МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Декан факультету
комп'ютерних інформаційних
технологій

Ігор ЯКИМЕНКО

«29» 08 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи

Віктор ОСТРОВЕРХОВ

«29» 08 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни

«МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»

Ступінь вищої освіти – **бакалавр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека та захист інформації**
Освітньо-професійна програма – **«Кібербезпека»**

Кафедра кібербезпека

Форма навчання	Курс	Сем.	Лекції (год.)	Практ. заняття (год.)	ІРС (год.)	Тренінг, (год.)	СРС (год.)	Разом (год.)	Залік (сем)	Іспит (сем)
ДФН	2	3,4	60	60	7	16	127	270	3	4

29.08.2025

Тернопіль
2025

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності – 125 Кібербезпека та захист інформації, затвердженої на засіданні Вченої ради ЗУНУ протокол № 10 від 23 червня 2024 р.

Робочу програму склав доцент кафедри кібербезпеки, к.т.н. Якименко Ігор Зіновійович

Робоча програма затверджена на засіданні кафедри кібербезпеки протокол № 1 від 26.08.2025р.

Завідувач кафедри Василь ЯЦКІВ

Гарант ОП Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСИЦПЛІНИ "МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ"

1. Опис дисципліни "Математичні основи захисту інформації"

Дисципліна – Математичні методи захисту інформації	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 10	Галузь знань 12 Інформаційні технології	Нормативна навчальна дисципліна циклу дисциплін професійної та практичної підготовки Мова викладання - *українська*
Кількість залікових модулів – 9	Спеціальність 125 Кібербезпека та захист інформації	Рік підготовки – 3 Семестр – 5, 6
Кількість змістових модулів – 6	Ступінь вищої освіти – бакалавр	Лекції – 60 год. Практичні заняття – 60 год.
Загальна кількість годин – 270		Самостійна робота – 127 год. Тренінг – 16 год Індивідуальна робота – 7 год.
Тижневих годин: 3 семестр – 9 год. з них аудиторних – 4 год. 4 семестр – 9 год. з них аудиторних – 4 год.		Вид підсумкового контролю – залік, іспит

2. Мета й завдання вивчення дисципліни

2.1. Мета вивчення дисципліни

Метою вивчення дисципліни є розвиток математичного мислення, набуття студентами глибоких, узагальнених та міцних математичних знань та вмінь, необхідних для вивчення фахових дисциплін за спеціальністю 125 «Кібербезпека та захист інформації» та для практичної професійної діяльності; оволодіння навичками розв’язання задач математичного захисту інформації та аналізу загроз інформаційній безпеці, вироблення умінь та навичок застосування математичних методів до розв’язування технічних задач з інформаційної та/або кібербезпеки та захисту інформації.

2.2 Завдання вивчення дисципліни.

Основними завданнями вивчення дисципліни є формування компетентностей та умінь щодо здатності розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 13. Здатність виконувати оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах.

2.4 Передумови для вивчення дисципліни.

Теоретичною базою вивчення дисципліни «Математичні методи захисту інформації» є попередні навчальні дисципліни: «Вища математика»

2.5. Результати навчання

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.

ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах.
ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

3. Програма дисципліни

Змістовний модуль 1. **Подільність цілих чисел**.

Тема1. Множини натуральних, цілих та раціональних чисел

Поняття множини. Аксіоми Пеано. Аксіоматичне означення методу математичної індукції. Алгебраїчні операції на множині натуральних чисел. Відношення порядку множини натуральних чисел. Класи еквівалентності у множині раціональних чисел. Подільність у множині цілих чисел. Теорема про ділення з остачею.

Тема 2. Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне

Поняття НСД. Алгоритм Евкліда. Властивості НСД. Взаємно прості числа та їхні основні властивості. Найбільший спільний дільник кількох чисел. Найменше спільне кратне (НСК) цілих чисел.

Тема 3. Прості й складені числа

Прості числа та їхні властивості. Нескінченність множини простих чисел. Розклад складених чисел на прості множники. Основна теорема арифметики. Решето Ератосфена. Канонічне задання натуральних чисел.

Тема 4. Числові функції

Мультиплікативні числові функції. Функції $\tau(n)$, $\sigma(n)$, $\{x\}$, $\lfloor x \rfloor$. Функція Ойлера $\varphi(n)$, функція Мебіуса $\mu(n)$, функція Кармайкла $\lambda(n)$.

Змістовний модуль 2. Конгруенції (порівняння)

Тема 5. Конгруенції

Означення конгруенції. Приклади. Властивості конгруенцій.

Тема 6. Повна та зведена система лишків

Повна система лишків. Зведена система лишків. Теорема Ойлера і Ферма. Мультиплікативність функцій Ойлера.

Тема 7. Лінійні конгруенції з одним невідомим

Конгруенції першого степеня. Способи розв'язування конгруенцій першого степеня: метод спроб, метод рівносильних перетворень.

Тема 8. Обернений елемент за множенням

Розвязування діафантових рівнянь. Китайська теорема про лишки. Системи конгруенцій з одним невідомим. Тести простоти. Тест псевдопростоти Ферма.

Тема 9. Конгруенції вищих степенів

Конгруенції n-го степеня за простим модулем. Побудова рівносильних конгруенцій. Число розв'язків конгруенцій n-го степеня за простим модулем. Конгруенції n-го степеня за складеним модулем.

Тема 10. Конгруенції другого степеня

Загальні положення. Квадратичні лишки. Конгруенція за простим непарним модулем. Символ Лежандра. Символ Якобі.

Тема 11. Первісні корені

Означення порядків чисел і класів чисел за даним модулем. Властивості порядків за модулем. Первісні корені. Знаходження первісних коренів за елементарними модулями

Тема 12. Дискретні логарифми (індекси)

Поняття індекса (дискретного логарифма). Побудова таблиць індексів. Застосування індексів до розв'язання конгруенцій.

Тема 13. Арифметичні застосування теорії конгруенцій

Ознаки подільності. Перевірка результатів арифметичних дій. Перетворення звичайного дробу в десятковий.

Змістовний модуль 3. Елементи теорії груп

Тема 14. Алгебри. Бінарна алгебраїчні операція

Поняття бінарної операції. Напівгрупа. Нейтральний та обернений елемент.

Тема 15. Група. Підгрупа

Поняття групи. Приклади груп. Властивості груп. Підгрупи. Критерій підгрупи. Циклічні групи. Порядок елемента групи. Таблиці Келі.

Тема 16. Група перестановок

Симетрична групи (група перестановок). Добуток перестановок. Порядок перестановки. Знак перестановки. Парність перестановки. Інверсія.

Змістовний модуль 4. Елементи теорії кілець

Тема 17. Многочлени, подільність многочленів

Поняття многочлена. Операції над многочленами. Теорема про ділення многочленів з остачею. Алгоритм ділення многочлена з остачею. Означення НСД та НСК двох многочленів. Знаходження найбільшого спільного дільника двох многочлена (алгоритм Евкліда).

Тема 18. Теорема Безу та схема Горнера

Незвідні многочлена. Основна теорема алгебри Кратні корені. Похідна многочлена. Результант многочленів. Дискримінант многочлена.. Формули Вієта.

Тема 19. Кільце. Підкільце

Означення кільця. Підкільце. Приклади числових кілець. Типи кілець. Властивості кілець. Асоціативні кільця. Комутативні кільця. Кільця з одиницею. Дільники нуля. Оборотні елементи. Область цілісності. Підкільце кільця. Критерій підкільця. Китайська теорема про остачі.

Тема 20. Фактор-кільця та ідеали

Ідеали кільця. Приклади ідеалів. Головні ідеали. Операції над ідеалами. Конгруенції за ідеалом. Кільця лишків кільця за ідеалом. Фактор-кільце. Зв'язок між класами кільця цілих чисел за ідеалом I та класами лишків кільця цілих чисел за модулем m.

Тема 21. Теорема Ейлера, мала теорема Ферма.

Мультиплікативна група кільця лишків за модулем n. Приклади груп лишків. Основні властивості груп лишків. Ознаки подільності. Порівняння по натуральному модулю. Системи лишків. Повна система лишків. Гомоморфізм кілець. Ізоморфізм кілець.

Тема 22. Поле. Підполе

Означення поля. Приклади. Характеристика поля. Підполе поля. Критерій підполя. Розширення поля. Алгебра над полем. Ізоморфізм полів.

Змістовний модуль 5. Теорія еліптичних кривих

Тема 23. Елементарні відомості про еліптичні криві

Основні визначення. Способи побудови еліптичних кривих.

Тема 24. Умова несингулярності еліптичної кривої

Операція додавання і побудова групи точок еліптичної кривої. Відшукання точок еліптичної кривої над скінченним полем.

Тема 25. Число елементів групи точок еліптичної кривої

Порядок точки еліптичної кривої. Вибір еліптичної кривої і базової точки

Змістовний модуль 6. Генератори псевдовипадкових чисел

Тема 26. Псевдовипадкова послідовність

Основні визначення випадкової послідовності. Вимоги до псевдовипадкових послідовностей. Лінійна рекурентна послідовність з максимальним періодом.

Тема 27. Псевдовипадкова послідовність на базі багатомодульних перетворень

Методи і засоби перевірки на випадковість.

Тема 28. Генератор псевдовипадкових чисел

Лінійний конгруентний генератор псевдовипадкових чисел. Метод Фібоначчі із запізненням. Генератор псевдовипадкових чисел на основі алгоритму BBS. Генератори псевдовипадкових чисел на основі регістрів зсуву з оберненим зв'язком.

4. Структура залікового кредиту дисципліни «Математичні методи захисту інформації»

Теми занять	Кількість годин					
	Лекції	Практ. заняття	СРС	Тре-н інг	ІРС	Контр. заходи
Змістовний модуль 1. Подільність цілих чисел						
Тема 1. Множини натуральних, цілих та раціональних чисел	2	2	4	3	1	Поточн. опит.
Тема 2. Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне	2	2	5			
Тема 3. Прості й складені числа	2	2	4			
Тема 4. Числові функції	3	3	5			
Змістовний модуль 2. Елементи теорії груп						
Тема 5. Конгруенції	2	2	5	5	2	Поточн. опит.
Тема 6. Повна та зведена система лишків	2	2	4			
Тема 7. Лінійні конгруенції з одним невідомим	2	2	4			
Тема 8. Обернений елемент за множенням	2	2	4			
Тема 9. Конгруенції вищих степенів	3	3	5			
Тема 10. Конгруенції другого степеня	2	2	5			
Тема 11. Первісні корені	2	2	5			
Тема 12. Дискретні логарифми (індекси)	2	2	5			
Тема 13. Арифметичні застосування теорії конгруенцій	2	2	4			
Змістовний модуль 3. Функціональні структури САУ. Типові ланки. Передавальні функції						
Тема 14. Алгебри. Бінарна алгебраїчні операція	2	2	5	2	1	Поточн. опит.
Тема 15. Група. Підгрупа	2	2	4			
Тема 16. Група перестановок	2	2	4			
Змістовний модуль 4. Елементи теорії кілець						
Тема 17. Многочлени, подільність многочленів	2	2	5	2	1	Поточн. опит.
Тема 18. Теорема Безу та схема Горнера	3	3	4			
Тема 19. Кільце. Підкільце	2	2	5			
Тема 20. Фактор-кільця та ідеали	2	2	5			
Тема 21. Теорема Ейлера, мала теорема Ферма	2	2	4			
Тема 22. Поле. Підполе	2	2	5			
Змістовний модуль 5. Теорія еліптичних кривих						
Тема 23. Елементарні відомості про еліптичні криві	2	2	4	2	1	Поточн. опит.
Тема 24. Умова несингулярності еліптичної кривої	3	2	5			
Тема 25. Число елементів групи точок еліптичної кривої	2	2	4			
Змістовний модуль 6. Генератори псевдовипадкових чисел						
Тема 26. Псевдовипадкова послідовність	2	2	4	2	1	Поточн. опит.
Тема 27. Псевдовипадкова послідовність на базі багатомодульних перетворень	2	2	5			
Тема 28. Генератор псевдовипадкових чисел	2	2	5			
Всього:	**60**	**60**	**127**	**16**	**7**	

5. Тематика практичних робіт

Теми практичних занять з дисципліни "Математичні методи захисту інформації"

Практична робіт 1. Операції з цілими числами та метод математичної індукції

- Виконання операцій у множинах натуральних і цілих чисел
- Застосування методу математичної індукції для доведення теорем

- Розв'язування задач на подільність цілих чисел

Практична робота 2. Алгоритм Евкліда та його застосування

- Знаходження НСД двох і більше чисел за допомогою алгоритму Евкліда
- Обчислення НСК цілих чисел
- Розв'язування задач на взаємно прості числа

Практична робота 3. Факторизація чисел та прості числа

- Розклад натуральних чисел на прості множники
- Застосування решета Ератосфена
- Канонічне представлення натуральних чисел

Практична робота 4. Обчислення числових функцій

- Обчислення функції Ойлера $\varphi(n)$
- Знаходження значень функції Мебіуса $\mu(n)$
- Розрахунок функції Кармайкла $\lambda(n)$

Практична робота 5. Основні операції з конгруенціями

- Виконання арифметичних операцій з конгруенціями
- Застосування властивостей конгруенцій
- Розв'язування простих задач на конгруенції

Практична робота 6. Системи лишків та теорема Ойлера

- Побудова повних і зведених систем лишків
- Застосування теорем Ойлера і Ферма
- Обчислення степенів за модулем

Практична робота 7. Лінійні конгруенції

- Розв'язування лінійних конгруенцій методом спроб
- Застосування методу рівносильних перетворень
- Знаходження кількості розв'язків конгруенцій

Практична робота 8. Системи конгруенцій та оберненні елементи

- Розв'язування систем конгруенцій за допомогою китайської теореми про лишки
- Знаходження оберненних елементів за множенням
- Розв'язування діофантових рівнянь

Практична робота 9. Конгруенції вищих степенів

- Розв'язування конгруенцій n-го степеня за простим модулем
- Побудова рівносильних конгруенцій
- Аналіз кількості розв'язків конгруенцій

Практична робота 10. Квадратичні лишки

- Знаходження квадратичних лишків за простим модулем
- Обчислення символів Лежандра і Якобі
- Розв'язування квадратичних конгруенцій

Практична робота 11. Первісні корені

- Знаходження порядків елементів за модулем
- Обчислення первісних коренів за простим модулем
- Застосування первісних коренів у криптографії

Практична робота 12. Дискретні логарифми

- Побудова таблиць індексів
- Розв'язування конгруенцій за допомогою індексів
- Застосування дискретних логарифмів

Практична робота 13. Застосування теорії конгруенцій

- Побудова ознак подільності
- Перевірка арифметичних обчислень
- Перетворення дробів у десяткові

Практична робота 14. Бінарні операції та напівгрупи

- Визначення бінарних операцій на множинах
- Знаходження нейтральних та обернених елементів
- Перевірка властивостей напівгруп

Практична робота 15. Групи та підгрупи

- Перевірка групових властивостей
- Побудова таблиць Келі для скінченних груп
- Знаходження порядків елементів групи

Практична робота 16. Група перестановок

- Виконання операцій з перестановками
- Обчислення порядків перестановок
- Визначення парності перестановок

Практична робота 17. Операції з многочленами

- Ділення многочленів з остачею
- Знаходження НСД многочленів за алгоритмом Евкліда
- Розклад многочленів на множники

Практична робота 18. Корені многочленів

- Застосування теореми Безу та схеми Горнера
- Знаходження кратних коренів многочленів
- Обчислення дискримінанта многочлена

Практична робота 19. Кільця та їх властивості

- Перевірка кільцевих властивостей
- Знаходження дільників нуля та оборотних елементів
- Визначення областей цілісності

Практична робота 20. Ідеали та фактор-кільця

- Побудова ідеалів кілець
- Виконання операцій над ідеалами
- Побудова фактор-кілець

Практична робота 21. Гомоморфізми кілець

- Перевірка властивостей гомоморфізмів
- Знаходження ядер і образів гомоморфізмів
- Застосування теорем про ізоморфізм

Практична робота 22. Поля та їх розширення

- Перевірка властивостей полів
- Знаходження характеристик полів
- Побудова розширень полів

Практична робота 23. Еліптичні криві над дійсними числами

- Побудова еліптичних кривих
- Перевірка умов несингулярності
- Візуалізація еліптичних кривих

Практична робота 24. Операції на еліптичних кривих

- Виконання операції додавання точок
- Знаходження точок еліптичних кривих над скінченними полями
- Обчислення оберненних елементів

Практична робота 25. Параметри еліптичних кривих для криптографії

- Обчислення порядку групи точок
- Знаходження порядку базової точки
- Вибір параметрів для криптографічних застосувань

Практична робота 26. Псевдовипадкові послідовності

- Генерація лінійних рекурентних послідовностей
- Перевірка періодичності послідовностей
- Оцінка якості псевдовипадкових послідовностей

Практична робота 27. Тестування випадковості

- Застосування статистичних тестів
- Аналіз розподілу псевдовипадкових чисел
- Перевірка автокореляційних властивостей

Практична робота 28. Реалізація генераторів псевдовипадкових чисел

- Програмування лінійного конгруентного генератора
- Реалізація генератора на основі алгоритму BBS
- Імплементація генераторів на регістрах зсуву
- Порівняльний аналіз різних генераторів

6. Самостійна робота студентів

На самостійну роботу кожному здобувачу пропонується написання і представлення реферату на запропоновану або самостійно вибрану тему.

Орієнтовна тематика рефератів:

1. Історія розвитку теорії чисел та її застосування в криптографії.
2. Алгоритм Евкліда та його розширення: математичні основи та криптографічні застосування.
3. Прості числа та їх роль у сучасній криптографії.
4. Тести простоти: детерміністичні та ймовірнісні методи.
5. Факторизація великих чисел та безпека RSA.
6. Китайська теорема про лишки в криптографічних обчисленнях.
7. Квадратичні лишки та символи Лежандра в криптоаналізі.
8. Первісні корені та їх застосування в алгоритмі Діффі-Хеллмана.
9. Дискретні логарифми: складність та методи розв'язування.
10. Еліптичні криві над скінченними полями: математичні властивості.
11. Криптографія еліптичних кривих: переваги та застосування.
12. Протоколи обміну ключами на еліптичних кривих (ECDH).
13. Цифрові підписи на еліптичних кривих (ECDSA).
14. Поліноміальна арифметика та її роль в алгоритмі AES.
15. Поля Галуа та їх застосування в криптографії.
16. Лінійні конгруентні генератори псевдовипадкових чисел.
17. Генератор Блюма-Блюма-Шуба та його криптографічні властивості.
18. Статистичні тести якості псевдовипадкових послідовностей.
19. Потокові шифри на основі лінійних регістрів зсуву.
20. Математичні основи блочних шифрів та S-блоків.
21. Теорія інформації та ентропія в контексті криптографії.
22. Квантова криптографія: математичні принципи та перспективи.
23. Постквантова криптографія: нові математичні підходи.
24. Гомоморфне шифрування та його математичні основи.
25. Математичні методи криптоаналізу та їх еволюція.

7. Організація і проведення тренінгу з дисципліни «Математичні методи захисту інформації»

Тема тренінгу: розв'язування задач з різних розділів «Математичних методів захисту інформації».

Цей тренінг охоплює ключові аспекти «Математичних методів захисту інформації», поєднуючи теоретичні знання з практичними навичками. Студенти отримають практичні навички розв'язування задач, які будуть їм потрібні у професійній діяльності в галузі кібербезпеки та криптографії.

Мета тренінгу: забезпечити студентів комплексними теоретичними знаннями та практичними навичками в галузі розв'язування практичних задач з «Математичних методів захисту інформації».

Перелік завдань для тренінгу:

1. Розв'язування задач з розділу «Теорія чисел та конгруенції».
2. Розв'язування задач з розділу «Алгебраїчні структури».
3. Розв'язування задач з розділу «Еліптичні криві».
4. Розв'язування задач з розділу «Генератори псевдовипадкових чисел».

8. Методи навчання

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; самостійна робота студентів; робота в Інтернет

9. Методи оцінювання

В процесі вивчення дисципліни «Математичні методи захисту інформації» використовуються наступні методи оцінювання навчальної роботи студентів:

– поточне оцінювання;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання практичних занять;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий екзамен.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Математичні методи захисту інформації» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Семестр 3 – залік

Модуль 1		Модуль 2		Модуль 3	Модуль 4
20%	20%	20%	20%	5%	15%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за оцінювання практичних робіт №1-6.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів, за темами 1-6	Оцінка за даний модуль визначається як середнє арифметичне оцінювання практичних робіт №7-13.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів, за темами 7-13	Визначається як середнє арифметичне за виконання завдань за темами №1-2 тренінгу	Оцінка за виконаний і представлений реферат на вибрану тему.

Семестр 4 – екзамен

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінг	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за оцінювання практичних робіт №14-22.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів, за темами 14-22	Оцінка за даний модуль визначається як середнє арифметичне за оцінювання практичних робіт №23-28	1.Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів, за темами №23-28	Визначається як середнє арифметичне за виконання завдань за темами №3-4 тренінгу	Оцінка за виконаний і представле-ний реферат на вибрану тему.	1. Теорети-чні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

СЕМЕСТР 3 (ЗАЛІК)

Поточне оцінювання під час практичних робіт:

90–100 балів – у повному обсязі володіє навчальним матеріалом з математичних основ захисту інформації, вільно, самостійно та аргументовано його викладає під час відповідей на практичних заняттях, глибоко та всебічно розкриває зміст теоретичних питань з подільності цілих чисел, конгруенцій, алгебраїчних структур; демонструє розуміння криптографічних застосувань математичних методів.

75–89 балів – достатньо повно володіє навчальним матеріалом з теорії чисел та основних алгебраїчних структур, але при викладанні деяких питань з конгруенцій вищих степенів, первісних коренів або дискретних логарифмів не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки в обчисленнях.

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст з математичних методів захисту інформації, але без глибокого всебічного аналізу властивостей числових функцій, конгруенцій або групових структур, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки в застосуванні алгоритму Евкліда, розв'язуванні конгруенцій.

60–64 бали – не в повному обсязі володіє навчальним матеріалом з основних розділів курсу, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань з подільності чисел, числових функцій, основ теорії груп та кілець, допускаючи при цьому суттєві неточності.

1–59 балів – не володіє навчальним матеріалом з математичних методів захисту інформації, не розкриває зміст теоретичних питань з базових розділів теорії чисел та алгебраїчних структур.

СЕМЕСТР 4 (ЕКЗАМЕН)

Поточне оцінювання

Аналогічні критерії як для семестру 3, але з фокусом на:

- Розділ 3: Теорія еліптичних кривих
- Розділ 4: Генератори псевдовипадкових чисел

Тренінг

90–100 балів – у повному обсязі володіє навчальним матеріалом з математичних методів захисту інформації, вільно самостійно та аргументовано його використовує під час розв'язування практичних криптографічних задач тренінгу; демонструє глибоке розуміння взаємозв'язку між теоретичними математичними концепціями та їх практичним застосуванням у криптографії.

75–89 балів – достатньо повно володіє навчальним матеріалом з математичних основ криптографії, але при розв'язуванні окремих задач тренінгу з реалізації криптографічних алгоритмів або аналізу їх безпеки не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки в математичних обчисленнях.

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при розв'язування задач тренінгу з математичних методів криптографії, але без глибокого всебічного аналізу математичних властивостей алгоритмів, обґрунтування та аргументації вибору параметрів, допускаючи при цьому суттєві неточності та помилки в реалізації алгоритмів.

60–64 бали – не в повному обсязі володіє навчальним матеріалом з математичних основ захисту інформації, фрагментарно (без аргументації та обґрунтування) його використовує, частково розв'язуючи задачі тренінгу з базових криптографічних перетворень, допускаючи при цьому суттєві неточності.

1–59 балів – не володіє навчальним матеріалом з математичних методів криптографії, не розв'язує задачі тренінгу з реалізації криптографічних алгоритмів, не бере участі у колективних завданнях під час проведення тренінгу.

Самостійна робота

90–100 балів – зміст та захист реферату з математичних методів захисту інформації свідчить про високий рівень опанування навчального матеріалу, реферат містить елементи самостійного дослідження сучасних тенденцій у застосуванні математичних методів в

криптографії, аналіз новітніх криптографічних алгоритмів або математичних підходів до забезпечення інформаційної безпеки, студент на високому рівні виявляє творчий підхід до аналізу математичних аспектів кібербезпеки.

75–89 балів – зміст та захист реферату загалом свідчить про належний рівень опанування навчального матеріалу з математичних основ криптографії, можуть бути несуттєві не доопрацювання в частині глибокого математичного аналізу або недостатньо повного розкриття криптографічних застосувань, студент належно виявляє творчий підхід до дослідження обраної теми.

60–74 балів – поставлені завдання з дослідження математичних аспектів захисту інформації виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими з математичної точки зору, свідчать про недостатній рівень опанування теоретичного матеріалу з теорії чисел, алгебраїчних структур або їх криптографічних застосувань; студент припускається значних помилок у викладенні математичних концепцій, в окремих моментах виявляє творчий підхід до виконання завдань.

1–59 балів – завдання з дослідження математичних методів захисту інформації практично не виконані; відсутні авторські напрацювання в галузі математичних основ криптографії; грубі помилки у викладенні базових математичних понять та їх застосування в криптографії, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до дослідження математичних проблем інформаційної безпеки.

Модульний контроль, Екзамен

(Модульний), Екзаменаційний білет складається з двох теоретичних питань, за кожне з яких можна отримати від 0 до 30 балів (максимум 60 балів), та однієї практичної задачі, за яку можна отримати від 0 до 40 балів.

Теоретичні питання (по 30 балів кожне):

15–30 балів – студент отримує цю кількість балів, якщо у повному обсязі володіє навчальним матеріалом з математичних методів захисту інформації, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання з теорії чисел, конгруенцій, алгебраїчних структур, еліптичних кривих або генераторів псевдовипадкових чисел, демонструє розуміння їх криптографічних застосувань.

1–14 балів – студент отримує цю кількість балів, якщо в цілому володіє навчальним матеріалом з основних розділів математичних методів захисту інформації, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання з базових математичних структур, допускаючи при цьому суттєві неточності в математичних викладках, відповіді на запитання щодо криптографічних застосувань нечіткі.

Практичне завдання (40 балів):

25–40 балів – студент отримує цю кількість балів, якщо у повному обсязі володіє навчальним матеріалом з математичних методів, правильно розв'язує практичну задачу з обчислення числових функцій, розв'язування конгруенцій, операцій на алгебраїчних структурах, роботи з еліптичними кривими або аналізу псевдовипадкових послідовностей і правильно інтерпретує отримані результати з точки зору їх застосування в криптографії, демонструє самостійність виконання математичних обчислень.

10–24 балів – у достатньому обсязі володіє навчальним матеріалом з основних математичних методів захисту інформації, правильно розв'язує практичну задачу, але на додаткові контрольні запитання про криптографічні застосування результатів відсутня повна відповідь, допускає несуттєві неточності в проміжних обчисленнях та фрагментарно (без повної аргументації) інтерпретує отримані результати, демонструє самостійність виконання основних етапів розв'язання.

1–9 балів – не в повному обсязі володіє матеріалом з математичних основ захисту інформації, фрагментарно розв'язує практичне завдання з елементарних розділів теорії чисел або алгебраїчних структур, допускає суттєві неточності в базових математичних обчисленнях, поверхнево його викладає, недостатньо розкриває зміст поставлених питань щодо практичного застосування математичних методів у криптографії.

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1-28
2	Персональні комп'ютери	1-28
3	Наявність доступу до мережі Інтернет	1-28
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-28
5	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-28
6	Операційна система: Windows 10/11, Linux Ubuntu. Базове програмне забезпечення: MS Office, телекомунікаційне програмне забезпечення (Internet Explorer, Opera, Google Chrome, Firefox)	1-28
7	Математичні пакети: Python з бібліотеками (NumPy, SymPy, Matplotlib), Sage, Mathematica або аналогічні	4, 8-12, 23-28
8	Спеціалізоване програмне забезпечення для роботи з великими числами (GMP Library, PARI/GP)	2-3, 8-13
9	Криптографічні бібліотеки та інструменти (OpenSSL, Crypto++, PyCrypto)	11-12, 23-28
10	Онлайн-калькулятори для модульної арифметики та роботи з простими числами	2-13
11	Програмне забезпечення для візуалізації еліптичних кривих (GeoGebra, Desmos)	23-25
12	Інструменти для статистичного аналізу псевдовипадкових послідовностей (NIST Statistical Test Suite)	26-28

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Авдєєва Т.В. Прикладна алгебра. Алгебраїчні структури. Морфізми. Основи теорії зображень груп. Навчальний посібник /Т.В. Авдєєва, В.М. Горбачук.- К.: НТУУ «КПІ», 2015. – 56 с.
2. Бобало Ю. Я. Інформаційна безпека : навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
3. Болдарєва О. М. Методичні рекомендації до самостійної роботи з дисципліни «Алгебра і теорія чисел» (курс лекцій) / О. М. Болдарєва, О. М. Яковлєва. - Одеса : ПНПУ імені К. Д. Ушинського, 2021. - 54 с. URL: http://dspace.pdpu.edu.ua/handle/123456789/11802?locale=uk

4. Гаврилків В.М. Елементи теорії груп та теорії кілець: навчальний посі бник / В.М. Гаврилків. — Івано-Франківськ: Голіней, 2018. — 148 с.
5. Головащук Н.С., Кочубінська Є.А., Овсієнко С.А.. Збірник задач з теорії кілець (базовий курс). – Навчальний посі бник для студентів механіко – математичного факультету. – К.: Видавничо–поліграфічний центр "Київський універси тет", 2013. – 86 с.
6. Дармосюк В. М. Алгебра та теорія чисел: конгруенції та їх застосування (завдання для самостійної роботи та методичні вказівки до їх виконання)/ В. М. Дармосюк, О. Ю. Пархоменко: посібник для самостійної та дистанційної роботи студентів. – Миколаїв: Миколаївський національний університет ім. В.О. Сухомлинського, 2021– 152 с.
7. Кулаковська І. В. Дискретна математика. Частина 1. Множини, відношення та математичні основи криптографії. Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз»: методичні вказівки / І. В. Кулаковська. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. – 100 с.
8. Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021 – 244 с.
9. Оглобліна О. І. Елементи теорії чисел: навч. посіб. / О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. – Суми: Сумський державний університет, 2015. – 186 с.
10. Стасюк М. Елементи математичних основ криптографії: навчальний посібник / Марта СТАСЮК – Львів: ЛДУ БЖД, 2021. – 216 с.
11. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем : навч. посіб. / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький: ХНУ, 2021. 174 с.
12. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 2018. – 816 p.
13. Washington L. Elliptic Curves: Number Theory and Cryptography / L. Washington. – 2nd Edition. – Chapman and Hall/CRC, 2018. – 513 p.
14. Hoffstein J. An Introduction to Mathematical Cryptography / J. Hoffstein, J. Pipher, J. Silverman. – 2nd Edition. – Springer, 2014. – 538 p.
16. Баняс Б. Методи формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем / Б. Баняс // Матеріали IX науково-технічної конференції „Інформаційні моделі, системи та технології", 08-09 грудня 2021 року. — Т. : ТНТУ, 2021. — С. 25–27.
17. Бедратюк Л.П. Дискретні струкутри. Навч.посібник для студентів вищих навч.закладів.- Хмельницький: ХНУ, 2014. – 106 с.
18. Мілінчук Ю.А. Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи забезпечення безпеки інформації» для бакалаврів напряму підготовки 12 Інформаційні технології/ Ю.А. Мілінчук, І.А. Сєчкін –Дніпро: НТУ «ДП», 2020. – 9 с.
19. Петрушак, В.С. Аналіз методів та засобів формування псевдовипадкової послідовності чисел/ В. С. Петрушак, І. В. Столярчук // Вісник Хмельницького національного університету. Технічні науки. – 2016. – №1. – С. 49-51.
20. Баришев Ю. В. Методи формування псевдовипадкових чисел для псевдонедетермінованих геш-функцій [Текст] / Ю. В.Баришев, Т. А. Кравчук // Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації», м. Вінниця, 19-21 квітня 2016 р. – Вінниця: ВНТУ, 2016. – С. 58-60.
21. Жовмір О. А. Застосування ланцюгових дробів до розв'язування діофантових рівнянь [Електронний ресурс] / О. А. Жовмір, Н. В. Сачанюк-Кавецька // Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2023)», Вінниця, 22 червня 2023 р. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2023/paper/view/17290.

22. Федоренко Н.Д. Дискретна математика: навчальний посібник у двох частинах / Н.Д. Федоренко та ін. – Ч. 1. – К.: КНУБА, 2014 – 104 с.
23. Silverman J. The Arithmetic of Elliptic Curves / J. Silverman. – 2nd Edition. – Springer, 2009. – 513 p.
24. Shoup V. A Computational Introduction to Number Theory and Algebra / V. Shoup. – 2nd Edition. – Cambridge University Press, 2009. – 580 p.
25. Ferguson N. Cryptography Engineering: Design Principles and Practical Applications / N. Ferguson, B. Schneier, T. Kohno. – Wiley, 2010. – 384 p.
26. Cryptology ePrint Archive [Електронний ресурс]. – Режим доступу: https://eprint.iacr.org/
27. NIST Post-Quantum Cryptography Standardization [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography
28. Number Theory Web [Електронний ресурс]. – Режим доступу: http://www.numbertheory.org/
29. The On-Line Encyclopedia of Integer Sequences (OEIS) [Електронний ресурс]. – Режим доступу: https://oeis.org/
30. Sage Mathematical Software System [Електронний ресурс]. – Режим доступу: https://www.sagemath.org/
31. OpenSSL Cryptography and SSL/TLS Toolkit [Електронний ресурс]. – Режим доступу: https://www.openssl.org/