ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет інформаційних технологій
Кафедра вищої математики та комп'ютерних застосувань

ЗАТВЕРДЖУЮ
Декан факультету
інформаційних технологій
Тетяна ГОВОРУЩЕНКО
«05» 09
2024 р.

СИЛАБУС

Навчальна дисципліна **Математичні основи захисту інформації**
Освітньо-професійна програма Кібербезпека та захист інформації
Рівень вищої освіти Перший (бакалаврський)

Таблиця 1 – Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Самарук Наталія Миколаївна
Профайл викладача(ів)	https://math.khmnu.edu.ua/samaruk-nataliya-mykolayivna/
E-mail викладача(ів)	samaruk_nm@ukr.net
Контактний телефон	
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=9020
Консультації	**Очні:** понеділок, 3-306, 10.00-11.00 **онлайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

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

Анотація дисципліни

Дисципліна «Математичні основи захисту інформації» є однією із дисциплін професійної підготовки і викладається для студентів денної форми здобуття освіти першого (бакалаврського) рівня спеціальності 125 – Кібербезпека та захист інформації.. Вона має забезпечити: здатність до розвитку математичного мислення; вміння застосовувати математичні знання у практичних ситуаціях і приймати обґрунтовані рішення; здійснювати покращення фахової діяльності та розвитку особистості.

Освітня компонента викладається для студентів денної форми здобуття освіти. При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема оглядові лекції, елементи комп'ютерної діагностики тощо.

Пререквізити − вища математика, теорія ймовірностей та математична статистика.
Кореквізити – прикладна криптологія.

Мета і завдання дисципліни

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.

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.

Очікувані 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.

Тематичний і календарний план вивчення дисципліни

Таблиця 3 – ***Тематичний і календарний план вивчення дисципліни***

№ тижня	Тема лекції*	Тема практичного заняття	Самостійна робота студента		
			зміст	год.	література
1	2	3	4	5	6
2 семестр					
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.	Подільність в множині цілих чисел.	ОТМ, ВДЗ	4	Л: [7, С. 14-19], [15, С. 14-68], [17, С. 7-8]. ПЗ: [17, С. 30-33].
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.	Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне.	ОТМ, ВДЗ	4	Л: [17, С. 8-12], [18, С. 87-91], [12, С. 24-29], [7, С. 30-35]. ПЗ: [17, С. 30-33, 36-39].
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.	Прості й складені числа.	ОТМ, ВДЗ,	4	Л: [17, С. 12-23], [18, С. 91-94], [7, С. 20-30]. ПЗ: [17, С. 30-33, 36-39].
4	**Числові функції.** Мультиплікативні числові функції. Функції $\tau(n)$, $\sigma(n)$, $\{x\}$, $[x]$. Функція Ойлера $\varphi(n)$,	Числові функції.	ОТМ, ВДЗ	4	Л: [17, С. 40-48], [12, С. 40-45]. ПЗ: [17, С. 49-53].

	функція Мебіуса μ(n), функція Кармайкла λ(n).				
5	**Конгруенції.** Означення конгруенції. Приклади. Властивості конгруенцій.	Конгруенції.	ОТМ, ВДЗ, **ТС-1 СР-1**	4	Л: [17, С. 54-58], [18, С. 111-115], [7, С. 43-47]. ПЗ: [17, С. 68], [9, С. 80-81].
6	**Повна та зведена система лишків.** Повна система лишків. Зведена система лишків. Теорема Ойлера і Ферма. Мультиплікативність функцій Ойлера.	Повна та зведена система лишків.	ОТМ, ВДЗ**,**	4	Л: [17, С. 58-66], [18, С. 115-120], [7, С. 47-48]. ПЗ: [17, С. 68], [9, С. 84-86].
7	**Лінійні конгруенції з одним невідомим**. Конгруенції першого степеня. Способи розв'язування конгруенцій першого степеня: метод спроб, метод рівносильних перетворень.	Лінійні конгруенції з одним невідомим.	ОТМ, ВДЗ,	4	Л: [17, С. 69-74], [18, С. 120-123], [7, С. 48-51] ПЗ: [17, С. 86-87], [8 С. 142-144]
8	Обернений елемент за множенням. Розвязування діафантових рівнянь. Китайська теорема про лишки. Системи конгруенцій з одним невідомим. Тести простоти. Тест псевдопростоти Ферма.	Обернений елемент за множенням. Системи конгруенцій з одним невідомим.	ОТМ, ВДЗ,	4	Л: [17, С. 77-84]. ПЗ: [17, С. 87-90], [8 С. 142-144].
9	**Конгруенції вищих степенів.** Конгруенції *n*-го степеня за простим модулем. Побудова рівносильних конгруенцій. Число розв'язків конгруенцій *n*-го степеня за простим модулем. Конгруенції *n*-го степеня за складеним модулем.	Конгруенції вищих степенів.	ОТМ, ВДЗ	4	Л: [17, С. 91-103], [10, С. 19-26]. ПЗ: [17, С. 106-107].
10	**Конгруенції другого степеня.** Загальні положення. Квадратичні лишки. Конгруенція за простим непарним модулем. Символ Лежандра. Символ Якобі.	Конгруенції другого степеня. Квадратичні лишки.	ОТМ, ВДЗ,	4	Л: [17, С. 108-141], [10, С. 26-30], [18, С. 134-143]. ПЗ: [17, С. 122], [9, С. 100-103].
11	**Первісні корені.** Означення порядків чисел і класів чисел за даним модулем. Властивості порядків за модулем. Первісні корені. Знаходження первісних коренів за елементарними модулями	Символ Лежандра. Символ Якобі.	ОТМ, ВДЗ	4	Л: [17, С. 141-170], [10, С. 30-33], [18, С. 155-162]. ПЗ: [17, С. 122], [9, С. 104].
12	**Дискретні логарифми (індекси).** Поняття індекса (дискретного логарифма). Побудова таблиць індексів. Застосування індексів до розв'язання конгруенцій.	Первісні корені.	ОТМ, ВДЗ	4	Л: [17, С. 123-170], [10, С. 33-34], [18, С. 162-178]. [14, С. 52-58]. ПЗ: [17, С. 172-172].
13	**Арифметичні застосування теорії конгруенцій** Ознаки подільності. Перевірка результатів арифметичних дій. Перетворення звичайного дробу в десятковий.	Дискретні логарифми (індекси).	ОТМ, ВДЗ, **КР-1**	5	Л: [10, С. 35-41]. ПЗ: [17, С. 172-173].
14	**Скінчені ланцюгові дроби.** Скінченні ланцюгові дроби. Подання раціональних чисел ланцюговими. Підхідні дроби ланцюгового дробу.	Скінчені ланцюгові дроби.	ОТМ, ВДЗ **ТС-2 СР-2**	5	Л: [18, С. 102-108], [7, С. 37-43]. ПЗ: [17, С. 33-36].
15	**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.	Нескінчені ланцюгові дроби.	ОТМ, ВДЗ, **СР-3, ТС-3**	5	Л: [18, С. 108-110], [17, С. 23-28]. ПЗ: [17, С. 33-36].

16	**Квадратичні ірраціональності і періодичні ланцюгові дроби.** Поняття квадратичної ірраціональності. Періодичний ланцюговий дріб. Теорема Лежандра.	Квадратичні ірраціональності і періодичні ланцюгові дроби.	ОТМ, ВДЗ,	5	Л: [18, С. 110-111]. ПЗ: [18, С. 110-111].
17	**Раціональні «вкорочення» як найкращі наближення.** Порядок наближення дійсних чисел раціональними. Найкращі наближення та ланцюгові дроби. Теорема Ліувілля. Діафантові наближення та діафантові рівняння.	Раціональні «вкорочення» як найкращі наближення.	ОТМ, ВДЗ **КР-2**	5	Л: [18, С. 111-112], [17, С. 29-30]. ПЗ: [18, С. 111-112], [17, С. 29-30].
18	**Застосування ланцюгових дробів.** Розв'язування конгруенцій першого степеня. Розв'язування діофантових рівнянь $aX+bY=c$. Рівняння Пелля.	Застосування ланцюгових дробів.	ОТМ, ВДЗ	5	Л: [18, С. 123-131], [17, С. 74-76], [3, С. 10-14]. ПЗ: [18, С. 123-131], [17, С. 74-76], [3, С. 10-14].
3 семестр					
1	**Алгебри. Бінарна алгебраїчні операція** Поняття бінарної операції. Напівгрупа. Нейтральний та обернений елемент.	Бінарна операція. Напівгрупа. Моноїд.	ОТМ, ВДЗ	4	Л: [1, С. 6--7]. ПЗ: [11, С.55-58].
2	**Група. Підгрупа.** Поняття групи. Приклади груп. Властивості груп. Підгрупи. Критерій підгрупи. Циклічні групи. Порядок елемента групи. Таблиці Келі.	Група. Підгрупа. Циклічна група. Порядок елемента групи. ТЬаблиці Келі.	ОТМ, ВДЗ	4	Л: [18, С. 7-35], [14, С. 8-9], [8, С. 5-85]. [1, С. 15-16]. ПЗ: [8, С. 15-17, 26-28, 33-35, 48-50]. [9, С. 29]. [1, С. 17].
3	**Група перестановок.** Симетрична групи (група перестановок). Добуток перестановок. Порядок перестановки. Знак перестановки. Парність перестановки. Інверсія.	Група перестановок. Порядок перестановки. Парність перестановки. Інверсія.	ОТМ, ВДЗ,	4	Л: [9, С. 12-16]. ПЗ: [1, С. 19-20].
4	**Многочлени, подільність многочленів.** Поняття многочлена. Операції над многочленами. Теорема про ділення з остачею. Алгоритм ділення з остачею. Означення НСД та НСК двох многочленів. Знаходження НСД (алгоритм Евкліда).	Многочлени, подільність многочленів.	ОТМ, ВДЗ	5	Л: [18, С. 51-61], [14, С. 12-14], [13, С. 126-134]. ПЗ: [1, С. 107-114].
5	**Теорема Безу та схема Горнера**. Незвідні многочлена. Основна теорема алгебри Кратні корені. Похідна многочлена. Результант многочленів. Дискримінант многочлена.. Формули Вієта.	Теорема Безу та схема Горнера. Основна теорема алгебри. Формули Вієта.	ОТМ, ВДЗ, **ТС-1 СР-1**	5	Л: [14, С. 12-14], [13, С. 134-141]. ПЗ: [11, С. 184-186, 194-197, 203-205].
6	**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.	Кільце. Підкільце.	ОТМ, ВДЗ**,**	5	Л: [18, С. 35-38], [14, С. 9-11], [8, С. 85-103]. ПЗ: [9, С. 33-37], [8, С. 103-105].
7	**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.	Фактор-кільця та ідеали.	ОТМ, ВДЗ,	5	Л: [18, С. 38-51], [8, С. 106-114]. ПЗ: [9, С. 37-40], [8, С. 115-117].
8	Теорема Ейлера, мала теорема Ферма. Мультиплікативна група кільця лишків за модулем n. Приклади груп лишків. Основні	Конгруенції і класи лишків за ідеалом.	ОТМ, ВДЗ, **КР-1**	5	Л: [8, С. 126-132]. [2, С. 8-9, 21-23, 40-41]. ПЗ: [9, С. 40-43].

	властивості Повна система лишків. Гомоморфізм кілець. Ізоморфізм кілець.				
9	**Поле. Підполе.** Означення поля. Приклади. Характеристика поля. Підполе поля. Критерій підполя. Розширення поля. Алгебра над полем. Ізоморфізм полів.	Поле. Підполе.	ОТМ, ВДЗ	5	Л: [18, С. 70-85]. [2, С. 8-9, 21-23, 40-41]. ПЗ: [18, С. 70-85].
10	**Позиційні системи числення.** Позиційні системи числення.	Позиційні системи числення.	ОТМ, ВДЗ,	5	Л: [12, С. 48-49], [19, С. 11-13], [6, С. 7-9]. [20, С. 40-44]. ПЗ: [20, С. 40-44].
11	Арифметичні дії в позиційних системах. Перехід до іншої позиційної системи. Ознаки подільності. Систематичні дроби.	Арифметичні дії в позиційних системах.	ОТМ, ВДЗ	5	Л: [12, С. 48-49], [19, С. 11-13], [6, С. 7-9]. [20, С. 44-46]. ПЗ: [20, С. 40-44].
12	**Нестандартні системи числення.** Нестандартні системи числення.	Перехід до іншої позиційної системи. Ознаки подільності. Систематичні дроби.	ОТМ, ВДЗ **ТС-2 СР-2**	5	Л: [19, С. 13-24]. ПЗ: [20, С. 44-46].
13	Елементарні відомості про еліптичні криві. Основні визначення. Способи побудови еліптичних кривих.	Еліптичні криві.	ОТМ, ВДЗ,	5	Л: [18, С. 179-182], [14, С. 107-109], [5, С. 109-110]. ПЗ: [18, С. 179-182], [14, С. 107-109], [5, С. 109-110],
14	Умова несингулярності еліптичної кривої. Операція додавання і побудова групи точок еліптичної кривої. Відшукання точок еліптичної кривої над скінченним полем.	Операція додавання і побудова групи точок еліптичної кривої.	ОТМ, ВДЗ **КР-2**	5	Л: [18, С. 182-188], [14, С. 109-112], [5, С. 111-114]. ПЗ: [18, С. 182-188], [14, С. 109-112], [5, С. 111-114].
15	Число елементів групи точок еліптичної кривої. Порядок точки еліптичної кривої. Вибір еліптичної кривої і базової точки.	Число елементів групи точок еліптичної кривої.	ОТМ, ВДЗ,	5	Л: [18, С. 188-199], [5, С. 114]. ПЗ: [18, С. 188-199], [5, С. 114].
16	**Псевдовипадкова послідовність.** Основні визначення випадкової послідовності. Вимоги. Лінійна рекурентна послідовність з максимальним періодом. Псевдовипадкова послідовність на базі багатомодульних перетворень.	Псевдовипадкова послідовність.	ОТМ, ВДЗ, **ТС-3 СР-3**	5	Л: [21, С. 49-51], [22, С. 147-154]. ПЗ: [21, С. 49-51], [22, С. 147-154].
17	**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.	Генератор псевдовипадкових чисел.	ОТМ, ВДЗ	5	Л: [16, С. 3-9], [4, С. 25-26], [22, С. 147-154]. ПЗ: [16, С. 3-9], [4, С. 25-26], [22, С. 147-154].

ОТМ - опрацювання теоретичного матеріалу.

ВДЗ – виконання домашніх завдань

Примітка: * Лекції та практичні заняття проводяться щотижня по дві години.

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і практичні заняття згідно з розкладом, не запізнюватися на заняття, курсову роботу та інші домашні завдання виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних занять студент має підготуватися за відповідною

темою і проявляти на занятті активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання і зарахування результатів навчання здобувачів вищої освіти у ХНУ (вебсайт Університету (https://khmnu.edu.ua/): розділ «Нормативні документи», рубрика – «Положення», сторінка – «Положення про організацію освітньої діяльності».).

Критерії оцінювання результатів навчання.

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 урахуванням коефіцієнта вагомості і встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування; засвоєння теоретичного матеріалу з тем перевіряється письмовим (тестовим) контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом розв'язання задач та захисту індивідуальних домашніх завдань. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; вміння студента обґрунтувати прийняті рішення та розв'язувати задачі; своєчасне виконання домашніх індивідуальних завдань з теми.

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**

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. При цьому, у першому та другому семестрі, за вітчизняною шкалою ставиться «відмінно», «добре», або «задовільно». За шкалою ЄКТС ставиться буквене позначення оцінки, що відповідає набраній студентом кількості балів.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

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

Питання для підсумкового контролю з дисципліни
2семестр

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.

3 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. 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.

Рекомендована література

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 посібник / 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 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.

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.