Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра програмного забезпечення комп'ютерних систем

Алгоритмічно-програмні методи захисту інформації

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 рік навчання, 2 семестр*
Обсяг дисципліни	*Лекції: 36 год., лабораторні заняття: 18 год, самостійна робота: 66 год.*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота, календарний контроль*
Розклад занять	*Згідно розкладу на весняний семестр поточного навчального року (rozklad.kpi.ua)*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: к.т.н., доцент, Онай Микола Володимирович, onay@pzks.fpm.kpi.ua Лабораторні заняття: к.т.н., доцент, Онай Микола Володимирович, onay@pzks.fpm.kpi.ua
Розміщення курсу	Google classroom. Доступ надається зареєстрованим студентам.

Програма навчальної дисципліни

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

Вивчення дисципліни «Алгоритмічно-програмні методи захисту інформації» дозволяє сформувати у студентів компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з аналізом та використанням систем криптографічного захисту інформації.

Дисципліна «Алгоритмічно-програмні методи захисту інформації» забезпечує успішне виконання магістерської дисертації та засвоєння знань при виконанні індивідуальних завдань, при продовженні навчання в аспірантурі з різноманітних природничо-наукових дисциплін.

***Метою** вивчення дисципліни «Алгоритмічно-програмні методи захисту інформації» є формування у здобувачів освіти здатності аналізувати криптографічні системи; обирати криптографічний алгоритм відповідно до сформульованої задачі; забезпечувати роботу сучасних криптосистем; виконувати налагодження та розроблення програмного забезпечення для криптографічного захисту.*

***Предметом** дисципліни «Алгоритмічно-програмні методи захисту інформації» є методи побудови систем захисту інформації.*

Після засвоєння дисципліни «Алгоритмічно-програмні методи захисту інформації» ***результатами навчання*** *є:*

уміння:

- *аналізувати результати роботи відомих криптографічних протоколів;*
- *оцінювати стійкість криптографічних алгоритмів;*
- *узагальнювати отримані експериментальні результати*

досвід:

- *розроблення програмних засобів шифрування, дешифрування даних та створення електронного цифрового підпису;*
- *створення програмного забезпечення еліптичної криптографії;*
- *застосування криптографічних стандартів при розробленні програмного забезпечення.*

Дисципліна «Алгоритмічно-програмні методи захисту інформації» підсилює
ФК07 *Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах;*
та сприяє форуванню
ПРН10 *Модифікувати існуючі та розробляти нові алгоритмічні рішення детального проєктування програмного забезпечення.*

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

Успішному вивченню дисципліни «Алгоритмічно-програмні методи захисту інформації» передує вивчення дисципліни «Методологія інженерії програмного забезпечення» навчального плану підготовки магістрів за спеціальністю 121 Інженерія програмного забезпечення.

Отримані в результаті засвоєння дисципліни «Алгоритмічно-програмні методи захисту інформації» теоретичні знання та практичні уміння можуть бути корисні для проведення наукових досліджень за темою дисертації.

3. Зміст навчальної дисципліни

Дисципліна «Алгоритмічно-програмні методи захисту інформації» передбачає вивчення таких тем:

Тема 1. Проблематика криптографії

Тема 2. Загальні принципи побудови симетричних криптосистем

Тема 3. Сучасні симетричні криптосистеми

Тема 4. Елементи абстрактної алгебри

Тема 5. Класичні асиметричні шифри

Тема 6. Криптографія на еліптичних кривих

Тема 7. Електронний цифровий підпис

Модульна контрольна робота

Залік

4. Навчальні матеріали та ресурси

Базова література:

1. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря

Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с

3. Блінцов Володимир Степанович, Гальчевський Юрій Леонідович. Математичні основи криптології: Навчальний посібник для студ. вищих навч. закл. / Національний ун-т кораблебудування ім. адмірала Макарова. - Миколаїв : НУК, 2006. - 232с. : рис., табл; - ISBN 966-321-056

4. Горбенко Іван Дмитрович, Гріненко Тетяна Олексіївна. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. спец. "Комп'ютерні науки", "Комп'ютена інженерія", "Прикладна математика", "Інформаційна безпека" вищ. навч. закл. / Харківський національний ун-т радіоелектроніки. - Х. : ХНУРЕ, 2004. - Бібліогр.: с. 364-368.

5. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145-2002

Додаткова література:

1. Wenbo Mao Modern Cryptography: Theory and Practice : Pearson P T R; 1st edition

2. Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption : No Starch Press (November 6, 2017)

3. Thomas R. Shemanske Modern Cryptography and Elliptic Curves: A Beginner's Guide : American Mathematical Society (July 31, 2017)

4. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno Cryptography Engineering: Design Principles and Practical Applications Wiley; 1st edition (March 15, 2010)

5. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (Author) An Introduction to Mathematical Cryptography Springer; Softcover reprint of hardcover 1st ed. 2008 edition (December 1, 2010)

6. Seth James Nielson, Christopher K. Monson Practical Cryptography in Python: Learning Correct Cryptography by Example Apress; 1st ed. edition (September 27, 2019)

7. Lawrence C. Washington Elliptic Curves: Number Theory and Cryptography Chapman and Hall/CRC; 2nd edition (April 3, 2008)

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	*Тип навчального заняття*	*Опис навчального заняття*
Тема 1. Проблематика криптографії		
1	*Лекція 1. Проблематика криптографії*	*Класифікація криптографічних систем. Ключ шифрування. Симетрична криптосистема. Асиметрична криптосистема. Диференціальний, лінійний та інтерполяційний криптоаналіз. Сфери застосування криптографії. Імітозахист. Ідентифікація користувачів. Способи зберігання пароля. Контроль цілісності інформації. Аутентифікація інформації. Електронний цифровий підпис.*

Тема 2. Загальні принципи побудови симетричних криптосистем		
2	*Лекція 2. Загальні принципи побудови симетричних криптосистем*	*Моноалфавітні шифри заміни. Шифр Цезаря. Узагальнений шифр Цезаря. Шифр Плейфейера. Шифр Хіла. Поліалфавітні шифри заміни. Шифр Віженера. Шифри перестановки.*
Тема 3. Сучасні симетричні криптосистеми		
3	*Лекція 3. Шифр Фейстеля*	*Шифр Фейстеля як практична реалізація ідей Шеннона. Блочний шифр. Раунд шифрування. Алгоритм обчислення раундових підключів.*
4	*Лабораторне заняття 1*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів: шифр Цезаря, шифр Плейфейєра, шифр Лестера Хілла.*
5	*Лекція 4. Стандарт шифрування даних (DES)*	*Конкурс NBS. Спрощений DES. Раундова функція. Перестановка з розширенням. S-матриця. Лавинний ефект. Схема генерування підключів. Перестановка з вибором. Режими роботи DES. Багатократні DES. Розширений DES.*
6	*Лекція 5. Стандарт AESя*	*Конкурс NIST. Вимоги до нового алгоритму. Критерії для аналізу алгоритму. SP-мережі. Структура "Квадрат". Алгоритм Rijndael. Способи подання блока відкритого тексту та ключа. Етапи шифрування алгоритму Rijndael. Заміна байтів та подання даних, як елементів поля GF(28). Математична складова операції перемішування стовпців. Матричне подання етапу перемішування стовпців. Формування раундового ключа з основного. Особливості побудови алгоритму дешифрування. Алгоритм дешифрування з прямим порядком перетворень.*
7	*Лабораторне заняття 2*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів: шифр перестановки, шифр Віженера.*
8	*Лекція 6. Міжнародний алгоритм шифрування даних (IDEA) та шифр Blowfish*	*Відмінність від класичної структури Фейстеля. МА-сктруктура. Особливості генерування підключів в IDEA. Взаємозв'язок підключів дешифрування з підключами шифрування.Основні математичні операції в IDEA. Алгоритм Blowfish. Вибір початкогового значення P-масиву та таблиці замін. Порівняння алгоритмів IDEA та Blowfish з іншими симетричними криптосистемами.*

9	*Лекція 7. Шифр RC5 та загальні підходи до побудови блочних і поточних шифрів*	*Параметри для визначення алгоритму RC5. Способи запису багатобайтових слів. Особливості формування раундових підключів. Режими роботи RC5. Потокові системи шифрування. Синхронні системи та системи із самосинхронізацією. Регістри зсуву з лінійним зворотним зв'язком. Примітивний многочлен. Приклади використання потокових шифрів у системах зв'язку.*
10	*Лабораторне заняття 3*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів: потрійний DES (реалізувати три модифікації), розширений DES (реалізувати три модифікації), міжнародний алгоритм шифрування даних (IDEA)*
15	*Модульна контрольна робота 1*	
Тема 4. Елементи абстрактної алгебри		
11	*Лекція 8. Арифметика у класах лишків за модулем, Теорема Ферма та Ейлера*	*Основні алгебраїчні структури. Групоїд. Напівгрупа. Моноїд. Група. Адитивні та мультиплікативні групи. Порядок елемента. Твірний елемент групи. Циклічна група. Алгебраїчна структура кільце. Поняття подільності та порівнянності за модулем. Дільник нуля. Клас конгруентності. Підгрупа. Теорема Лагранжа. Канонічне розкладення числа.Функція Ейлера. Приведена система лишків. Теорема Ейлера. Теорема Ферма як частковий випадок теореми Ейлера. Первісні або примітивні корені. Методи пошуку первісних коренів.*
12	*Лабораторне заняття 4*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів: шифр RC5 (використовувати значення параметрів не менше ніж 32/12/8), шифр Rijndael*
13	*Лекція 9. Алгоритми перевірки чисел на простоту та арифметика довгих чисел*	*Тести чисел на простоту. Тест за допомогою повного перебору. Тест Люка-Лемера для чисел Мерсена. Тест Ферма. Арифметика довгих цілих чисел. Множення Карацуби. FFT-множення. Особливості виконання операції знаходження остачі за модулем для довгих цілих чисел.*
Тема 5. Класичні асиметричні шифри		
14	*Лекція 10. Генерування випадкових простих чисел та принципи побудови криптосистем з відкритим ключем*	*Тест Мілера-Рабіна. Тест Соловея-Штрасена. AKS-тест. Одностороння функція. Протоколи розподілу ключів.*
16	*Лекція 11. Обмін ключами за схемою Діффі-Хелмана, алгоритм*	*Основна математична операція у схемі Діффі-Хелмана. Зв'язок задачі дискретного логарифмування з алгоритмом Діффі-Хелмана.*

	RSA та методи факторизації чисел	*Узагальнення алгоритму Діффі-Хелмана. Алгоритм створення відкритого та секретного ключів RSA. Передача зашифрованого повідомлення за допомогою алгоритму RSA. Зв'язок алгоритму RSA із задачею факторизації. Вибір параметрів алгоритму RSA. Факторизація цілих чисел. Перебір дільників. ρ-метод Полларда. Алгоритм Полларда-Штрасена.*
17	*Лабораторне заняття 5*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів або виконувати задані математичні операції у скінченних алгебраїчних структурах: алгоритм шифрування RSA, алгоритм цифрового підпису RSA*
18	*Лекція 12. Схема Ель-Гамаля та методи знаходження дискретного логарифму*	*Вибір ключів схеми Ель-Гамаля. Відкриті та секретні параметри схеми Ель-Гамаля. Алгоритм шифрування та дешифрування за методом Ель-Гамаля. Індекс елемента за модулем. Умова існування індексу. Одностороння функція. Дискретне логарифмування. Метод Шенкса.*
Тема 6. Криптографія на еліптичних кривих		
19	*Лекція 13. Визначення поняття еліптичної кривої*	*Еліптична крива у формі Вейерштрасса. Елементарні операції над точками еліптичної кривої. Проективна система координат. Сингулярні еліптичні криві.*
20	*Лабораторне заняття 6*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних за допомогою одного з алгоритмів або виконувати задані математичні операції у скінченних алгебраїчних структурах: алгоритм шифрування Ель-Гамаля, алгоритм цифрового підпису Ель-Гамаля, алгоритм пошуку оберненого елемента поля GF(pm) у многочленному поданні, метод Шенкса та метод узгодження*
21	*Лекція 14. Еліптичні криві над скінченними полями GF(p) та $GF(p^m)$*	*Різновиди полів Галуа. Мультиплікативна група скінченного поля. Порядок мультиплікативної групи кільця лишків. Пошук мультиплікативно оберненого елемента в полі GF(p). Особливості виконання операцій над елементами поля GF(pm). Суперсинуглярні та несуперсингулярні еліптичні криві. Група точок еліптичної кривої.*
22	*Лекція 15. Еліптичний аналог обміну ключами за схемою Діффі-Хелмана*	*Основна математична операція у схемі Діффі-Хелмана на еліптичній кривій. Множення точки еліптичної кривої на число. Зв'язок задачі дискретного логарифмування на еліптичній кривій з алгоритмом Діффі-Хелмана.*

		Узагальнення алгоритму Діффі-Хелмана в еліптичній криптографії.
Тема 7. Електронний цифровий підпис		
23	*Лекція 16. Стандарт цифрового підпису (DSS), алгоритм RSA та схема Ель-Гамаля в режимі цифрового підпису*	*Рекомендовані алгоритми генерування простих чисел для DSA. Використання DES в алгоритмі DSA. Основні параметри схеми цифрового підпису. Система перевірки реалізації алгоритму на відповідність стандарту. Особливості використання алгоритму RSA для формування цифрового підпису. Алгоритм формування цифрового підпису за допомогою схеми Ель-Гамаля. Перевірка цифрового підпису.*
24	*Лекція 17. Еліптичні алгоритми формування електронного цифрового підпису*	*Алгоритм DSA на еліптичній кривій. Особливості генерування ключів ECDSA. Алгоритм обчислення та перевірки цифрового підпису. Вимоги до еліптичної кривої, що використовується в алгоритмів ECDSA. Еліптичні аналоги алгоритмів RSA та Ель-Гамаля в режимі цифрого підпису.*
25	*Лабораторне заняття 7*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних або створення електронного цифрового підпису за допомогою одного з алгоритмів: ECDSA, EdDSA*
26	*Лабораторне заняття 8*	*Розробити програму на будь-якій мові програмування, яка буде реалізувати шифрування та дешифрування даних або створення електронного цифрового підпису за допомогою одного з алгоритмів: ECMQV, ECQV*
27	*Модульна контрольна робота*	

6. Самостійна робота студента

Дисципліна «Алгоритмічно-програмні методи захисту інформації» ґрунтується на самостійній підготовці до аудиторних занять на теоретичні та практичні теми.

№ з/п	*Назва теми, що виноситься на самостійне опрацювання*	*Кількість годин*	*Література*
1	*Підготовка до лекції №1*	*2*	*1-3*
2	*Підготовка до лекції №2*	*2*	*1-3*
3	*Підготовка до лекції №3*	*2*	*1-3*
4	*Підготовка до лабораторного заняття №1*	*2*	*1-3*
5	*Підготовка до лекції №4*	*2*	*1-3*
6	*Підготовка до лекції №5*	*2*	*1-3*
7	*Підготовка до лабораторного заняття №2*	*2*	*1-3*
8	*Підготовка до лекції №6*	*2*	*1-3*

9	*Підготовка до лекції №7*	*2*	*1-3*
10	*Підготовка до лабораторного заняття №3*	*2*	*1-3*
11	*Підготовка до модульної контрольної роботи 1*	*8*	*1-3*
12	*Підготовка до лекції №8*	*2*	*2-5*
13	*Підготовка до лабораторного заняття №4*	*2*	*2-5*
14	*Підготовка до лекції №9*	*2*	*2-5*
15	*Підготовка до лекції №10*	*2*	*2-5*
16	*Підготовка до лекції №11*	*2*	*2-5*
17	*Підготовка до лабораторного заняття №5*	*2*	*2-5*
18	*Підготовка до лекції №12*	*2*	*2-5*
19	*Підготовка до лекції №13*	*2*	*2-5*
20	*Підготовка до лабораторного заняття №6*	*2*	*2-5*
21	*Підготовка до лекції №14*	*2*	*2-5*
22	*Підготовка до лекції №15*	*2*	*2-5*
23	*Підготовка до лекції №16*	*2*	*2-5*
24	*Підготовка до лекції №17*	*2*	*2-5*
25	*Підготовка до лабораторного заняття №7*	*2*	*2-5*
26	*Підготовка до лабораторного заняття №8*	*2*	*2-5*
27	*Підготовка до модульної контрольної роботи 2*	*8*	*2-5*

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- *Відвідування лабораторних занять може бути епізодичним та за потреби захисту робіт комп'ютерного практикуму.*
- *Правила поведінки на заняттях: активність, повага до присутніх, відключення телефонів.*
- *Дотримання політики академічної доброчесності.*
- *Правила захисту робіт комп'ютерного практикуму: роботи повинні бути зроблені згідно з варіантом здобувача освіти, що визначається псевдовипадково за генератором псевдовипадкових чисел (www.random.org) на початку семестру.*
- *Правила призначення заохочувальних та штрафних балів є наступними.*

Заохочувальні бали нараховуються за:
- точні та повні відповіді під час опитувань за матеріалами лекцій. Протягом семестру на лекціях відбувається ***бліц-опитування*** *за темами минулих лекцій. Максимальна кількість балів за бліц-опитування: 3 бали.*
- творчий підхід у виконанні робіт комп'ютерного практикуму. Максимальна кількість балів за всі роботи – 2 бали.

Штрафні бали нараховуються за:
- плагіат (код програми не відповідає варіанту завдання, ідентичність коду програми серед різних робіт) у роботах комп'ютерного практикуму: -5 балів за кожну спробу.

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

Протягом семестру аспіранти виконують 8 лабораторних занять. Максимальна кількість балів за кожне лабораторне заняття: 6 балів.

Бали нараховуються за:
- якість виконання лабораторної роботи: 0-2 бали;
- відповідь на теоретичні запитання під час захисту лабораторної роботи: 0-2 бали;
- своєчасне представлення роботи до захисту: 0-2 бали.

Критерії оцінювання якості виконання:
2 бали – робота виконана якісно, в повному обсязі;
1 бал – робота виконана в повному обсязі, але містить незначні помилки;
0 балів – робота виконана не в повному обсязі, або містить суттєві помилки.

Критерії оцінювання відповіді:
2 бали – відповідь повна, добре аргументована;
1 бал – в цілому відповідь правильна, але має недоліки або незначні помилки;
0 балів – немає відповіді або відповідь неправильна.

Критерії оцінювання своєчасності представлення роботи до захисту:
2 бали – робота представлена до захисту не пізніше вказаного терміну;
0 балів – робота представлена до захисту пізніше вказаного терміну.

Максимальна кількість балів за виконання та захист лабораторних робіт:
6 балів × 8 лаб. = 48 балів.

*Завдання на **модульну контрольну роботу** складається з 3 запитань – 2 теоретичних та 1 практичного. Відповідь на кожне теоретичне запитання оцінюється 15 балами, а відповідь на практичне запитання оцінюється 22 балами.*

Критерії оцінювання кожного теоретичного запитання контрольної роботи:
14-15 балів – відповідь правильна, повна, добре аргументована;
11-13 балів – відповідь правильна, розгорнута, але не дуже добре аргументована;
8-10 балів – в цілому відповідь правильна, але має недоліки;
5-7 балів – у відповіді є незначні помилки;
1-4 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь неправильна.

Критерії оцінювання практичного запитання контрольної роботи:
19-22 бали – відповідь правильна, розрахунки виконані у повному обсязі;
14-18 балів – відповідь правильна, але не дуже добре підкріплена розрахунками;
9-13 балів – в цілому відповідь правильна, але має недоліки;
5-8 балів – у відповіді є незначні помилки;
1-4 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь неправильна.

Максимальна кількість балів за модульну контрольну роботу:
15 балів × 2 теоретичні запитання + 22 бали × 1 практичне запитання = 52 бали.

Рейтингова шкала з дисципліни дорівнює:
$R_c = R_{ком.практ} + R_{МКР} = 48$ *балів + 52 бали = 100 балів.*

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
На першій атестації (8-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 50 % від максимальної кількості балів (20 балів), яку може отримати студент до першої атестації.

На другій атестації (14-й тиждень) студент отримує «зараховано», якщо його поточний рейтинг не менше 50 % від максимальної кількості балів (35 балів), яку може отримати студент до другої атестації.

Семестровий контроль: ***залік***

Умови допуску до семестрового контролю:
За семестрового рейтингу (R_C) не менше 60 балів та зарахуванні усіх робіт комп'ютерного практикуму аспірант отримує залік «автоматом» відповідно до таблиці (Таблиця відповідності рейтингових балів оцінкам за університетською шкалою). В іншому разі він має виконати залікову контрольну роботу.

Необхідною умовою допуску до виконання залікової контрольної роботи є виконання і захист комп'ютерного практикуму.

Студент може спробувати підвищити свою оцінку шляхом написання залікової контрольної роботи, при цьому його бали, отримані за семестр, анулюються («жорстка» система оцінювання).

Склад та критерії оцінювання залікової контрольної роботи:

Завдання на ***залікову контрольну роботу*** *складається з 4 запитань – 2 теоретичних та 2 практичних. Відповідь на кожне теоретичне та практичне запитання оцінюється 25 балами.*

Критерії оцінювання кожного теоретичного запитання контрольної роботи:
24-25 балів – відповідь правильна, повна, добре аргументована;
21-23 бали – відповідь правильна, розгорнута, але не дуже добре аргументована;
17-20 балів – в цілому відповідь правильна, але має недоліки;
12-16 балів – у відповіді є незначні помилки;
1-11 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь неправильна.

Критерії оцінювання практичного запитання контрольної роботи:
24-25 балів – відповідь правильна, розрахунки виконані у повному обсязі;
21-23 бали – відповідь правильна, але не дуже добре підкріплена розрахунками;
17-20 балів – в цілому відповідь правильна, але має недоліки;
12-16 балів – у відповіді є незначні помилки;
1-11 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь неправильна.

Максимальна кількість балів за модульну контрольну роботу:
25 балів × 2 теоретичних запитання + 25 балів × 2 практичних запитання = 100 балів.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
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

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік запитань, які виносяться на семестровий контроль.

Робочу програму навчальної дисципліни (силабус):

Складено к.т.н., доц., Онай М.В.

Ухвалено кафедрою ПЗКС (протокол №8 від 25.01.2023)

Погоджено Методичною комісією факультету прикладної математики (протокол №6 від 27.01.2023)