



# ПРИКЛАДНА АЛГЕБРА. ЧАСТИНА 1 (ПО 1.1)

## 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, осінній семестр</i>
Обсяг дисципліни	Загальна кількість: (4 кр.) 120 год. Лекційних занять: 36 год. Практичних занять: 36 год. Самостійна робота студентів: 48 год.
Семестровий контроль/ контрольні заходи	<i>Залік, поточний контроль, модульна контрольна робота</i>
Розклад занять	<i><a href="http://ipt.kpi.ua/navchalnij-protses">http://ipt.kpi.ua/navchalnij-protses</a></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.

#### 2. 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 1» 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* – сформулювати 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).

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

### **3. 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 «Прикладна алгебра 1» «Спеціальні розділи обчислювальної математики», «Симетрична криптографія», «Асиметричні криптосистеми та протоколи», «Теорія інформації та кодування».

## 4. Зміст навчальної дисципліни

### Розділ 1. Алгебраїчні системи з однією операцією.

- Тема 1.1. Основні алгебраїчні системи з однією операцією та їх властивості.
- Тема 1.2. Теорема Лагранжа та її наслідки.
- Тема 1.3. Означення і властивості циклічних груп.
- Тема 1.4. Група перестановок та її властивості.
- Тема 1.5. Дія групи на множину. Теорема Келі.
- Тема 1.6. Нормальні підгрупи. Факторгрупа.
- Тема 1.7. Відображення груп. Теорема про ізоморфізм груп.

### Розділ 2. Алгебраїчні системи з двома операціями.

- Тема 2.1. Означення кільця, типи кілець.
- Тема 2.2. Підкільце, ідеал, типи ідеалів.
- Тема 2.3. Поле, характеристика поля.
- Тема 2.4. Факторкільце. Відображення кілець.
- Тема 2.5. Властивості факторкілець за ідеалами.

### Розділ 3. Факторіальні та Евклідові кільця.

- Тема 3.1. Факторіальне кільце
- Тема 3.2. Евклідове кільце.
- Тема 3.3. Кільце цілих чисел як евклідове кільце.
- Тема 3.4. Кільце поліномів як евклідове кільце.

### Розділ 4. Алгоритми та їх складність.

- Тема 4.1. Час роботи алгоритмів.
- Тема 4.2. Імовірнісні алгоритми.

## 5. Навчальні матеріали та ресурси

Для опанування дисципліни рекомендується наступна література:

1. Конспект лекцій з рекомендованими задачами за курсом “Прикладна алгебра. Частина 1”.
2. 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.
3. 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.
4. Завадська Л.О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006. – 54с.
5. Вербицький О. В. Вступ до криптології / О.В. Вербицький– Львів: Видавництво науково-технічної літератури, 1998. – 247 с.
6. Koblitz N. A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – 312 p.

6.

## 7. 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. Алгебраїчні системи з однією операцією.

Тема 1.1. Основні алгебраїчні системи з однією операцією та їх властивості.

1. Означення операції та алгебраїчної системи.
2. Напівгрупа, моноїд, група – означення та властивості.
3. Властивості елементів моноїда та групи.

Тема 1.2. Теорема Лагранжа та її наслідки.

1. Підгрупа, класи суміжності.
2. Властивості класів суміжності.
3. Теорема Лагранжа.
4. Наслідки теореми Лагранжа.

Тема 1.3. Означення і властивості циклічних груп.

1. Означення циклічної групи.
2. Теорема про властивості циклічних груп.
3. Скінченні та нескінченні циклічні групи.

Тема 1.4. Група перестановок та її властивості.

1. Означення перестановки та групи перестановок.
2. Транспозиції, зсуви, обернені перестановки.
3. Знак перестановки.
4. Форми подання перестановки.

Тема 1.5. Дія групи на множину. Теорема Келі.

1. Означення дії групи на множину.
2. Підгрупи групи перестановок. Система утворюючих.
3. Теорема Келі.

Тема 1.6. Нормальні підгрупи. Факторгрупа.

1. Означення нормальної підгрупи.
2. Критерій нормальності.

3. Операція на класах суміжності за нормальною фактор групою. Коректність операції.
4. Факторгрупа за нормальною підгрупою.

Тема 1.7. Відображення груп. Теорема про ізоморфізм груп.

1. Означення гомоморфізму груп. Властивості гомоморфізму.
2. Типи гомоморфізмів.
3. Ядро та образ гомоморфізму.
4. Теорема про ізоморфізм груп.

## **Розділ 2. Алгебраїчні системи з двома операціями.**

Тема 2.1. Означення кільця, типи кілець.

1. Кільце. Властивості елементів кільця.
2. Типи кілець.
3. Мультиплікативна група кільця з одиницею.
4. Характеристика кільця.

Тема 2.2. Підкільце, ідеал, типи ідеалів.

1. Означення підкільця.
2. Характеристика кільця.
3. Типи елементів кільця.
4. Ідеал кільця, типи ідеалів.

Тема 2.3. Поле, характеристика поля.

1. Властивості характеристики.
2. Характеристика поля.
3. Теорема про скінченне цілісне кільце.

Тема 2.4. Факторкільце. Відображення кілець.

1. Класи лишків за ідеалом.
2. Операція на класах лишків, її коректність.
3. Факторкільце за ідеалом.
4. Відображення кілець.
5. Теорема про ізоморфізм кілець.

Тема 2.5. Властивості факторкілець за ідеалами.

1. Структура ідеала у різних кільцях.
2. Головний ідеал.
3. Кільце головних ідеалів.
4. Властивості факторкілець.

## **Розділ 3. Факторіальні та Евклідові кільця.**

Тема 3.1. Факторіальне кільце.

1. Прості та оборотні елементи.
2. Означення факторіального кільця.
3. Критерій факторіальності.
4. Фундаментальна теорема арифметики.

Тема 3.2. Евклідове кільце.

1. Означення Евклідового кільця.
2. Алгоритм Евкліда, його наслідки.
3. Факторіальність Евклідових кілець.

Тема 3.3. Кільце цілих чисел як евклідове кільце.

1. Алгоритм Евкліда в кільці цілих чисел. Коректність його роботи.
2. Кількість кроків у алгоритмі.
3. Наслідки алгоритму Евкліда.

Тема 3.4. Кільце поліномів як евклідове кільце.

1. Означення кільця поліномів, його властивості.
2. Теорема Безу.
3. Корені поліномів.
4. Незвідні поліноми. Критерій незвідності для поліномів 2 та 3 степеню.

## **Розділ 4. Алгоритми та їх складність.**

Тема 4.1 .Час роботи алгоритмів.

1. Чим вимірюється час роботи алгоритму.
2. Час роботи арифметичних алгоритмів.
3. Час роботи алгоритму піднесення до степеню.
4. Схема Горнера.

Тема 4.2 .Імовірнісні алгоритми.

1. Означення імовірнісного алгоритму.
2. Монте-Карло та Лас-Вегас алгоритми.
3. Алгоритми з Оракулами.
4. Алгоритми розпізнавання мови.
5. Поліноміальна звідність задач.

### **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 у посібниках [2, 3], які містять основні означення, твердження та формули, необхідні для розв'язування задач, та приклади розв'язання найбільш типових задач.

## **Розділ 1. Алгебраїчні системи з однією операцією.**

Заняття 1. Основні алгебраїчні системи з однією операцією та їх властивості.

Розв'язок задач на визначення та властивості алгебраїчної системи.

Заняття 2. Теорема Лагранжа та її наслідки.

Розв'язок задач на застосування властивостей класів суміжності та наслідків теореми Лагранжа.

Заняття 3. Означення і властивості циклічних груп.

Розв'язок задач на визначення та властивості циклічних груп.

Заняття 4. Група перестановок та її властивості.

Розв'язок задач на обчислення у групі перестановок

Заняття 5. Дія групи на множину. Теорема Келі.

Розв'язок задач на доведення властивостей групи перестановок та її елементів.

Заняття 6. Нормальні підгрупи. Факторгрупа.

Розв'язок задач на побудову факторгруп, знаходження нормальних підгруп та на доведення їх властивостей.

Заняття 7. Відображення груп. Теорема про ізоморфізм груп.

Розв'язок задач на побудову відображень груп та на доведення їх властивостей.

## **Розділ 2. Алгебраїчні системи з двома операціями.**

Заняття 8. Означення кільця, типи кілець.

Розв'язок задач на визначення та властивості кілець.

Заняття 9. Підкілець, ідеал, типи ідеалів.

Розв'язок задач на визначення та властивості ідеалу та визначення типів ідеалів.

Заняття 10. Поле, характеристика поля.

Розв'язок задач на визначення та властивості поля, обчислення характеристики поля, доведення її властивостей.

Заняття 11. Факторкілець. Відображення кілець.

Розв'язок задач на побудову відображень кілець.

Заняття 12. Властивості факторкілець за ідеалами.

Розв'язок задач на визначення та властивості факторкілець.

## **Розділ 3. Факторіальні та Евклідові кільця.**

Заняття 13. Факторіальне кільце.

Розв'язок задач на визначення та факторіальних та Евклідових кілець.

Заняття 14. Евклідове кільце.

Розв'язок задач на визначення та властивості Евклідового кільця.

Заняття 15. Кільце цілих чисел як евклідове кільце.

Розв'язок задач на визначення та властивості кільця цілих чисел, використання алгоритму Евкліда та його наслідків.

Заняття 16. Кільце поліномів як евклідове кільце.

Розв'язок задач на визначення та властивості кільця поліномів.



## **Розділ 4. Алгоритми та їх складність.**

Заняття 17. Час роботи алгоритмів.

Розв'язок задач на визначення часу роботи різних алгоритмів.

Заняття 18. Імовірнісні алгоритми.

Розв'язок задач на визначення та властивості імовірнісних алгоритмів.

## **8. 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:

- обробка і осмислення інформації, отриманої безпосередньо на заняттях; лекційних та практичних;
- робота з відповідними підручниками та особистим конспектом лекцій;
- виконання підготовчої роботи до практичних занять та до написання МКР;
- підготовка до складання семестрового контролю (заліку).

## **• Політика та контроль**

### **9.**

#### **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 відповідає 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»).

## 10. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Видами контролю успішності засвоєння матеріалу дисципліни є модульна контрольна робота (МКР) та колоквиум.

### Робота на практичних заняттях

На практичних заняттях за кожен 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 55. 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 розглядалися 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 зараховується.

### Умови допуску до заліку

В таблиці наведено умови допуску до семестрового контролю.

№	Обов'язкова умова допуску до заліку	Критерій
1	Поточний рейтинговий бал	≥ 15
2	МКР	Виконана

3	Виконано не менше 80% ДЗ	
---	--------------------------	--

Додаткові умови допуску до заліку, які заохочуються:

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

### Колоквіум

Колоквіум приймається у 2 етапи і складається із двох частин. Перша частина є письмовою тривалістю 1 академічна година. 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 містить обговорення результатів письмової частини та відповіді на два додаткових питання з теорії і проходить після письмової. Максимальний рейтинговий бал за усну частину 5.

Рейтингові бали (максимум 5) за усну частину заліку нараховуються згідно наступних критеріїв:

- 5 — 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;
- 4 — 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;
- 3 — 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;
- 2 — 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 1 — 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 заліку після співбесіди зі студентом.

№	Контрольний захід	Бал	Кількість	Всього
1	Модульна контрольна робота	25	1	25
2	Практичні заняття	55	1	55
3	Колоквіум	20	1	20
	Всього			100

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Значення рейтингу	Оцінка ECTS
$95 \leq \mathbf{RD} \leq 100$	відмінно
$85 \leq \mathbf{RD} \leq 94$	дуже добре
$75 \leq \mathbf{RD} \leq 84$	добре
$65 \leq \mathbf{RD} \leq 74$	задовільно
$60 \leq \mathbf{RD} \leq 64$	достатньо
$\mathbf{RD} < 60$	незадовільно
$\mathbf{RD} < 40$	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)