



# ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

## Робоча програма навчальної дисципліни (Силабус)

### Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>12 Інформаційні технології</i>
Спеціальність	<i>121 Інженерія програмного забезпечення</i>
Освітня програма	<i>Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>4 рік навчання, 8 семестр</i>
Обсяг дисципліни	<i>Лекції: 36 год., лабораторні заняття: 18 год, самостійна робота: 66 год.</i>
Семестровий контроль/ контрольні заходи	<i>Залік, модульна контрольна робота, календарний контроль</i>
Розклад занять	<i>Згідно розкладу на весняний семестр поточного навчального року (rozklad.kpi.ua)</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>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</i>

### Програма навчальної дисципліни

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

*Вивчення дисципліни «Програмні засоби захисту інформації» дозволяє сформуванню у студентів компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з аналізом та використанням систем криптографічного захисту інформації.*

*Дисципліна «Програмні засоби захисту інформації» забезпечує успішне виконання бакалаврської кваліфікаційної роботи та засвоєння знань і виконання індивідуальних завдань, при продовженні навчання в аспірантурі з різноманітних природничо-наукових дисциплін.*

*Метою вивчення дисципліни «Програмні засоби 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 «Програмні засоби захисту інформації» є методи побудови систем захисту інформації.*

*Вивчення дисципліни «Програмні засоби захисту інформації» підсилює формування у здобувачів освіти **фахових компетентностей (ФК)**, необхідних для розв'язання практичних задач професійної діяльності:*

***ФКО6** Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).*

*Вивчення дисципліни «Програмні засоби захисту інформації» сприяє формуванню у студентів наступних **програмних результатів навчання (ПРН)** за освітньою програмою:*

**ПРН21** Знати засоби, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

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

Успішному вивченню дисципліни «Програмні засоби захисту інформації» передують вивчення дисципліни «Алгоритмічне забезпечення мультимедійних та інформаційно-пошукових систем» навчального плану підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення.

Отримані в результаті засвоєння дисципліни «Програмні засоби захисту інформації» теоретичні знання та практичні уміння можуть бути корисні для виконання випускної кваліфікаційної роботи бакалавра.

## **3. Зміст навчальної дисципліни**

Дисципліна «Програмні засоби 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. Євсєєв, 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'ютерна 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
<i>Тема 1. Проблематика криптографії</i>		
1	<i>Лекція 1. Проблематика криптографії</i>	<i>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.</i>
<i>Тема 2. Загальні принципи побудови симетричних криптосистем</i>		
2	<i>Лекція 2. Загальні принципи побудови симетричних криптосистем</i>	<i>Моноалфавітні шифри заміни. Шифр Цезаря. Узагальнений шифр Цезаря. Шифр Плейфейера. Шифр Хіла. Поліалфавітні шифри заміни. Шифр Віженера. Шифри перестановки.</i>
<i>Тема 3. Сучасні симетричні криптосистеми</i>		
3	<i>Лекція 3. Шифр Фейстеля</i>	<i>Шифр Фейстеля як практична реалізація ідей Шеннона. Блочний шифр. Раунд шифрування. Алгоритм обчислення раундових підключів.</i>

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 AES	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. MA-структура. Особливості генерування підключів в IDEA. Взаємозв'язок підключів дешифрування з підключами шифрування. Основні математичні операції в IDEA. Алгоритм Blowfish. Вибір початкового 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. Поточкові системи шифрування. Синхронні системи та системи із самосинхронізацією. Регістри зсуву з лінійним зворотним зв'язком. Примітивний многочлен. Приклади використання поточкових 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. Частина 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-Штрассена. AKS-тест. Одностороння функція. Протоколи розподілу ключів.
16	Лекція 11. Обмін ключами за схемою Діффі-Хелмана, алгоритм RSA та методи факторизації чисел	Основна математична операція у схемі Діффі-Хелмана. Зв'язок задачі дискретного логарифмування з алгоритмом Діффі-Хелмана. 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. р-метод Поларда. Алгоритм Поларда-Штрассена.
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-Гамала та методи знаходження дискретного логарифму	Вибір ключів схеми Ель-Гамала. Відкриті та секретні параметри схеми Ель-Гамала. Алгоритм шифрування та дешифрування за методом Ель-Гамала. 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-



		<i>Гамалія, алгоритм цифрового підпису Ель-Гамалія, алгоритм пошуку оберненого елемента поля <math>GF(p^m)</math> у многочленному поданні, метод Шенкса та метод узгодження</i>
21	<i>Лекція 14. Еліптичні криві над скінченними полями <math>GF(p)</math> та <math>GF(p^m)</math></i>	<i>Різновиди полів Галуа. Мультиплікативна група скінченного поля. Порядок мультиплікативної групи кільця лишків. Пошук мультиплікативно оберненого елемента в полі <math>GF(p)</math>. Особливості виконання операцій над елементами поля <math>GF(p^m)</math>. Суперсингулярні та несуперсингулярні еліптичні криві. Група точок еліптичної кривої.</i>
22	<i>Лекція 15. Еліптичний аналог обміну ключами за схемою Діффі-Хелмана</i>	<i>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.</i>
<i>Тема 7. Електронний цифровий підпис</i>		
23	<i>Лекція 16. Стандарт цифрового підпису (DSS), алгоритм RSA та схема Ель-Гамалія в режимі цифрового підпису</i>	<i>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-Гамалія. Перевірка цифрового підпису.</i>
24	<i>Лекція 17. Еліптичні алгоритми формування електронного цифрового підпису</i>	<i>Алгоритм DSA на еліптичній кривій. Особливості генерування ключів ECDSA. Алгоритм обчислення та перевірки цифрового підпису. Вимоги до еліптичної кривої, що використовується в алгоритмі ECDSA. Еліптичні аналоги алгоритмів RSA та Ель-Гамалія в режимі цифрового підпису.</i>
25	<i>Лабораторне заняття 7</i>	<i>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</i>
26	<i>Лабораторне заняття 8</i>	<i>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</i>
27	<i>Модульна контрольна робота. Частина 2</i>	

## 6. Самостійна робота студента

Дисципліна «Програмні засоби 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 лекцій	16	1-4
2	Підготовка до комп'ютерного практикуму	27	1-4
3	Підготовка до модульної контрольної роботи. Частина 1	9	1-4
4	Підготовка до модульної контрольної роботи. Частина 2	9	1-4
5	Підготовка до заліку	5	1-4

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

**Відвідування занять.** Відсутність на аудиторному занятті не передбачає нарахування штрафних балів, оскільки фінальний рейтинговий бал студента формується виключно на основі оцінювання результатів навчання. Разом з тим, обговорення результатів виконання тематичних завдань, а також презентація / публічний виступ та участь у обговореннях та доповнення на семінарах оцінюватимуться під час аудиторних занять. Для активної участі у роботі семінару студент готується за рекомендованою викладачем до певного семінарського заняття літературою. Участь у роботі семінару також передбачає підготування доповідей та співдоповідей у межах усіх занять.

**Пропущені контрольні заходи оцінювання.** Кожен студент має право відпрацювати пропущені з поважної причини (лікарняний, мобільність тощо) заняття за рахунок самостійної роботи. Детальніше за посиланням: <https://kpi.ua/files/n3277.pdf>.

**Процедура оскарження результатів контрольних заходів оцінювання.** Студент може підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право аргументовано оскаржити результати контрольних заходів, пояснивши з яким критерієм не погоджуються відповідно до оціночного. Календарний контроль проводиться з метою підвищення якості навчання студентів та моніторингу виконання студентом вимог силабусу.

**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>.

**Інклюзивне навчання.** Засвоєння знань та умінь в ході вивчення дисципліни «Науково-дослідна діяльність у комп'ютерній інженерії» може бути доступним для більшості осіб з особливими освітніми потребами, окрім здобувачів з серйозними вадами зору, які не дозволяють виконувати завдання за допомогою персональних комп'ютерів, ноутбуків та/або інших технічних засобів.

**Навчання іноземною мовою.** У ході виконання завдань студентам може бути рекомендовано звернутися до англомовних джерел. Призначення заохочувальних та штрафних балів Відповідно до Положення про систему оцінювання результатів навчання сума всіх заохочувальних балів не може перевищувати 10% рейтингової шкали оцінювання.

Всі студенти повинні відвідувати лекційні та практичні заняття, на яких потрібно активно працювати над засвоєнням навчального матеріалу. За об'єктивних причин (наприклад - хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі індивідуально за погодженням із керівником курсу.

**Політика щодо дедлайнів та перескладання:**

Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

**Політика щодо академічної доброчесності:**

Усі письмові роботи перевіряються на наявність плагиату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт заборонені (в т. ч. із використанням мобільних пристроїв).

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

Протягом семестру студенти 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 20 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:

$R_c = R_{\text{ком.практ}} + R_{\text{опитув}} + R_{\text{МКР}} = 48 \text{ балів} + 52 \text{ бали} = 100 \text{ балів.}$

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.

Аспірант 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:

<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

## **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)