

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ



ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

Тетяна ГОВОРУЩЕНКО

Ім'я, ПРІЗВИЩЕ

01.09

2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні основи захисту інформації

Назва дисципліни

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 – ОПІ.03

Мова навчання – українська

Статус дисципліни: обов'язкова (загальної підготовки)

Факультет – Інформаційних технологій

Кафедра – Вищої математики та комп'ютерних застосувань

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт*	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття					
Д	1	2	5	150	66	32		34		84			+	
Д	2	3	5	150	66	32		34		84				+
Разом ДФН			10	300	132	64		68		168			1	1

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

Робоча програма складена


Підпис автора(ів)

канд. пед. наук, доцент
Науковий ступінь, чиєше звання,

Наталія САМАРУК
Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри

Вищої математики та комп'ютерних застосувань

Протокол від 19.08. 2025 № 1

Зав. кафедри


Підпис

Андрій РАМСЬКИЙ
Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету


Підпис

Тетяна ГОВОРУЩЕНКО
Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	<u>Кібербезпеки</u>		<u>Юрій КЛЮЧ</u>
Гарант освітньо-професійної програми, канд. техн. наук, доц.	<u>Кібербезпеки</u>		<u>Віктор ЧЕШУН</u>

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. Математичні методи, моделі та алгоритми, що лежать в основі сучасних засобів криптографії, стеганографії та захисту інформаційних систем від несанкціонованого доступу.

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

Результати навчання. Студент, який успішно завершив вивчення дисципліни повинен: *знати* основні математичні поняття та методи, що використовуються в теорії захисту інформації; *розуміти* принципи побудови криптографічних систем, хеш-функцій, електронного підпису; *володіти* методами аналізу стійкості алгоритмів захисту; *застосовувати* математичні методи для розв'язання задач захисту інформації; *будувати* та аналізувати алгоритми шифрування і автентифікації; *використовувати* математичні моделі для оцінки ефективності та безпеки систем; *обґрунтовувати* вибір методів захисту для конкретних задач; *проводити* математичний аналіз вразливостей алгоритмів і систем; *інтегрувати* математичні основи захисту у практичні інформаційні технології.

4) СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва розділу (теми)	Кількість годин, відведених на:		
	Лекції	Практичні заняття	Самостійна робота
<u>Другий семестр</u>			
Розділ 1. Подільність цілих чисел	8	8	28
Розділ 2. Конгруентності (порівняння)	16	16	28
Розділ 3. Ланцюгові дроби	8	10	28
Разом за 2-й семестр:	32	34	84
<u>Третій семестр</u>			
Розділ 4. Елементи теорії груп	6	6	17
Розділ 5. Елементи теорії кілець	12	12	17
Розділ 6. Системи числення	6	6	17
Розділ 7. Теорія еліптичних кривих	4	6	17
Розділ 8. Генератори псевдовипадкових чисел	4	4	16
Разом за 3-й семестр	32	34	84

5) ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотацій	Кількість годин
	2-й семестр	
	РОЗДІЛ 1. ПОДІЛЬНІСТЬ ЦІЛИХ ЧИСЕЛ	8
1	§ 1. Множини натуральних, цілих та раціональних чисел. Поняття множини. Аксиоми Пеано. Аксиоматичне 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
	РОЗДІЛ 2. КОНГРУЕНЦІЇ (ПОРІВНЯННЯ)	16
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. Розв'язування 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	2

	модулем. Символ Лежандра. Символ Якобі. [17, С. 108-141], [10, С. 26-30], [18, С. 134-143].	
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
	РОЗДІЛ 3. ЛАНЦЮГОВІ ДРОБИ	8
13	§ 1. Скінчені ланцюгові дроби. Скінченні ланцюгові дроби. Подання раціональних чисел ланцюговими. Підхідні дроби ланцюгового дроби. [18, С. 102-108], [7, С. 37-43].	2
14	§ 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 правильною нескінченною ланцюговою дробом. [18, С. 108-110], [17, С. 23-28].	2
15	§ 3. Квадратичні ірраціональності і періодичні ланцюгові дроби. Поняття квадратичної ірраціональності. Періодичний ланцюговий дріб. Теорема Лежандра. [18, С. 110-111]. § 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
16	§ 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:	32
	3-й семестр	
	РОЗДІЛ 4. ЕЛЕМЕНТИ ТЕОРІЇ ГРУП	6
1	§ 1 Алгебри. Бінарна алгебраїчна 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	2

	Кратні корені. Похідна многочлена. Результат многочленів. Дискримінант многочлена.. Формули Вієта. [14, С. 12-14], [13, С. 134-141].	
6	§ 2. Кільце. Підкільце. Означення кільця. Підкільце. Приклади числових кілець. Типи кілець. Властивості кілець. Асоціативні кільця. Комутативні кільця. Кільця з одиницею. Дільники нуля. Обороти 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 дробі. [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	4
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. Відшукування точок еліптичної кривої над скінченним полем. Число елементів групи точок еліптичної кривої. [18, С. 182-199], [14, С. 109-112], [5, С. 111-114].	2
	РОЗДІЛ 8. ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ	4
15	§ 1. Псевдовипадкова послідовність. Основні визначення випадкової послідовності. Вимоги до псевдовипадкових послідовностей. Лінійна рекурентна послідовність з максимальним періодом. Псевдовипадкова послідовність на базі багатомодульних перетворень. Методи і засоби перевірки на випадковість. [21, С. 49-51], [22, С. 147-154].	2
16	§ 2. 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. [16, С. 3-9], [4, С. 25-26], [22, С. 147-154].	2
	Разом за 3-й семестр:	32

5.2. Зміст практичних занять

Номер лекції	Тема практичного заняття	Кількість 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]. ТК №1 (Подільність цілих чисел).	2
	РОЗДІЛ 2. КОНГРУЕНЦІЇ (ПОРІВНЯННЯ)	16
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 другого степеня. Квадратичні лишки. Конгруенція за простим непарним модулем. [17, С. 122], [9, С. 100-103].	2
10	Символ Лежандра. Символ Якобі. [17, С. 122], [9, С. 104].	2
11	Первісні корені. [17, С. 172-172].	2
12	Дискретні логарифми (індекси). [17, С. 172-173]. КР №1 (Конгруенції).	2
	РОЗДІЛ 3. ЛАНЦЮГОВІ ДРОБИ	10
13	Скінчені ланцюгові дроби. [17, С. 33-36]. ІДЗ №1 (Подільність чисел. Конгруенції).	2
14	Нескінчені ланцюгові дроби. [17, С. 33-36].	2
15	Квадратичні ірраціональності і періодичні ланцюгові дроби. [18, С. 110-111].	2
16	Раціональні «вкорочення» як найкращі наближення. [18, С. 111-112], [17, С. 29-30]. ТК №2 (Ланцюгові дроби).	2
17	Застосування ланцюгових дробів. [18, С. 123-131], [17, С. 74-76], [3, С. 10-14].	2
	Разом за 2-й семестр:	34
	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. Тъаблиці Келі.	2

	[8, С. 15-17, 26-28, 33-35, 48-50]. [9, С. 29]. [1, С. 17].	
3.	Група перестановок. Порядок перестановки. Парність перестановки. Інверсія. [1, С. 19-20].	2
	РОЗДІЛ 5. ЕЛЕМЕНТИ ТЕОРІЇ КІЛЕЦЬ	12
4	Многочлени, подільність многочленів. [1, С. 107-114]. ТК №1 (Група).	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]. ІДЗ №1 (Многочлени).	2
7	Фактор-кільця та ідеали. [9, С. 37-40], [8, С. 115-117].	2
8	Конгруєнції 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]. КР №1 (Групи, кільця, поля).	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]. ТК №2 (Системи числення, еліптичні криві, генератори випадкових чисел).	2
17	Генератор псевдовипадкових чисел. [16, С. 3-9], [4, С. 25-26], [22, С. 147-154].	2
	Разом за 3-й семестр:	34

Позначення: КР – контрольна робота, ТК – тестовий контроль, ІДЗ – індивідуальне домашнє завдання.

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до практичних занять, контрольних робіт, тестування, виконанні індивідуальних завдань тощо. Крім цього до послуг студентів сторінка кафедри у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни, варіанти контрольних робіт та необхідні матеріали з її навчально-методичного забезпечення та контролю результатів навчання.

Зміст самостійної роботи студентів денної форми здобуття освіти

Номер тижня	Вид самостійної роботи	К-сть годин
-------------	------------------------	-------------

На самостійне опрацювання студентів виносяться визначене у методичних рекомендаціях до практичних занять та самостійної роботи індивідуальне домашнє завдання (ІДЗ) з відповідних тем. Керівництво самостійною роботою та контроль за виконанням індивідуального завдання здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

Вимоги до виконання індивідуального домашнього завдання викладені в Модульному середовищі для навчання на сторінці навчальної дисципліни.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням мультимедійних презентацій, методів візуалізації, пояснення, проблемного й інтерактивного навчання, методів стимулювання і мотивації, інтенсифікації та індивідуалізації навчання, тощо); практичні заняття (з використанням презентацій, інструктування, демонстрування, розв'язування типових і прикладних задач, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань тощо), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів роботи на практичних заняттях (опитування теоретичного матеріалу, розв'язування задач, участь у обговоренні ситуацій);
- тестовий контроль засвоєння теоретичного та практичного матеріалу;
- оцінювання результатів виконання індивідуального домашнього завдання;
- оцінювання контрольної роботи.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, **не допускається** до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який **має** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до практичних занять (вивчення теоретичного матеріалу з теми), активно працювати на занятті, розв'язувати задачі.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Пропущене практичне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять, тестування й виконання індивідуального домашнього завдання та контрольної роботи. Виконання індивідуального завдання завершується його здачею на перевірку у терміни, встановлені графіком самостійної роботи.

Здобувач вищої освіти, виконуючи контрольну роботу, тестування, індивідуальне домашнє завдання з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в

т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності **не допускаються**.

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах, які сприяють формуванню компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	Узагальнений зміст критерія оцінювання
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві помилки .
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три несуттєві помилки .
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Незадовільно (недостатній)	Здобувач вищої освіти 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. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.
-------------------------------	---

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі

Аудиторна робота				Контрольні заходи			Самос- тійна робота	Семестро- вий контроль	Разом
Другий семестр									Сума балів
Практичні заняття				ТК		КР	ІДЗ	Іспит	
1-4	5-8	9-12	13-17	1	2	1	1		
Кількість балів за вид навчальної роботи (мінімум-максимум)									
3-5	3-5	3-5	3-5	6-10	6-10	6-10	6-10	24-40	60-100**
12-20				12-20		6-10	6-10	24-40	

Аудиторна робота				Контрольні заходи		Самостійна робота	Семестровий контроль	Разом	
Третій семестр								Сума балів	
Практичні заняття				ТК		КР	ІДЗ		Іспит
1-3	4-9	10-12	13-17	1	2	1	1		
Кількість балів за вид навчальної роботи (мінімум-максимум)									
3-5	3-5	3-5	3-5	6-10	6-10	6-10	6-10	24-40	60-100**
12-20				12-20		6-10	6-10	24-40	

Примітки: ТК – тестовий контроль, КР – контрольна робота, ІДЗ – індивідуальне домашнє завдання.

На самостійне опрацювання студентів виносяться визначені у методичних рекомендаціях до практичних занять та самостійної роботи індивідуальне домашнє завдання (ІДЗ) з відповідних тем. Керівництво самостійною роботою та контроль за виконанням індивідуального завдання здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

Вимоги до виконання індивідуального домашнього завдання викладені в Модульному середовищі для навчання на сторінці навчальної дисципліни.

Оцінювання на практичних заняттях.

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; вільне володіння студентом математичною термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач; результати самостійних робіт. При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

Оцінювання результатів тестового контролю.

Кожний з тестів, передбачених Робочою програмою, складається із 10 тестових завдань, які є рівнозначними та передбачають розв'язування задач.

Відповідно до таблиці структурування видів робіт за тестовий контроль здобувач залежно від кількості правильних відповідей може отримати від 6 до 10 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-5	6	7	8	9	10
Відсоток правильних відповідей	0-59	60	70	80	90	100
Кількість отриманих балів	0	6	7	8	9	10

На тестування відводиться 30-40 хвилин. Тематичне тестування за матеріалом дисципліни проводиться в модульному середовищі для навчання Moodle або письмово, де студент записує правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну *наступного* контролю.

Оцінювання контрольної роботи.

Контрольна робота передбачає виконання п'яти практичних завдань (практичне завдання передбачає розв'язування задач з даних тем). При оцінюванні контрольної роботи враховуються: повнота відповіді та якість виконання. Кожне завдання контрольної роботи оцінюється 2 балами, загальна сума балів на позитивну оцінку становить від 6 до 10 балів. Контрольна робота виконується студентами під час аудиторних занять. Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни. При отриманні негативної оцінки за контрольну роботу слід перездати до терміну *наступного* контролю.

Розподіл балів при оцінюванні завдань контрольної роботи у першому-третьому семестрах

Кількість правильно розв'язаних задач	1	2	3	4	5
Відсоток правильних відповідей	0-59		60	80	100
Кількість отриманих балів	0		6	8	10

Оцінювання результатів виконання індивідуального домашнього завдання.

Індивідуальне домашнє завдання передбачає виконання студентом індивідуального варіанту завдань, запропонованого викладачем, з певного розділу дисципліни. Виконане та оформлене відповідно до вимог, визначених Методичними рекомендаціями, індивідуальне домашнє завдання (ІДЗ) комплексно оцінюється викладачем з урахуванням таких критеріїв: самостійність виконання; правильність розв'язання поставлених задач; обґрунтованість вибору методів розв'язання; повнота пояснень та аргументованість відповідей; якість оформлення та дотримання вимог до структури і змісту роботи.

Результат виконання здобувачем вищої освіти кожного ІДЗ оцінюється відповідно до таблиці **Критеріїв оцінювання навчальних досягнень здобувача вищої освіти** з урахуванням рівня досягнення запланованих програмних результатів навчання та сформованих компетентностей. За підсумками захисту присвоюється відповідна сума балів (мінімальний позитивний бал – 6 бали, максимальний – 10 балів).

У разі, якщо здобувач вищої освіти виявив рівень знань і виконання ІДЗ, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку доопрацьоване ІДЗ у терміни, погоджені з викладачем.

Оцінювання результатів підсумкового семестрового контролю (іспит).

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	Для кожного окремого виду завдань		
	Мінімальний (достатній) бал (задовільно)	Потенційні позитивні бали* (середній бал) (добре)	Максимальний (високий) бал (відмінно)
Теоретичне питання (оцінюються від 3 до 5 балів)	3	4	5
Практичне завдання (7 задач, кожна з яких оцінюється від 3 до 5 балів)	21	28	35
Разом:	24		40

Примітка. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти**).

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	Іспит/диференційований залік
A	90-100	Зараховано	Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
D	66-72		
E	60-65		
FX	40-59	Незараховано	Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		Незадовільно/Fail – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

Другий семестр

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. Індеси (дискретні логарифми). Індеси за елементарними модулями, за модулем 2, за складеним модулем. Побудова таблиць індесів. Застосування індесів 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.

Третій семестр

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. Результат 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. Обороти 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. Відшукування 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. Лінійний конгруентний генератор псевдовипадкових чисел. Метод Фібоначчі із запізненням. Генератори псевдовипадкових чисел на основі регістрів зсуву з оберненим зв'язком.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Вища математика» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі: <https://msn.khmnmu.edu.ua/course/view.php?id=9020>.

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

Вивчення навчальної дисципліни не потребує використання спеціального програмного прикладного забезпечення, крім загальноновживаних програм і операційних систем.

13. Рекомендована література:

Основна

1. Баняс Б. Методи формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем / Б. Баняс // Матеріали ІХ науково-технічної конференції «Інформаційні моделі, системи та технології», 08-09 грудня 2021 року. — Т. : ТНТУ, 2021. — С. 25–27. — (Інформаційні системи та технології, кібербезпека).
2. 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>
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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. Сечкін – Дніпро: НТУ «ДП», 2020. – 9 с.
9. 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.
10. 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.
11. 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. Дмитрієнко В. Д. Вступ у математичні методи у наукових дослідженнях / В.Д. Дмитрієнко, С.Ю. Леонов: навчальний посібник. – Харків: НТУ – ХПІ, 2022 – 112 с.
13. Гаврилків В.М. Елементи теорії груп та теорії кілець: навч. посібник. – Івано-Франківськ: Голіней, 2023. – 153 с.

Додаткова

14. Москаленко Ю. Д., Коваленко О. В., Черкаська Л. П. Алгебра і теорія чисел : метод. рек. до проведення практ. занять та організації самостійної роботи студентів предметної спеціальності 014.04 Середня освіта (Математика). – Полтава : ПНПУ імені В. Г. Короленка, 2021. – 96 с.

15. Лукашова Т. Д., Друшляк М. Г. Алгебра і теорія чисел: навчальний посібник для студентів спеціальності 014 «Середня освіта. Математика». Ч.I. – Суми: СумДПУ ім. А.С. Макаренка, 2022. – 123 с.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL: <https://msn.khmnu.edu.ua/course/view.php?id=9020>
2. Електронна бібліотека ХНУ. URL: <http://library.khmnu.edu.ua/>
3. Інституційний репозитарій ХНУ. URL : <https://elar.khmnu.edu.ua/home>

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: *знати* основні математичні поняття та методи, що використовуються в теорії захисту інформації; *розуміти* принципи побудови криптографічних систем, хеш-функцій, електронного підпису; *володіти* методами аналізу стійкості алгоритмів захисту; *застосовувати* математичні методи для розв'язання задач захисту інформації; *будувати* та аналізувати алгоритми шифрування і автентифікації; *використовувати* математичні моделі для оцінки ефективності та безпеки систем; *обґрунтовувати* вибір методів захисту для конкретних задач; *проводити* математичний аналіз вразливостей алгоритмів і систем; *інтегрувати* математичні основи захисту у практичні інформаційні технології.

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 – 64 год., практичних занять – 68 год., самостійної роботи – 168 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, колоквиуми, комп'ютерне тестування.

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

Навчальні ресурси:

1. 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.
2. 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.
3. Модульне середовище. URL: <https://msn.khmn.edu.ua/course/view.php?id=9020>
4. Електронна бібліотека. URL: http://lib.khnu.km.ua/asp/php_f/plage_lib.php

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