знання в рамках шкільного курсу алгебри та геометрії, а також вони повинні засвоїти основні поняття та методи курсів «Алгебра та геометрія», «Дискретна математика» та «Математичний аналіз»

Отримані практичні навички та засвоєнні теоретичні знання під час вивчення навчальної дисципліни можна використовувати в подальшому в таких дисциплінах, як «Спеціальні розділи обчислювальної математики», «Симетрична криптографія», «Асиметричні криптосистеми та протоколи», «Теорія інформації та кодування».

3. Зміст навчальної дисципліни

Розділ 1. Елементи теорії чисел.

Тема 1.1. Конгруенції та їх властивості. Системи конгруенцій.

Тема 1.2. Структура мультиплікативної групи скінченного поля.

Тема 1.3. Квадратичні лишки та нелишки.

Тема 1.4. Добування квадратного кореня за модулем.

Тема 1.5. Псевдопрості числа.

Тема 1.6. Генерація простих чисел.

Розділ 2. Скінченні поля.

Тема 2.1. Розширення полів.

Тема 2.2. Поле як векторний простір над підполем.

Тема 2.3. Властивості простого розширення. Поле розкладу.

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

Тема 2.5. Примітивні елементи поля.

Тема 2.6. Корені незвідних поліномів.

Тема 2.7. Слід та норма елемента поля.

Тема 2.8. Базиси поля над підполем.

Тема 2.9. Порядки поліномів.

Тема 2.10. Примітивні поліноми.

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

Тема 2.12. Функція Мебіуса. Обчислення кількості незвідних поліномів.

4. Навчальні матеріали та ресурси

Для опанування дисципліни рекомендується наступна література:

1. *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.

2. *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.

3. Завадська Л.О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006. – 54с.

4. *Вербицький О. В.* Вступ до криптології / О.В. Вербицький– Львів: Видавництво науково-технічної літератури, 1998. – 247 с.

5. *Koblitz N.* A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – 312 p.

- **Навчальний контент**

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 просих 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 характеризаційна теорема скінченних полів. Критерій підполя.
1. Допоміжні леми.
2. Головна характеризаційна 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, 2], 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.

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.

Заняття 3. Псевдопрості числа.

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

Розділ 2. Скінченні поля.

Заняття 4. Розширення полів.

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

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.

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.

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.

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.

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.

6. Самостійна робота студента/аспіранта

Самостійна робота студентів має на меті розвиток творчих здібностей та активізація їх розумової діяльності, формування потреби безперервного самостійного поповнення знань та розвиток морально-вольових якостей. Завданням самостійної роботи студентів є навчити студентів самостійно працювати з літературою, творчо сприймати навчальний матеріал і осмислювати його. Метою самостійної роботи є формування навичок до щоденної роботи з метою одержання та узагальнення знань, умінь і навичок.

На самостійну роботу відводяться наступні види завдань:

- робота з відповідними підручниками та особистим конспектом лекцій;
- виконання ДЗ
- виконання підготовчої роботи до практичних занять та до написання МКР і РР;
- підготовка до складання семестрового контролю (екзамену).

• Політика та контроль

•

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Відвідування лекцій, а також відсутність на них, не оцінюється. Однак, студентам рекомендується (вкрай необхідно) відвідувати заняття, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для успішного складання заліку. При цьому встановлюється безпосередній контакт з викладачем, який відповість на всі питання та пояснить незрозумілий матеріал.

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.

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 контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами (згідно «Положення про систему забезпечення якості вищої освіти у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського», «Положення про організацію навчального процесу»).

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

Видами контролю успішності засвоєння матеріалу дисципліни є модульна контрольна робота (МКР), розрахункова робота (РР) та семестровий контроль.

Робота на практичних заняттях

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 30. З огляду на обмежену кількість виходів до дошки студенти зацікавлені у активній участі в роботі на практичних заняттях.

Модульна контрольна робота

Модульна контрольна робота проводиться після завершення першої частини курсу протягом двох академічних годин на практичних заняттях. Вона складається з 5 задач і передбачає письмовий їх розв'язок. Задачі підібрані подібними до тих, що розглядались на практичних заняттях та під час виконання домашніх робіт.

Робота оцінюється за чіткими критеріями з позначенням коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Критерії оцінювання модульної контрольної роботи:

- максимальна кількість балів за кожне питання – повна правильна відповідь, 95% інформації, у потрібних місцях наведено малюнки, позначення, є письмовий коментар щодо базових понять та методів, які використовуються під час розв'язку задачі,
- 75% балів — розв'язок правильний, але не всі умови попереднього пункту виконано,
- 60% балів — наведено правильні базові означення, але сам розв'язок неправильний.
- Відповіді є списаними, студент не в змозі їх пояснити, відповідь не зараховуються.

Розрахункова робота

Розрахункова робота виконується студентами самостійно. На її виконання надається не менше двох тижнів. Вона складається з 10 задач і передбачає письмовий їх розв'язок. Задачі підібрані подібними до тих, що розглядались на практичних заняттях та під час виконання домашніх робіт.

Робота оцінюється за чіткими критеріями з позначенням коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Критерії оцінювання розрахункової роботи:

- максимальна кількість балів за кожне питання – повна правильна відповідь, 95% інформації, у потрібних місцях наведено малюнки, позначення, є письмовий коментар щодо базових понять та методів, які використовуються під час розв'язку задачі,
- 75% балів — розв'язок правильний, але не всі умови попереднього пункту виконано,

- 60% балів — наведено правильні базові означення, але сам розв’язок неправильний.
- Відповіді є списаними, студент не в змозі їх пояснити, відповідь не зараховуються.

Умови допуску до іспиту

В таблиці наведено умови допуску до семестрового контролю.

№	Обов’язкова умова допуску до екзамену	Критерій
1	Поточний рейтинговий бал	≥20
2	МКР	Виконана
3	РР	Виконана
4	Виконано не менше за 80% ДЗ	

Додаткові умови допуску до іспиту, які заохочуються:

- активна самостійна робота над теоретичним матеріалом: пошук та використання інформаційних ресурсів та матеріалів, що доповнюють поточний курс (додаються заохочувальні бали);

Семестровий контроль (екзамен)

Екзамен приймається у 2 етапи і складається із двох частин. Перша частина є письмовою тривалістю 1 академічної години. Друга частина є усною у формі співбесіди.

Письмова частина передбачає відповіді на два теоретичних питання та розв’язок однієї задачі. Кількість балів за кожну задачу та відповідність набраних балів оцінці в університетській шкалі встановлюється викладачами в білетах до письмової роботи в залежності від складності задачі. Максимальний рейтинговий бал за письмову частину 15.

Усна частина (за білетом) містить обговорення результатів письмової частини та відповіді на два додаткових питання з теорії і проходить після письмової. Максимальний рейтинговий бал за усну частину 25.

Загальна оцінка за екзамен складається із стартового рейтингу, отриманого протягом семестру, та рейтингових балів, набраних під час заліку. Рейтингові бали (максимум 15) за усну частину заліку нараховуються згідно наступних критеріїв:

- 22-25 — повна правильна відповідь, 95% інформації, наведено малюнки, позначення, є письмовий коментар щодо базових понять та методів, означення та формулювання теорем є вірними, повна правильна відповідь на уточнюючі запитання;
- 15-21 — правильна відповідь, 75% інформації, наведено малюнки, позначення, є письмовий коментар щодо базових понять та методів, означення та формулювання теорем є по суті правильними, але неповними, правильна відповідь на майже всі уточнюючі запитання;
- 10-14 — по суті правильна але неповна відповідь, 60% інформації, наведено малюнки та позначення, відсутні письмові коментарі щодо базових понять та методів, означення та формулювання теорем є по суті правильними, але неповними, правильна відповідь на більшість уточнюючих запитань;
- 5-9 — відповідь неповна, 45% інформації, не наведено потрібні малюнки та позначення, відсутні письмові коментарі щодо базових понять та методів, означення та формулювання теорем є здебільшого правильними але неповними, відповіді на уточнюючі запитання є неповними;
- від 0 до 4 — відповідь неповна, 30% інформації, не наведено потрібні малюнки та позначення, відсутні письмові коментарі щодо базових понять та методів, означення та

формулювання теорем є неточними, відповіді на уточнюючі запитання є неповними або відсутні взагалі.

Остаточна оцінка **RD** є сумою рейтингових балів отриманих за поточний контроль та балів отриманих на іспиті.

№	Контрольний захід	Бал	Кількість	Всього
1	Модульна контрольна робота	15	1	15
2	РР	15	1	15
3	Практичні заняття	30	1	30
4	Екзамен	40	1	40
	Всього			100

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Значення рейтингу	Оцінка ECTS
95 ≤ **RD** ≤ 100	відмінно
85 ≤ **RD** ≤ 94	дуже добре
75 ≤ **RD** ≤ 84	добре
65 ≤ **RD** ≤ 74	задовільно
60 ≤ **RD** ≤ 64	достатньо
RD < 60	незадовільно
RD < 40	не допущено

Робочу програму навчальної дисципліни (силабус):
Складено професором кафедри ММЗІ, професором, д.т.н. Ковальчук Л.В.
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)