

СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ (ПО 18)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Обов'язкова (нормативна) (цикл професійної та практичної підготовки)</i>
Форма навчання	<i>Змішана</i>
Рік підготовки, семестр	<i>3 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: (5 кред) 150 год Лекційних занять: 36 год Практичних занять: 18 год Лабораторних робіт (Комп'ютерних практикумів): 18 год Самостійної роботи студентів: 78 год</i>
Семестровий контроль/ контрольні заходи	<i>екзамен / МКР, РР</i>
Розклад занять	<i>http://ipt.kpi.ua/navchalnij-protses</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: доцент Завадська Людмила Олексіївна к.ф.-м.н., с.н.с. (zavadskalo-ipt@ill.kpi.ua) Практичні: доцент Завадська Людмила Олексіївна к.ф.-м.н., с.н.с. (zavadskalo-ipt@ill.kpi.ua) Комп'ютерний практикум: асистент Грубіян Євген Олександрович (grubian.euhen@gmail.com)</i>
Розміщення курсу	<i>GoogleClassroom: https://classroom.google.com/c/ODAwOTYxMjc3ODAw?cjc=2cdeghmr</i>

Програма навчальної дисципліни

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

Проблеми безпеки інформації за останні роки набули виключної актуальності, при цьому забезпечення захисту інформаційних технологій має комплексний характер. Серед різних методів захисту інформації (технічних, правових, організаційних та інших) важливе місце

займають криптографічні методи. Робота сучасних криптографічних систем (особливо асиметричних) базується на обчислювальних алгоритмах, які працюють з дуже великими числами або у певних алгебраїчних структурах.

Метою навчальної дисципліни «Спеціальні розділи обчислювальної математики» є формування у студентів здатностей застосовувати найуживаніші у криптології теоретико-числові, алгебраїчні та обчислювальні методи і алгоритми, а також практичних навичок їх програмної реалізації.

Предмет навчальної дисципліни: обчислювальні алгоритми, які лежать в основі побудови, функціонування та аналізу як симетричних, так і асиметричних сучасних криптосистем, включно з криптосистемами на еліптичних кривих, та їх ефективна комп'ютерна реалізація.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

Знати основні обчислювальні алгоритми, які використовуються при побудові, функціонуванні та аналізі сучасних криптографічних систем захисту інформації.

Вміти програмно реалізувати ефективні методи обчислень в арифметиці великих чисел, а також у скінченних полях характеристики 2, розв'язувати рівняння другого степеня у певних алгебраїчних структурах, будувати еліптичні криві у простому скінченному полі та полі характеристики 2 і виконувати операції у групах точок цих кривих, будувати реєстри зсуву з лінійним зворотним зв'язком над довільним скінченим полем та аналізувати властивості множини послідовностей, які вони генерують.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні компетентності та результати навчання за Стандартом вищої освіти:

Загальні компетентності

- ЗК 01 – Здатність учитися і оволодівати сучасними знаннями.
- ЗК 02 – Здатність застосовувати знання у практичних ситуаціях.
- ЗК 03 – Здатність генерувати нові ідеї (креативність).
- ЗК 05 – Здатність проведення досліджень на відповідному рівні.
- ЗК 06 – Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК 07 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- ЗК 08 – Знання та розуміння предметної області та розуміння професійної діяльності.
- ЗК 10 – Навички у використанні інформаційних і комунікаційних технологій.

Фахові компетентності

ФК 01 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

ФК 02 – Здатність виконувати завдання, сформульовані у математичній формі.

ФК 03 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

ФК 07 – Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.

ФК 13 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

ФК 14 – Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібну точність і надійність результату.

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 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 9 – Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач.

ПРН 11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символічних алгоритмів.

ПРН 13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.

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 успішного засвоєння даної дисципліни необхідне володіння знаннями та уміннями, які набувають студенти при вивченні таких дисциплін та кредитних модулів: «Дискретна математика 1», «Алгебра та геометрія 1», «Програмування 1,2», «Прикладна алгебра 1,2», «Алгоритми та структури даних», «Математична логіка та теорія алгоритмів», «Теорія складності»,

В свою чергу, результати навчання з дисципліни «Спеціальні розділи обчислювальної математики» використовуються при вивченні наступних дисциплін: «Симетрична криптографія», «Асиметричні криптографічні системи та протоколи 1,2», «Теорія інформації та кодування», «Теоретико-числові алгоритми в криптології».

3. Зміст навчальної дисципліни

Розділ 1. Арифметика великих чисел.

Тема 1.1. Алгоритми швидкого множення.

Тема 1.2. Алгоритми швидкої модулярної редукції.

Розділ 2. Операції у полях характеристики 2.

Тема 2.1. Поліноміальні та нормальні базиси, особливості операцій у них.

Тема 2.2. Оптиміальні нормальні базиси. Множення у ОНБ. Алгоритм Іто-Цудзії.

Розділ 3. Розв'язання квадратних рівнянь у деяких алгебраїчних структурах.

Тема 3.1. Квадратичність. Здобування квадратних коренів у кільцях лишків.

Тема 3.2. Розв'язання квадратних рівнянь у полях характеристики 2.

Розділ 4. Еліптичні криві.

Тема 4.1. Еліптичні криві над простими скінченними полями.

Тема 4.2. Еліптичні криві над полями характеристики 2.

Розділ 5. Регістри зсуву з лінійним зворотним зв'язком.

Тема 5.1. Регістри зсуву з лінійним зворотним зв'язком, способи їх завдання, періоди вихідних послідовностей, m -послідовності та їх властивості.

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. *Анісімов А.В.* Алгоритмічна теорія великих чисел. К.: Академперіодика, 2001. – 218с.
2. *Ковальчук Л. В., Яремчук Ю. Є.* Прикладна алгебра. Частина 1. Основи абстрактної алгебри. Вінниця: ВНТУ, 2015 – 98с.
3. *Завадська Л.О., Яковлев С.В.* Спеціальні розділи обчислювальної математики. Конспект лекцій. [електронний ресурс], – Режим доступу: https://www.dropbox.com/s/2bb7slab7u7kzb9/SROM_conspect.pdf.

Допоміжна рекомендована література

1. *T. Itoh and S. Tsujii.* A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases. *Information and Computation* 78:171-177, 1988.
2. Neal Koblitz. A course in number theory and cryptography. – Springer-Verlag, 1994. – 235 pp.
3. *J. L. Massey,* Shift-register synthesis and BCH decoding, *IEEE Trans. Information Theory*, IT-15 (1969), 122—127.

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 лекцій застосовуються пояснювально-ілюстративний метод та метод проблемного викладу. Для проведення практичних занять застосовуються репродуктивний та евристичний методи. Для проведення комп'ютерного практикуму застосовуються частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами задачу створення комп'ютерних програм, що реалізують типові алгоритми ефективних обчислень, їх реалізації на конкретних прикладах та формулювання висновків з результатів роботи.

У курсі використовуються безкоштовні версії наступного програмного забезпечення: Python, C++, Rust, можливі й інші відкриті мови програмування.

Лекційні заняття та комп'ютерний практикум проводяться у дистанційній формі на основі платформи проведення онлайн-зустрічей Zoom, а також електронної пошти та каналу Telegram.

Практичні заняття проводяться очно, при цьому як допоміжний інструмент використовується веб-сервіс Google Classroom.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Поняття великого числа, класичні алгоритми арифметики великих чисел. Алгоритми множення великих чисел, оцінка їх ефективності. Алгоритм Карацуби. Схема Горнера для піднесення до степеня.
2	Алгоритми модулярної редукції. Алгоритм Баррета.
3	Алгоритм Монтгомері, множення з модулярною редукцією.
4	Базиси скінченного поля. Поліноміальні та нормальні базиси. Операції у поліноміальному базисі.
5	Нормальні базиси у скінченному полі характеристики 2. Піднесення до квадрата, обчислення сліду у нормальному базисі.
6	Виконання операції множення у нормальному базисі. Мультиплікативна матриця. Гаусівські нормальні базиси, тип гаусівського нормального базису
7	Оптимальні нормальні базиси. Обчислення мультиплікативної матриці для оптимальних нормальних базисів I та II типу.
8	Обчислення оберненого за множенням елемента у нормальному базисі. Алгоритм Іто-Цудзії.
9	Квадратичні лишки. Символи Лежандра та Якобі, їх властивості.
10	Здобування квадратних коренів за простим модулем.
11	Здобування квадратних коренів за модулем, що є добутком двох нерівних простих чисел.
12	Розв'язання квадратних рівнянь у скінченних полях характеристики 2.
13	Означення еліптичної кривої над полями різних характеристик, уведення операції додавання точок еліптичної кривої, геометрична інтерпретація.
14	Вивід формул для координат суми точок еліптичної кривої над полем характеристики не 2 і не 3. Побудова еліптичної кривої на простим полем, приклади. Знаходження порядків точок кривої.
15	Побудова еліптичної кривої над полем характеристики 2. Приклади.
16	Властивості суперсингулярних та несуперсингулярних еліптичних кривих над полем характеристики 2. Операції додавання у групі точок цих кривих.
17	Поняття лінійної рекурентної послідовності над скінченним полем та регістра зсуву з лінійним зворотним зв'язком.
18	Характеристичний поліном лінійного регістра зсуву, періоди лінійних рекурентних послідовностей, послідовності максимального періоду.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Класичні алгоритми арифметики великих чисел. Алгоритм Карацуби, схема Горнера. Алгоритм Баррета, редукція Монтгомері.
2	Виконання операцій у полях характеристики 2 у поліноміальному та нормальному базисах.
3	Визначення типу гаусівського нормального базису. Виконання множення у

	нормальному базисі. Обчислення мультиплікативної матриці для ОНБ.
4	Здобування квадратних коренів за простим модулем та модулем, що є добутком двох нерівних простих чисел.
5	Розв'язання квадратних рівнянь у скінченних полях характеристики 2 у поліноміальному та нормальному базисах.
6	Побудова еліптичної кривої на простим полем характеристики не 2 і не 3. Обчислення координат суми точок. Знаходження порядків точок кривої.
7	Побудова еліптичної кривої над полем характеристики 2.
8	Побудова реєстрів зсуву з лінійним зворотним зв'язком за характеристичним поліномом, імпульсної функції, супроводжуючої матриці. Визначення циклової структури реєстра за властивостями характеристичного поліному.
9	Модульна контрольна робота.

Лабораторні роботи (Комп'ютерний практикум)

№ з/п	Назва теми заняття
1-2	Комп'ютерний практикум 1. Багаторозрядна арифметика.
3-4	Комп'ютерний практикум 2. Багаторозрядна модулярна арифметика.
5-6	Комп'ютерний практикум 3. Реалізація операцій у скінченних полях характеристики 2 (поліноміальний базис).
7-8	Комп'ютерний практикум 4. Реалізація операцій у скінченних полях характеристики 2 (нормальний базис).
9	Підведення підсумків.

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 домашніх завдань також необхідне для підготовки до модульної контрольної роботи.

При виконанні лабораторної роботи (комп'ютерного практикуму) студент має розібратися у відповідному теоретичному матеріалі за допомогою наданої літератури включно з методичними вказівками до даного практикуму, написати відповідну комп'ютерну програму, зробити за її допомогою вказані у методичних вказівках обчислення та зробити відповідні висновки.

Викладач, що проводить практикум, консультує студентів з питань його виконання, перевіряє правильність роботи програми та приймає усний звіт студента з питань створення комп'ютерної програми та відповідного теоретичного матеріалу. Крім того, викладачем проводиться перевірка програми на плагіат.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу. Для підготовки до виконання розрахункової роботи слід скористатися методичними вказівками до її виконання. Завдання на розрахункову роботу надає викладач, який також встановлює граничні строки для її здачі; студенту надається не менше трьох тижнів на виконання розрахункової роботи.

Самостійна робота студента

№ з/п	Вид самостійної роботи	Кількість годин СРС
1.	Підготовка до лекційних занять	9
2.	Підготовка до практичних занять	9
3.	Підготовка до КП	16
4.	Підготовка до МКР	2
5.	Виконання розрахункової роботи	12
6.	Підготовка до екзамену	30
	Загалом	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 навички, необхідні для виконання домашніх завдань, контрольної та розрахункової робіт. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички.

Пропущені контрольні заходи

Результат модульної контрольної роботи для студента, який не з'явився на контрольний захід, є нульовим. Якщо пропуск стався без поважної причини, студент має можливість написати контрольну, але максимальний бал за нього буде дорівнювати 50% від загальної кількості балів. У разі, якщо пропуск стався з поважних причин (наприклад, хвороби), про що бажано попередити викладача, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання модульної контрольної роботи не допускається.

За невчасно зданий комп'ютерний практикум знижується оцінка на кількість балів, що залежить від величини затримки і оголошується викладачем на першому занятті.

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.

Правила захисту індивідуальних завдань та лабораторних робіт

Захист виконаної лабораторної роботи (комп'ютерного практикуму) відбувається наступним чином: студент демонструє роботу написаної ним комп'ютерної програми (коду), викладач надає зауваження, вказує на недоліки (якщо такі є) та дає рекомендації студенту для їх

виправлення. Студент має можливість доопрацювати код і спробувати здати його повторно на одному з наступних занять.

Захист розрахункової роботи відбувається 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. Виконану та повністю оформлену розрахункову роботу кожен студент захищає індивідуально у встановлений викладачем термін.

Оголошення результатів контрольних заходів

Результати виконання контрольних заходів оголошуються кожному студенту окремо у його присутності (при дистанційній формі навчання – за опомогою системи Classroom або у листах електронної пошти) та супроводжуються оціночними листами, в яких студенти можуть побачити свою оцінку за певними критеріями, а також позначення основних помилок та коментарі до них.

На усному екзамені студенту оголошується оцінка після закінчення відповіді на кожне теоретичне питання або задачу із зазначенням усіх помилок, коментарями, зауваженнями тощо, після чого оголошується загальна оцінка за екзамен, що є сумою оцінок за теоретичні питання та задачі.

Академічна доброчесність

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

Норми етичної поведінки

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

Процедура оскарження результатів контрольних заходів

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

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

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

Поточний контроль:

№ з/п	Контрольний захід	Макс бал	Ваговий бал	Кількість	Всього
1.	Модульна контрольна робота	16	1	1	16
2.	Розрахункова робота	16	1	1	16
3.	Лабораторна робота (комп'ют. практикум)	7	1	4	28
4.	Екзамен	40	1	1	40
	Всього				100

Поточний контроль здійснюється шляхом опитування на практичних заняттях, а також при здачі лабораторних робіт (комп'ютерних практикумів), модульної контрольної роботи та розрахункової роботи. Виконання лабораторних робіт, МКР та РР є обов'язковим.

Критерії оцінювання МКР та РР:

- | | |
|---|-------------|
| • Повне виконання, неprincipові помилки | 14-16 балів |
| • Часткове виконання, істотні помилки | 8-13 балів |
| • Присутні ідеї без реалізації | 4-7 балів |
| • Роботу не зараховано | 0-3 бали |

Критерії оцінювання виконання лабораторних робіт (комп'ютерних практикумів):

Максимальна оцінка за виконання і задачу одного КП дорівнює 7 балів, з яких

5 балів — коректно виконаний комп'ютерний практикум (проходить весь набір стандартних тестів арифметичних операцій КП в необхідній алгебраїчній системі);

1 бал — коректно оформлений протокол комп'ютерного практикуму із завантаженням вихідного коду на GitHub;

1 бал — стилістика та оформлення коду: логічна модульна структура, коректні та логічні назви функцій, змінних, модулів.

Факторами, що можуть знизити оцінку (не менше нуля балів) є:

- невчасна здача КП: -1 бал за кожні 2 тижні після кінцевої дати здачі;
- арифметичні операції виконуються надзвичайно довго (понад 50 секунд за операцію): -2 бали;
- надмірне використання засобів штучного інтелекту (ШІ) без коректного пояснення студентом коду: від -1 до -7 балів залежно від ступеню зловживання ШІ та відсутності розуміння того, як працює комп'ютерний практикум;
- повний плагіат — лабораторна оцінюється в нуль балів. У цьому випадку студент має переробити код.

За активну роботу на **практичних заняттях** передбачено заохочувальні бали (0,5-1 бал за одне практичне заняття). На практичних заняттях обговорюється, зокрема, виконання домашніх завдань.

Заохочувальні бали (не більше 10 за семестр) не входять у 100 семестрових балів. Порядок нарахування заохочувальних балів оголошується викладачем на першому занятті.

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, 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.

Семестровий контроль: екзамен. Проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску є:

- семестровий рейтинг ≥ 30 ;
- написання МКР на позитивну оцінку (≥ 4)
- виконання та захист розрахункової роботи (≥ 4);
- здача всіх комп'ютерних практикумів.

Рейтингова оцінка за семестр складається з результатів роботи в семестрі (включно із заохочувальними балами) та оцінки відповіді на екзамені:

Студенти, які протягом семестру отримали менше ніж 30 балів, але виконали решту умов допуску, можуть з метою допуску до семестрової атестації (екзамену) пройти співбесіду, результат якої оцінюється максимум в 20 балів. Якщо результати співбесіди у сумі з балами, отриманими в семестрі, не менше за 30, студент отримує $R_c = 30$ та допуск до екзамену.

Критерії екзаменаційного оцінювання:

Підчас екзамену забороняється використання будь-яких додаткових довідкових матеріалів, користування телефонами та іншими гаджетами.

Оцінка студента на екзамені складається з балів, що він отримує за:

- 1) відповідь на теоретичне питання №1,
- 2) відповідь на теоретичне питання №2,
- 3) розв'язок задачі,
- 4) відповідь на додаткові питання.

4.1. Відповідь на теоретичні питання №1, №2

Максимальна кількість балів за відповідь на одне теоретичне питання – 12.

Результат кожної відповіді оцінюється за такими критеріями:

- | | |
|--|--------------|
| - повна правильна відповідь | 12 балів, |
| - повна правильна відповідь з незначними неточностями | 10-11 балів, |
| - неповна (у невеликій мірі) правильна відповідь з незначними неточностями | 8-9 балів, |
| - неповна відповідь з невеликою кількістю неточностей | 5-7 балів, |
| - часткова відповідь з помилками | 3-4 бали, |
| - відповідь на окремі несуттєві пункти в питанні з помилками | 1-2 бали, |
| - неправильна відповідь з суттєвими помилками або відповідь не дана | 0 балів. |

4.2. Розв'язок задачі.

Максимальна кількість балів за задачу – 10.

Результат розв'язання задачі оцінюється за такими критеріями:

- | | |
|---|------------|
| - виконання завдання (розв'язок) у повному обсязі, правильна відповідь | 10 балів, |
| - розв'язок з незначною кількістю непринципових неточностей або описок | 9 балів, |
| - хід розв'язку правильний, відповідь невірна з причини непринципових помилок | 6-8 балів, |
| - часткове виконання, є помилки, неповне обґрунтування або неправильна відповідь | 3-5 балів, |
| - хід розв'язку неправильний, відповідь невірна, але у виконанні присутнє раціональне зерно та деяке розуміння задачі | 1-2 бали, |
| - завдання не виконане або виконане з грубими помилками, немає обґрунтування відповіді | 0 балів. |

4.3. Відповідь на додаткові питання.

Для перевірки рівня засвоєння матеріалу курсу в цілому студент отримує три додаткових питання. Максимальна кількість балів за додаткові питання – 6.

Результат відповіді на кожне питання оцінюється за такими критеріями:

- вірна відповідь 2 бали,
- відповідь вірна в основному, з деякими неточностями 1 бал,
- відповідь невірна або відповіді немає 0 балів.

Максимальна кількість балів, що студент може отримати на іспиті, дорівнює:

$$R_E = 12 + 12 + 10 + 6 = 40 \text{ балів.}$$

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):

Складено: доцентом кафедри ММЗІ, к.ф.-м.н., с.н.с. Завадською Л.О.

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2025 від 25.06.2025р).

Погоджено Методичною комісією ФТІ (протокол № 6/2025 від 30.06.2025 р.)