ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Тетяна ГОВОРУЩЕНКО
«__05__» ____09____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	10 кредитів ЄКТС
Шифр дисципліни	ОПП.03
Мова навчання	Українська
Статус дисципліни	Обов'язкова (професійної підготовки)
Факультет	Інформаційних технологій
Кафедра	Вищої математики та комп'ютерних застосувань

Форми здобуття освіти	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	2	5	150	72	36		36		78			+	
Д	2	3	5	150	68	34		34		82				+
Разом ДФН			**10**	**300**	**140**	**70**		**70**		**160**				

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю 125 «Кібербезпека та захист інформації»

Програма складена _____ к.пед.н., доцент _____ Наталія САМАРУК
Підпис — Вчений ступінь, звання — Ініціали, прізвище викладача

Схвалена на засіданні кафедри вищої математики та комп'ютерних застосувань

Протокол № 1 від "30" 08 2024 р. Зав. кафедри _____ Андрій РАМСЬКИЙ

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис — Ініціали, прізвище

Хмельницький 2024

МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Тип (статус) дисципліни	Обов'язкова професійної підготовки
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Другий-третій
Кількість призначений кредитів ЄКТС	10,0
Форми здобуття освіти, для яких викладається дисципліна	Денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни повинен: *адаптуватися* в умовах частої зміни технологій професійної діяльності, *організовувати* власну професійну діяльність; *аналізувати*, аргументувати, приймати рішення на основі вивчених математичних теорій для розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *обирати* оптимальні математичні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, *критично осмислювати* їхню ефективність; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних математичних теорій захисту інформації; *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах на основі математичних теорій та понять.

Зміст навчальної дисципліни. Подільність цілих чисел, конгруентності (порівняння), ланцюгові дроби, елементи теорії груп та теорії кілець, системи числення, теорія еліптичних кривих, генератори псевдовипадкових чисел.

Пререквізити − вища математика, теорія ймовірностей та математична статистика.

Кореквізити – прикладна криптологія.

Запланована навчальна діяльність: лекцій – 70 год., практичних занять – 70 год., самостійної роботи – 160 год.; разом – 300 год.

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і візуалізації), практичні заняття (з використанням методів проблемного навчання, застосування ІКТ, практикумів), самостійна робота (індивідуальні домашні завдання).

Форми оцінювання результатів навчання: усне опитування, письмові самостійні та контрольні роботи, захист індивідуальних домашніх завдань, колоквіуми, комп'ютерне тестування.

Вид семестрового контролю: залік – 2 семестр, іспит – 3 семестр.

Навчальні ресурси:

1. Стасюк М. Елементи математичних основ криптографії : навчальний посібник / Марта СТАСЮК – Львів : ЛДУ БЖД, 2021. – 216 с.

2. Оглобліна О. І. Елементи теорії чисел : навч. посіб. / О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. – Суми : Сумський державний університет, 2015. – 186 с

3. 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.

4. Модульне середовище. URL: https://msn.khmnu.edu.ua/course/view.php?id=9020

5. Електронна бібліотека. URL: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: канд. пед. наук, доцент Самарук Н.М.

3) Пояснювальна записка

Дисципліна «Математичні основи захисту інформації» є однією із фундаментальних дисциплін і займає провідне місце у професійній підготовці фахівців освітнього рівня «бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації». У відповідності з діючим навчальним планом дану дисципліну студенти спеціальності «Кібербезпека та захист інформації» вивчають у 2-му та 3-му семестрах.

Пререквізити − вища математика, теорія ймовірностей та математична статистика.

Кореквізити – прикладна криптологія.

Відповідно до Стандарту вищої освіти із зазначеної спеціальності та освітньої програми дисципліна сприяє розширенню і поглибленню:

компетентності:

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

програмні результати навчання:

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

Мета 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.

Предмет дисципліни. Застосуваннях теорії ймовірностей, теорії складності алгоритмів, теорії груп, кілець та полів, теорії чисел та алгоритми, які використовуються в криптографічних системах.

Завдання дисципліни. Формування базових математичних знань для розв'язання різних задач у професійній діяльності; формування умінь та навичок застування математичних теорії до розробки алгоритмів захисту даних та їх криптоаналізу.

Результати навчання. Студент, який успішно завершив вивчення дисципліни повинен: *адаптуватися* в умовах частої зміни технологій професійної діяльності, *організовувати* власну професійну діяльність; *аналізувати*, аргументувати, приймати рішення на основі вивчених математичних теорій для розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *обирати* оптимальні математичні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, *критично осмислювати* їхню ефективність; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних математичних теорій захисту інформації; *виконувати* впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах на основі математичних теорій та понять.

4) СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва розділу (теми)	Кількість годин, відведених на:		
	Лекції	**Практичні заняття**	**Самостійна робота**
Другий семестр			
Розділ 1. Подільність цілих чисел	8	8	16
Розділ 2. Конгруентності (порівняння)	18	18	37
Розділ 3. Ланцюгові дроби	10	10	25
Разом за 2-й семестр:	**36**	**36**	**78**
Третій семестр			
Розділ 4. Елементи теорії груп	6	6	8
Розділ 5. Елементи теорії кілець	12	12	34
Розділ 6. Системи числення	6	6	15
Розділ 7. Теорія еліптичних кривих	6	6	15
Розділ 8. Генератори псевдовипадкових чисел	4	4	10
Разом за 3-й семестр	**34**	**34**	**82**

5) ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотацій	Кіль-кість годин
	2-й семестр	
	РОЗДІЛ 1. ПОДІЛЬНІСТЬ ЦІЛИХ ЧИСЕЛ	**8**
1	**§ 1. 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. [7, С. 14-19], [15, С. 14-68], [17, С. 7-8].	2
2	**§ 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. [17, С. 8-12], [18, С. 87-91], [12, С. 24-29], [7, С. 30-35].	2
3	**§ 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. [17, С. 12-23], [18, С. 91-94], [7, С. 20-30].	2
4	**§ 4. Числові функції.** Мультиплікативні числові функції. Функції $\tau(n)$, $\sigma(n)$, $\{x\}$, $[x]$. Функція Ойлера $\varphi(n)$, функція Мебіуса $\mu(n)$, функція Кармайкла $\lambda(n)$. [17, С. 40-48], [12, С. 40-45].	2
		2
	РОЗДІЛ 2. КОНГРУЕНЦІЇ (ПОРІВНЯННЯ)	**18**
5	**§ 1. Конгруенції.** Означення конгруенції. Приклади. Властивості конгруенцій. [17, С. 54-58], [18, С. 111-115], [7, С. 43-47].	2
6	**§ 2. Повна та зведена система лишків.** Повна система лишків. Зведена система лишків. Теорема Ойлера і Ферма. Мультиплікативність функцій Ойлера. [17, С. 58-66], [18, С. 115-120], [7, С. 47-48].	2
7	**§ 3. Лінійні конгруенції з одним невідомим**. Конгруенції першого степеня. Способи розв'язування конгруенцій першого степеня: метод спроб, метод рівносильних перетворень. [17, С. 69-74], [18, С. 120-123], [7, С. 48-51]	2
8	Обернений елемент за множенням. Розвязування діафантових рівнянь. Китайська теорема про лишки. Системи конгруенцій з одним невідомим. Тести простоти. Тест псевдопростоти Ферма. [17, С. 77-84].	2
9	**§ 4. 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. [17, С. 91-103], [10, С. 19-26].	2

10	**§ 5. Конгруенції другого степеня.** Загальні положення. Квадратичні лишки. Конгруенція за простим непарним модулем. Символ Лежандра. Символ Якобі. [17, С. 108-141], [10, С. 26-30], [18, С. 134-143].	2
11	**§ 6. Первісні корені.** Означення порядків чисел і класів чисел за даним модулем. Властивості порядків за модулем. Первісні корені. Знаходження первісних коренів за елементарними модулями [17, С. 141-170], [10, С. 30-33], [18, С. 155-162].	2
12	**§ 7. Дискретні логарифми (індекси).** Поняття індекса (дискретного логарифма). Побудова таблиць індексів. Застосування індексів до розв'язання конгруенцій. . [17, С. 123-170], [10, С. 33-34], [18, С. 162-178]. [14, С. 52-58].	2
13	**§ 7. Арифметичні застосування теорії конгруенцій** Ознаки подільності. Перевірка результатів арифметичних дій. Перетворення звичайного дробу в десятковий. [10, С. 35-41].	2
	РОЗДІЛ 3. ЛАНЦЮГОВІ ДРОБИ	**10**
14	**§ 1. Скінчені ланцюгові дроби.** Скінченні ланцюгові дроби. Подання раціональних чисел ланцюговими. Підхідні дроби ланцюгового дробу. [18, С. 102-108], [7, С. 37-43].	2
15	**§ 2. Нескінчені ланцюгові дроби.** Подання дійсних ірраціональних чисел правильними нескінченними ланцюговими дробами. Підхідні дроби нескінченних ланцюгових дробів. Розкладання дійсного ірраціонального числа в правильний нескінченний ланцюгову дріб. Збіжність правильних нескінченних ланцюгових дробів. Єдиність подання дійсного ірраціонального числа правильної нескінченної ланцюгової дробом. [18, С. 108-110], [17, С. 23-28].	2
16	**§ 3. Квадратичні ірраціональності і періодичні ланцюгові дроби.** Поняття квадратичної ірраціональності. Періодичний ланцюговий дріб. Теорема Лежандра. [18, С. 110-111].	2
17	**§ 4. Раціональні «вкорочення» як найкращі наближення.** Порядок наближення дійсних чисел раціональними. Найкращі наближення та ланцюгові дроби. Теорема Ліувілля. Діафантові наближення та діафантові рівняння. [18, С. 111-112], [17, С. 29-30].	2
18	**§ 5. Застосування ланцюгових дробів.** Розв'язування конгруенцій першого степеня. Розв'язування діофантових рівнянь $aX+bY=c$. Рівняння Пелля. [18, С. 123-131], [17, С. 74-76], [3, С. 10-14].	2
	***Разом за 2-й семестр*:**	**36**
	3-й семестр	
	РОЗДІЛ 4. ЕЛЕМЕНТИ ТЕОРІЇ ГРУП	**6**
1	**§ 1 Алгебри. Бінарна алгебраїчні операція** Поняття бінарної операції. Напівгрупа. Нейтральний та обернений елемент. . [1, С. 6--7].	2
2	**§ 2. Група. Підгрупа.** Поняття групи. Приклади груп. Властивості груп. Підгрупи. Критерій підгрупи. Циклічні групи. Порядок елемента групи. Таблиці Келі. [18, С. 7-35], [14, С. 8-9], [8, С. 5-85]. [1, С. 15-16].	2
3	**§ 3. Група перестановок.** Симетрична групи (група перестановок). Добуток перестановок. Порядок перестановки. Знак перестановки. Парність перестановки. Інверсія. [9, С. 12-16].	2
	РОЗДІЛ 5. ЕЛЕМЕНТИ ТЕОРІЇ КІЛЕЦЬ	**12**

4	**§ 1. 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). [18, С. 51-61], [14, С. 12-14], [13, С. 126-134].	2
5	Теорема Безу та схема Горнера. Незвідні многочлена. Основна теорема алгебри Кратні корені. Похідна многочлена. Результант многочленів. Дискримінант многочлена.. Формули Вієта. [14, С. 12-14], [13, С. 134-141].	2
6	**§ 2. 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. [18, С. 35-38], [14, С. 9-11], [8, С. 85-103].	2
7	**§ 3. 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*. [18, С. 38-51], [8, С. 106-114].	2
8	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. [8, С. 126-132]. [2, С. 8-9, 21-23, 40-41].	2
9	**§ 4. Поле. Підполе.** Означення поля. Приклади. Характеристика поля. Підполе поля. Критерій підполя. Розширення поля. Алгебра над полем. Ізоморфізм полів. [18, С. 70-85]. [2, С. 8-9, 21-23, 40-41].	2
	РОЗДІЛ 6. СИСТЕМИ ЧИСЛЕННЯ	**6**
10	**§ 1. Позиційні системи числення.** Позиційні системи числення. [12, С. 48-49], [19, С. 11-13], [6, С. 7-9]. [20, С. 40-44].	2
11	Арифметичні дії в позиційних системах. Перехід до іншої позиційної системи. Ознаки подільності. Систематичні дроби. [12, С. 48-49], [19, С. 11-13], [6, С. 7-9]. [20, С. 44-46].	2
12	**§ 2. Нестандартні системи числення.** Нестандартні системи числення. [19, С. 13-24].	2
	РОЗДІЛ 7. ТЕОРІЯ ЕЛІПТИЧНИХ КРИВИХ	**6**
13	Елементарні відомості про еліптичні криві. Основні визначення. Способи побудови еліптичних кривих. [18, С. 179-182], [14, С. 107-109], [5, С. 109-110],	2
14	Умова несингулярності еліптичної кривої. Операція додавання і побудова групи точок еліптичної кривої. Відшукання точок еліптичної кривої над скінченним полем. [18, С. 182-188], [14, С. 109-112], [5, С. 111-114].	2
15	Число елементів групи точок еліптичної кривої. Порядок точки еліптичної кривої. Вибір еліптичної кривої і базової точки. [18, С. 188-199], [5, С. 114].	2
	РОЗДІЛ 8. ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ	**4**
16	**§ 1. Псевдовипадкова послідовність.** Основні визначення випадкової послідовності. Вимоги до псевдовипадкових послідовностей. Лінійна рекурентна послідовність з максимальним періодом.	2

	Псевдовипадкова послідовність на базі багатомодульних перетворень. Методи і засоби перевірки на випадковість. [21, С. 49-51], [22, С. 147-154].	
17	**§ 2. Генератор псевдовипадкових чисел.** Лінійній 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. [16, С. 3-9], [4, С. 25-26], [22, С. 147-154].	2
	***Разом за 3-й семестр*:**	**34**

5.2. Зміст практичних занять

Номер лекції	**Тема практичного заняття**	**Кіль-кість годин**
	2-й семестр	
	РОЗДІЛ 1. ПОДІЛЬНІСТЬ ЦІЛИХ ЧИСЕЛ	**8**
1	Подільність в множині цілих чисел. [17, С. 30-33].	2
2	Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне. [17, С. 30-33, 36-39].	2
3	Прості й складені числа. [17, С. 30-33, 36-39].	2
4	Числові функції. [17, С. 49-53].	2
	РОЗДІЛ 2. КОНГРУЕНЦІЇ (ПОРІВНЯННЯ)	**18**
5	Конгруенції. [17, С. 68], [9, С. 80-81].	2
6	Повна та зведена система лишків. [17, С. 68], [9, С. 84-86].	2
7	Лінійні конгруенції з одним невідомим. [17, С. 86-87], [8 С. 142-144]	2
8	Обернений елемент за множенням. Системи конгруенцій з одним невідомим. [17, С. 87-90], [8 С. 142-144].	2
9	Конгруенції вищих степенів. [17, С. 106-107].	2
10	Конгруенції другого степеня. Квадратичні лишки. Конгруенція за простим непарним модулем. [17, С. 122], [9, С. 100-103].	2
11	Символ Лежандра. Символ Якобі. [17, С. 122], [9, С. 104].	
12	Первісні корені. [17, С. 172-172].	2
13	Дискретні логарифми (індекси). [17, С. 172-173].	2
	РОЗДІЛ 3. ЛАНЦЮГОВІ ДРОБИ	**10**
14	Скінчені ланцюгові дроби. [17, С. 33-36].	2
15	Нескінчені ланцюгові дроби. [17, С. 33-36].	2
16	Квадратичні ірраціональності і періодичні ланцюгові дроби. [18, С. 110-111].	2

17	Раціональні «вкорочення» як найкращі наближення. [18, С. 111-112], [17, С. 29-30].	2
18	Застосування ланцюгових дробів. [18, С. 123-131], [17, С. 74-76], [3, С. 10-14].	2
	***Разом за 2-й семестр*:**	**36**
	3-й семестр	
	РОЗДІЛ 4. ЕЛЕМЕНТИ ТЕОРІЇ ГРУП	**6**
1	Алгебри. Бінарна алгебраїчна операція. Напівгрупа. Моноїд. [11, С.55-58].	2
2	Група. Підгрупа. Циклічна група. Порядок елемента групи. ТЬаблиці Келі. [8, С. 15-17, 26-28, 33-35, 48-50]. [9, С. 29]. [1, С. 17].	2
3.	Група перестановок. Порядок перестановки. Парність перестановки. Інверсія. [1, С. 19-20].	
	РОЗДІЛ 5. ЕЛЕМЕНТИ ТЕОРІЇ КІЛЕЦЬ	**12**
4	Многочлени, подільність многочленів. [1, С. 107-114].	2
5	Теорема Безу та схема Горнера. Основна теорема алгебри. Формули Вієта. [11, С. 184-186, 194-197, 203-205].	2
6	Кільце. Підкільце. [9, С. 33-37], [8, С. 103-105].	2
7	Фактор-кільця та ідеали. [9, С. 37-40], [8, С. 115-117].	2
8	Конгруенції і класи лишків за ідеалом. [9, С. 40-43].	2
9	Поле. Підполе. [18, С. 70-85].	2
	РОЗДІЛ 6. СИСТЕМИ ЧИСЛЕННЯ	**6**
10	Позиційні системи числення. [20, С. 40-44].	2
11	Арифметичні дії в позиційних системах. [20, С. 40-44].	2
12	Перехід до іншої позиційної системи. Ознаки подільності. Систематичні дроби. [20, С. 44-46].	2
	РОЗДІЛ 7. ТЕОРІЯ ЕЛІПТИЧНИХ КРИВИХ	**6**
13	Еліптичні криві. [18, С. 179-182], [14, С. 107-109], [5, С. 109-110],	2
14	Операція додавання і побудова групи точок еліптичної кривої. [18, С. 182-188], [14, С. 109-112], [5, С. 111-114].	2
15	Число елементів групи точок еліптичної кривої. Порядок точки еліптичної кривої. [18, С. 188-199], [5, С. 114].	2
	РОЗДІЛ 8. ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ	**4**
16	Псевдовипадкова послідовність. [21, С. 49-51], [22, С. 147-154].	2
17	Генератор псевдовипадкових чисел. [16, С. 3-9], [4, С. 25-26], [22, С. 147-154].	2
	***Разом за 3-й семестр*:**	**34**

У процесі виконання практичних робіт з дисципліни студенти денної форми здобуття освіти набувають практичних навичок із: проведення математичних розрахунків, створення математичних моделей процесів, що відбуваються в професійній діяльності, відшукання ефективних та оптимальних методів розв'язування задач.

5.3. Зміст самостійної роботи (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні теоретичного матеріалу, підготовці до виконання практичних занять, виконанні індивідуальних завдань та тестування тощо.

Номер тижня	Вид самостійної роботи	К-сть годин
	2-й семестр	
1	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
2	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
3	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
4	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
5	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **СР-1.** 4. Підготовка до захисту **ТС-1.**	4
6	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
7	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
8	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
9	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
10	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
11	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
12	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
13	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. підготовка до **КР-1**.	5
14	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **СР-2.** 4. Підготовка до захисту **ТС-2.**	5
15	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
16	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
17	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до захисту **ТС-3**. 4. Підготовка до **СР-3.**	5
18	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до заліку.4. підготовка до **КР -2**	5
	ВСЬОГО:	**78**
	3-й семестр	
1	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
2	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
3	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	4
4	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
5	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **СР-1.** 4. Підготовка до захисту **ТС-1.**	5
6	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
7	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
8	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **КР-1.**	5
9	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
10	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
11	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
12	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **СР-2.** 4. Підготовка до захисту **ТС-2.**	5
13	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
14	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **КР -2**	5
15	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5
16	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять.	5

	3. Підготовка до **СР-3.** 4. Підготовка до захисту **ТС-3.**	
17	1. Опрацювання теоретичного матеріалу. 2. Підготовка до практичних занять. 3. Підготовка до **ПКЗ**.	5
	ВСЬОГО:	**82**

Позначення: СР − поточна самостійна робота; КР – модульна контрольна робота, ТС – тестування.

6) ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами, а також методами проблемного навчання, використовуються наочні засоби навчання (таблиці, графіки, презентації). Практичні заняття проводяться методами ілюстративно-пояснювального навчання і мають за мету – набуття студентами практичних навичок з математичного моделювання технічних процесів.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills:

- виконання завдань під час проведення практичних занять передбачає роботу у групах та розвиток здатностей до командної роботи;
- використання методів роботи у малих групах з призначенням тім-лідера, сприяє розвитку лідерських якостей у студентів;
- робота біля дошки у студентів розвиває вміння висловлювати та обґрунтовувати свою думку;
- робота над спільним розв’язанням математичних задач сприяє розвитку навичок адаптованості, гнучкості, комунікативності і вміння налагоджувати міжособистісні відносин в колективі;
- інтерактивне спілкування з проблемних питань під час лекцій, прилюдні виступи під час практичних занять з обґрунтуванням прийнятих рішень щодо вибору методів рішення математичної задачі в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики;
- виконання самостійної роботи студентами передбачає розвиток вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел, враховуючи специфіку математичних дисциплін;
- виконання індивідуальних домашніх завдань, що передбачає рішення проблемних завдань із застосуванням отриманих математичних знань, сприяє розвитку здатності до синтезу і аналізу;
- обмежений час на виконання практичних і тестових завдань, терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

7) МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лекційних та практичних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- проведення поточних самостійний робіт (СР);
- тестовий контроль (ТС);
- проведення контрольної роботи (КР).

Поточні самостійні роботи (СР) виконуються на аудиторних заняттях і розраховані на 15-30 хвилин. Контроль за проведенням СР покладається на викладача практичних занять. Контрольна робота (КР) здійснюються письмово під контролем лектора, який перевіряє та оцінює письмові роботи. Підсумковий контрольний захід (ПКЗ) здійснюється письмово та проводиться лектором у спеціально відведений для цього час.

Семестровий контроль проводиться у формі заліку та іспиту. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу, який проводиться у вигляді контрольної роботи за матеріалом семестру. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

8) ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ У СЕМЕСТРІ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за ***чотирибальною*** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих ***позитивно*** з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

На основі результатів поточного контролю і підсумкового контрольного заходу виставляється підсумкова семестрова оцінка. На основі аналізу контролю знань викладач удосконалює курс лекцій, звертаючи особливу увагу на ті розділи, чи теми, з яких було найбільше неточних відповідей, що свідчить про методичні чи інші недоліки при висвітленні вказаних тем або розділів.

Кожний вид роботи оцінюється в балах від 0 до 5. Підсумкова кількість балів з дисципліни визначається як середньозважена з усіх видів робіт. За набраною студентом кількістю балів визначається відповідна оцінка.

Оцінювання знань студентів здійснюється за такими критеріями:

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	*2*
Відмінно	Студент виявляє повне розуміння теоретичного матеріалу, знання теорем та математичних формул; прослідковується розуміння причинно-наслідкових зав'язків, вміння користуватися математичною термінологією; студент правильно розв'язує всі математичні задачі, повністю продемонстровано процес розв'язування завдань, що супроводжується логічно викладеними поясненнями та обґрунтуваннями; допустимі одна-дві несуттєві похибки, що не впливають на правильність отриманих рішень.
Добре	Студент правильно розв'язує математичні задачі, розв'язок задач супроводжується поясненнями, але логіка пояснень в роботі та їх обґрунтування є недостатніми або розв'язки задач отримано нераціональним методом. Студентом не в повній мірі розкрито теоретичний матеріал. У роботі також допустимі дві-три несуттєві похибки, що не впливають на правильність отриманих розв'язків.
Задовільно	Студент загалом правильно розв'язує математичні задачі, але розв'язки задач представлені без необхідних пояснень і обґрунтувань або студент не повністю розв'язав запропоновані завдання. Допускає дві-три помилки в обчисленнях.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Студент не може розв'язати (частково або повністю) деякі завдання або в ході отримання розв'язку припускається суттєвих помилок, що зумовлює одержання хибних результатів.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі за ваговими коефіцієнтами

Аудиторна робота		*Самостійна, індивідуальна робота*	*Семестровий контроль, іспит*
Другий семестр			
Поточні самостійні роботи (СР)	Контрольна робота (КР)	Тестування (ТС)	Підсумковий контроль (ПКЗ)

1	2	3	1	2	1	2	3	1
ВК*: 0,5			**0,3**		**0,2**			
Третій семестр								
Поточні самостійні роботи (СР)			Контрольна робота (КР)		Тестування (ТС)			Підсумковий контроль (ПКЗ)
1	2	3	1	2	1	2	3	1
ВК*: 0,3			**0,2**		**0,1**			**0,4**

Якщо студент отримав негативну оцінку, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Оцінювання індивідуального домашнього завдання. Індивідуальне домашнє завдання передбачає виконання студентом індивідуального варіанту завдань, запропонованого викладачем, з певного розділу дисципліни. Оцінювання здійснюється за чотирибальною шкалою:

– оцінка відмінно ставиться, якщо студент правильно розв'язав всі завдання, повністю продемонстровано процес розв'язування завдань, що супроводжується логічно викладеними поясненнями та обґрунтуваннями. У роботі допустимі одна-дві несуттєві похибки, що не впливають на правильність отриманих рішень;

– оцінка добре ставиться, якщо студент правильно розв'язав всі завдання, проте логіка пояснень в роботі та їх обґрунтування є недостатніми або повними, або розв'язки задач отримано нераціональним методом. У роботі також допустимі дві-три несуттєві похибки, що не впливають на правильність отриманих розв'язків;

– оцінка задовільно ставиться, якщо студент загалом правильно розв'язав всі завдання індивідуального домашнього завдання, але представив розв'язки задач без необхідних пояснень і обґрунтувань або допустив дві-три помилки в обчисленнях, або неповністю розв'язав запропоновані завдання;

– оцінка незадовільно ставиться, якщо студент не розв'язав (частково або повністю) хоча б одну задачу контрольної роботи або в ході отримання розв'язку припустився суттєвої помилки, що зумовило одержання хибних результатів. Індивідуальне домашнє завдання виконується студентами в позаурочний час. Термін виконання та здачі індивідуального домашнього завдання оголошується заздалегідь викладем.

Оцінювання контрольної роботи. Контрольна робота передбачає для кожного студента виконання певного варіанту завдання, що складається з теоретичних питань за практичних завдань. Оцінювання контрольної роботи здійснюється за чотирибальною шкалою:

– оцінка відмінно ставиться, якщо студент правильно розв'язав всі задачі контрольної роботи, розв'язок задач супроводжується логічно викладеними поясненнями та обґрунтуваннями. Теоретичний матеріал повністю розкрито. Прослідковується розуміння причинно-наслідкових зав'язків, вміння користуватися математичною термінологією. У роботі допустимі одна-дві несуттєві похибки, що не впливають на якість отриманих рішень;

– оцінка добре ставиться, якщо студент правильно розв'язав всі задачі контрольної роботи, розв'язок задач супроводжується поясненнями, але логіка пояснень в роботі та їх обґрунтування є недостатніми або розв'язки задач отримано нераціональним методом. У роботі також допустимі дві-три несуттєві похибки, що не впливають на правильність отриманих розв'язків або не в повній мірі розкрито теоретичний матеріал;

– оцінка задовільно ставиться, якщо студент загалом правильно розв'язав всі задачі контрольної роботи, але представив розв'язки задач без необхідних пояснень і обґрунтувань або допустив дві-три помилки в обчисленнях;

– оцінка незадовільно ставиться, якщо студент не розв'язав (частково або повністю) хоча б одну задачу контрольної роботи або в ході отримання розв'язку припустився суттєвої помилки, що зумовило одержання хибних результатів.

Контрольна робота виконується студентами під час аудиторних занять. Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни.

Оцінювання самостійної роботи. Самостійна робота передбачає для кожного студента виконання індивідуального варіанту, що складається з практичних завдань. Самостійна робота

проводиться під час практичних занять. Оцінювання здійснюється за тими з критеріями, що і виконання індивідуального домашнього завдання. Оцінку за самостійну роботу викладач оголошує на наступному практичному занятті та виставляє її в електронний журнал. Студенти мають можливість переглянути написану з роботою та ознайомитись із зауваження щодо допущених помилок.

Оцінювання тестових завдань. Тематичне тестування за матеріалом семестру проводиться під час аудиторних занять в модульному середовищі для навчання Moodle. Тестові завдання мають рівноцінну вагу. Максимальна оцінка, яку може отримати студент – 5. Оцінку за тест студенти отримують автоматично після закінчення тестування.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з теоретичного питання і практичних задач. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС.

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання	
A	4,75–5,00	5	*Відмінно* – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	*Добре* – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	*Добре* – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	*Задовільно* – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	*Задовільно* – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	*Незадовільно* – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	*Незадовільно* – необхідна серйозна подальша робота і повторне вивчення дисципліни

9) ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ РЕЗУЛЬТАТІВ НАВЧАННЯ

1.. Поняття математичної індукції.
2. Подільність у множині цілих чисел. Теорема про ділення з остачею.
3. Поняття НСД.
4. Алгоритм Евкліда. Властивості НСД.
5. Найбільший спільний дільник кількох чисел.
6. Найменше спільне кратне (НСК) цілих чисел.
7. Прості числа та їхні властивості. Нескінченність множини простих чисел.
8. Розклад складених чисел на прості множники.
9. Основна теорема арифметики.
10. Решето Ератосфена.
11. Мультиплікативні числові функції. Функції $\tau(n)$, $\sigma(n)$, $\{x\}$, $[x]$.
12. Функція Ойлера $\varphi(n)$, функція Мебіуса $\mu(n)$, функція Кармайкла $\lambda(n)$.
13. Означення конгруенції. Приклади. Властивості конгруенцій. Класи лишків за модулем.
14. Повна система лишків. Зведена система лишків. Теорема Ойлера і Ферма. Мультиплікативність функцій Ойлера
15. Конгруенції першого степеня. Мала теорема Ферма. Теорема Ойлера (Ейлера).
16. Китайська теорема про лишки.
17. Обернений елемент за множенням.

18. Системи конгруенцій з одним невідомим.
19. Конгруенції *n*-го степеня за простим модулем. Число розв'язків конгруенцій *n*-го степеня за простим модулем. Конгруенції *n*-го степеня за складеним модулем.
20. Квадратичні лишки. Конгруенція за простим непарним модулем.
21. Символ Лежандра. Символ Якобі.
22. Означення порядків чисел і класів чисел за даним модулем. Властивості порядків за модулем. Первісні корені. Знаходження первісних коренів за елементарними модулями
23. Індекси (дискретні логарифми). Індекси за елементарними модулями, за модулем 2, за складеним модулем. Побудова таблиць індексів. Застосування індексів до розв'язання задач теорії чисел.
24. Скінченні ланцюгові дроби. Подання раціональних чисел ланцюговими. Підхідні дроби ланцюгового дробу.
25. Нескінченні ланцюгові дроби. Підхідні дроби нескінченних ланцюгових дробів. Розкладання дійсного ірраціонального числа в правильний нескінченний ланцюгову дріб.
26. Поняття квадратичної ірраціональності. Періодичний ланцюговий дріб. Теорема Лежандра.
27. Раціональні «вкорочення» як найкращі наближення.
28. Застосування ланцюгових дробів.
29. Алгебри. Алгебраїчна операція (внутрішній закон композиції). Основні властивості алгебраїчних операцій. Обернені операції. Приклади алгебр. Основні властивості алгебраїчних операцій. Закон композиції.
30. Група. Підгрупа.
31. Многочлени, подільність многочленів.
Поняття многочлена. Зв'язок поняття алгебраїчного многочлена над полем дійсних чисел та многочлена як функції. Теорема про ділення многочленів з остачею. Алгоритм ділення многочлена з остачею. Знаходження найбільшого спільного дільника двох многочлена (алгоритм Евкліда).
32. Теорема Безу та схема Горнера. Незвідні многочлена. Похідна многочлена та кратні корені. Результант многочленів. Дискримінант многочлена. Основна теорема алгебри. Формули Вієта.
33. 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.
34. 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*.
35. 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.
37. Означення поля. Приклади. Характеристика поля. Підполе поля. Критерій підполя. Розширення поля. Алгебра над полем.
38. Гомоморфізми та ізоморфізми алгебраїчних структур. Поняття відображення. Типи відображень. Гомоморфізм та ізоморфізм груп. Гомоморфізм кілець. Ізоморфізм кілець та полів.
39. Арифметичні дії в позиційних системах. Перехід до іншої позиційної системи. Ознаки подільності. Систематичні дроби.\
39. Нестандартні системи числення.
40. Елементарні відомості про еліптичні криві. Основні визначення. Способи побудови еліптичних кривих. Операція додавання і побудова групи точок еліптичної кривої. Відшукання точок еліптичної кривої над скінченним полем.
41. Число елементів групи точок еліптичної кривої. Порядок точки еліптичної кривої. Вибір еліптичної кривої і базової точки.
42. Псевдовипадкова послідовність. Основні визначення випадкової послідовності. Вимоги до псевдовипадкових послідовностей. Методи і засоби перевірки на випадковість.
43. Генератор псевдовипадкових чисел. Лінійній конгруентний генератор псевдовипадкових чисел. Метод Фібоначчі із запізненням. Генератори псевдовипадкових чисел на основі регістрів зсуву з оберненим зв'язком.

10) НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Математичні основи захисту інформації» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі.

11) РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Авдєєва Т. В. Лінійна алгебра в задачах та прикладах [Електронний ресурс] : збірник задач для студентів 1 курсу ФМФ / Т. В. Авдєєва, В. М. Шраменко ; НТУУ «КПІ». – Електронні текстові дані (1 файл: 714 Кбайт). – Київ : НТУУ «КПІ», 2016. – 205 с.

2. 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.

3. Бамбенкова, Ю. Застосування ланцюгових дробів [Текст] / Ю. Бамбенкова // Фізико-математична освіта : збірник наукових праць / Міністерство освіти і науки, Сумський державний педагогічний університет імені А. С. Макаренка, Фізико-математичний факультет ; редкол.: Ф. М. Лиман, В. С. Іваній, М. В. Каленик та ін. – Суми : Вид-во СумДПУ імені А. С. Макаренка, 2015. – Вип. 1 (7). – С. 9–14.

4. 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. — (Інформаційні системи та технології, кібербезпека).

5. 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.

6. Білак Ю.Ю. Системи числення: методичні рекомендації з базової теми дисципліни «Інформатика» / Ю.Ю. Білак, Л.Я. Данько-Товтин. – Ужгород: ДВНЗ «УжНУ», 2015. – 24 с.

7. 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

8. Гаврилків В.М. Елементи теорії груп та теорії кілець: навчальний посі бник / В.М. Гаврилків. — Івано-Франківськ: Голіней, 2018. — 148 с.

9. Заїка О. В., Сухойваненко Л.Ф. , Прокопець Т.О. Алгебра і теорія чисел : навчальний посібник / О. В. Заїка, Л.Ф. Сухойваненко, Т.О. Прокопець. – Глухів: ФОП Цьома С.П., 2023. – 264 с.

10. 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.

11. Завдання до практичних занять з лінійної алгебри: навч. посіб./ О. О. Безущак, О. Г. Ганюшкін, Є. А. Кочубінська – К. : Видавничо-поліграфічний центр “Київський університет”, 2016. – 255 с.

12. Кулаковська І. В. Дискретна математика. Частина 1. Множини, відношення та математичні основи крипто графії. Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпе чення», 122 «Комп’ютерні науки», 124 «Системний аналіз» : методичні вказівки / І. В. Кулаковська. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2021. – 100 с.

13. Лінійна алгебра та аналітична геометрія : курс лекцій для студентів ІТ спеціальностей / А. О. Рамський, Н. О. Ярецька, О. А. Поплавська. – Хмельницький : ХНУ, 2022. – 253 с.

14. 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.

15. Медведєва М.О. Числові системи: навчальний посібник для студентів фізико-математичних факультетів педагогічних університетів / укл. М.О. Медведєва, В.В. Ефендієв – Умань : УКВПП. – 2017. – 153 с.

16. 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.

17. Оглобліна О. І. Елементи теорії чисел : навч. посіб. / О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. – Суми : Сумський державний університет, 2015. – 186 с.

18. Стасюк М. Елементи математичних основ криптографії : навчальний посібник / Марта СТАСЮК
19. Тарарака В.Д. Прикладна теорія цифрових автоматів: навчальний посібник. – Житомир: ЖДТУ, 2019. – 183с.
20. Лялецький О. Окремі розділи дисретної математики (Матеріали лекцій здисциплдіни «Дискретна математика») / Лялецький Олександр Вадимович. – К.: Атералекс-принт, 2018.
21. Петрушак, В.С. Аналіз методів та засобів формування псевдовипадкової послідовності чисел [Текст] / В. С. Петрушак, І. В. Столярчук // Вісник Хмельницького національного університету. Технічні науки. – 2016. – №1. – С. 49-51.
22. 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.

Додаткова

23. 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.
24. Гиря Н. П.Елементи теорії чисел : навчально-методичний посібник з елементів алгебри та теорії чисел / укладачі Н. П. Гиря, О. О. Заварзіна, Є. О. Каролінський, Л. Ю. Полякова. – Харків : ХНУ імені В. Н. Каразіна, 2024. – 48 с.
25. 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. – Електрон. текст. дані. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2023/paper/view/17290.

12) ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище. URL: https://msn.khmnu.edu.ua/course/view.php?id=9020
2. Електронна бібліотека. URL: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.
3. Репозитарій ХНУ. URL : https://library.khmnu.edu.ua/#.