Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ Олег Ілляшенко
(підпис) (ім'я та ПРІЗВИЩЕ)

« 31 » серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теоретичні основи криптології
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека та захист інформації»
(код і найменування спеціальності)

Освітня програма: «Безпека інформаційних і комунікаційних систем»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): __Андрій Карпенко, ст. викладач, д-р філософії_ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____
__комп’ютерних систем, мереж і кібербезпеки_____
(назва кафедри)

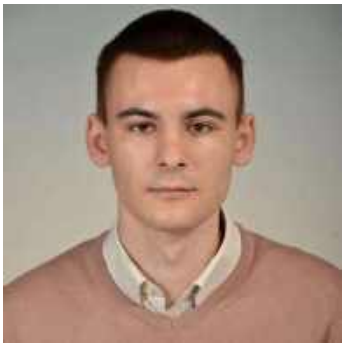
Протокол № 1 від « 29» серпня 2025 р.

Завідувач кафедри д.т.н., професор _____ _Вячеслав Харченко___
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК_____
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача



ПІБ: Карпенко Андрій Сергійович

Посада: старший викладач

Науковий ступінь: Ph.D.

Вчене звання: відсутнє

Перелік дисциплін, які викладає:
захист інформації в комп'ютерних мережах, теоретичні основи криптології, управління інформаційною безпекою, теорія та технології розробки безпечних розподілених систем.

Напрями наукових досліджень:
хмарні технології, кібербезпека, тестування програмного забезпечення.

Контактна інформація:
a.karpenko@csn.khai.edu, +380507095250

2. Опис навчальної дисципліни

Форма здобуття освіти	*денна*
Семестр	4-й
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 3.5 кредитів ЄКТС / 105 годин (64 аудиторних, з яких: лекції – 32, лабораторні – 32; СРЗ – 41);
Види навчальної діяльності	Лекції, лабораторні заняття, розрахункова робота, самостійна робота.
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит.
Пререквізити	Вища математика, дискретна математика, фізика, моделі та структури даних

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – ознайомлення тих, хто навчається, з методологією, основними поняттями, методами та алгоритмами елементарної теорії чисел і теорії алгебраїчних структур, а також набуття навичок розрахунку параметрів числових систем, рішення порівнянь різного ступеня, роботи з алгебраїчними структурами (групами, кільцями, полями) та еліптичними кривими для їх застосування в сучасних криптографічних системах.

Завдання – вивчення принципів і методів елементарної теорії чисел (подільність, прості числа, порівняння, функції теорії чисел), теорії алгебраїчних структур (групи, кільця, поля Галуа), а також основ теорії еліптичних кривих як математичного апарату для побудови та аналізу сучасних криптографічних алгоритмів і протоколів захисту інформації.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(ЗК1) здатність застосовувати знання у практичних ситуаціях.

(ЗК2) знання та розуміння предметної області і розуміння професійної діяльності.

(ЗК3) здатність спілкуватися державною мовою як усно, так і письмово.

(ЗК4) здатність спілкуватися іноземною мовою.

(ЗК5) здатність вчитися і оволодівати сучасними знаннями.

Спеціальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(СК1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

(СК3) здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

(СК6) здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

(СК8) здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

(СК10) Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно встановленою політикою інформаційної безпеки.

Результати навчання:

(РН1) вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

(РН2) спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

(РН4) організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

(РН7) застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

(РН8) застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

(РН9) знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

(РН10) використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

(РН18) аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Основні поняття елементарної теорії чисел і основи теорії порівнянь

Тема 1. Вступ до навчальної дисципліни. Базові поняття елементарної теорії чисел

Анотація: Розглядаються предмет, мета вивчення та задачі дисципліни. Вивчається класифікація чисел як математичних об'єктів, прості числа та їх властивості, роль простих чисел у сучасній криптографії. Аналізуються теорема про ділення з лишком, основна теорема арифметики та факторизація.

Тема лекції 1: Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни. Класифікація чисел як математичних об'єктів. Досконалі та дружні числа.

Тема лекції 2: Прості числа та їх властивості. Числа Мерсена та Ферма. Роль простих чисел у криптографії. Теорема про ділення з лишком. Основна теорема арифметики і факторизація.

Тема лекції 3: Найбільший спільний дільник і найменше спільне кратне та їх властивості. Взаємно-прості числа. Способи обчислення НСД і НСК.

Тема лабораторного заняття 1: Рішення задач на тему «Подільність з лишком, ознаки подільності».

Самостійна робота здобувачів: Аксіома індукції. Аксіома Архімеда. Теореми, що стосуються натуральних чисел. Опрацювання матеріалу лекцій, підготовка до модульного контролю, виконання індивідуальних завдань, проходження тестування за результатами роботи на лекційних заняттях, формування питань до викладача.

Тема 2. Основи теорії порівнянь

Анотація: Вивчаються порівняння та їх властивості, повний та приведений набори лишків за даним модулем. Розглядаються арифметичні застосування теорії порівнянь.

Тема лекції 1: Порівняння та їх властивості. Повний та приведений набори лишків за даним модулем. Арифметичні застосування теорії порівнянь.

Тема лабораторного заняття 1: Рішення задач на тему «Прості і складові числа, найбільший спільний дільник і найменше спільне кратне».

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, виконання індивідуальних завдань.

Тема 3. Найважливіші функції і теореми елементарної теорії чисел

Анотація: Розглядаються мультиплікативні функції та їх властивості: функція Мьобіуса, функція Ейлера, функція Кармайкла. Вивчаються теорема Ейлера-Ферма, теорема Кармайкла, теорема Вільсона та Китайська теорема про лишки.

Тема лекції 1: Мультиплікативні функції та їх властивості. Функція Мьобіуса, функція Ейлера, функція Кармайкла.

Тема лекції 2: Теорема Ейлера-Ферма. Теорема Кармайкла. Теорема Вільсона. Китайська теорема про лишки.

Тема лабораторного заняття 1: Рішення задач за темами «Властивості порівнянь», «Арифметичні застосування теорії порівнянь», «Функції і теореми теорії чисел».

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до модульного контролю.

Модульний контроль 1

Змістовний модуль 2. Підвищення кібербезпеки глобально розподілених систем

Тема 4. Рішення порівнянь першого ступеню та систем порівнянь першого ступеню

Анотація: Вивчаються методи рішення порівнянь першого ступеню за способом Ейлера та на основі ланцюгових дробів. Розглядаються рішення систем порівнянь першого ступеню методом прямої заміни та на основі китайської теореми про лишки.

Тема лекції 1: Рішення порівнянь першого ступеню за способом Ейлера та на основі ланцюгових дробів. Рішення систем порівнянь першого ступеню методом прямої заміни та на основі китайської теореми про лишки.

Тема лабораторного заняття 1: Рішення порівнянь першого ступеню і систем порівнянь першого ступеню.

Самостійна робота здобувачів: Застосування теорії ланцюгових дробів для вирішення порівнянь першого ступеня. Виконання індивідуальних завдань.

Тема 5. Основи теорії квадратичних лишків

Анотація: Розглядаються квадратичні лишки за даним модулем та їх властивості. Вивчається критерій Ейлера, символи Лежандра та Якобі та їх властивості.

Тема лекції 1: Квадратичні лишки за даним модулем та їх властивості. Критерій Ейлера. Символи Лежандра та Якобі та їх властивості.

Тема лабораторного заняття 1: Рішення порівнянь другого ступеню. Обчислення символів Лежандра і Якобі.

Самостійна робота здобувачів: Порівняння другого ступеню за складовим модулем. Опрацювання матеріалу лекцій.

Тема 6. Основи теорії степінних лишків та індексів

Анотація: Вивчаються поняття про степінь числа за заданим модулем, первообразні корені та індекси (дискретні логарифми). Розглядається застосування індексів до рішення порівнянь різного ступеня.

Тема лекції 1: Степінь числа за заданим модулем, первообразні корені та індекси (дискретні логарифми). Застосування індексів до рішення порівнянь різного ступеня.

Тема лабораторного заняття 1: Рішення задач за темою «Показники числа за заданим модулем, первообразні корені та індекси».

Самостійна робота здобувачів: Первообразні корені та індекси за складовим модулем. Виконання індивідуальних завдань.

Модульний контроль 2

Змістовний модуль 3. Основні поняття теорії алгебраїчних систем і теорії груп

Тема 7. Основні поняття теорії алгебраїчних систем

Анотація: Розглядаються алгебраїчні системи (структури) та їх компоненти: закони композиції об'єктів, адитивне і мультиплікативне представлення властивостей, регулярний, нейтральний та зворотній елементи. Вивчається класифікація алгебраїчних систем.

Тема лекції 1: Алгебраїчні системи (структури) та їх компоненти. Закони композиції об'єктів. Регулярний, нейтральний та зворотній елементи. Класифікація алгебраїчних систем та їх приклади.

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, виконання індивідуальних завдань.

Тема 8. Основи теорії груп

Анотація: Вивчається поняття групи як алгебраїчної системи. Розглядаються групи підстановок, теорема Келі, ізоморфізм груп, циклічні групи. Аналізуються теорема Лагранжа, нормальні дільники групи, фактор-група, ядро гомоморфізму та теорема про гомоморфні відображення.

Тема лекції 1: Поняття групи. Приклади груп. Групи підстановок, парні та непарні підстановки. Теорема Келі. Ізоморфізм груп. Циклічні групи та їх підгрупи.

Тема лекції 2: Теорема Лагранжа та наслідки з неї. Нормальні дільники групи. Фактор-група. Ядро гомоморфізму та приклади гомоморфних відображень. Теорема про гомоморфні відображення.

Тема лабораторного заняття 1: Рішення задач за темою «Основи теорії груп».

Самостійна робота здобувачів: Гомоморфізм та ізоморфізм груп. Ядро гомоморфізму та приклади гомоморфних відображень. Нормальні дільники групи. Фактор-група. Теорема про гомоморфні відображення. Автоморфізми груп.

Змістовний модуль 4. Основи теорії кілець, полів і еліптичних кривих

Тема 9. Побудова архітектури розподіленої системи з урахуванням вимог до безпеки та надійності

Анотація: Розглядається поняття про кільце як алгебраїчну систему. Вивчаються підкільце, ідеал, дільник нуля, кільце цілісності. Аналізуються приклади кілець: кільце цілих чисел, кільце лишків за даним модулем, кільце многочленів.

Тема лекції 1: Поняття про кільце. Підкільце, ідеал. Дільник нуля, кільце цілісності. Приклади кілець та підкілець: кільце цілих чисел, кільце лишків за даним модулем, кільце многочленів.

Самостійна робота здобувачів: Факторіальність кільця многочленів і кільця цілих чисел. Ізоморфізм та гомоморфізми кілець. Китайська теорема про лишки та функція Ейлера з точки зору ізоморфізму кілець.

Тема 10. Основи теорії полів

Анотація: Вивчається поняття про поле як алгебраїчну систему. Розглядаються кінцеві поля (поля Галуа), характеристика поля, примітивний

елемент поля. Аналізуються кільце лишків за простим модулем та фактор-кільце многочленів як поле, елементи алгебри двійкових многочленів над кінцевим полем.

Тема лекції 1: Поняття про поле. Приклади полів. Кінцеві поля (поля Галуа). Характеристика поля. Примітивний (породжуючий) елемент поля.

Тема лекції 2: Кільце лишків за простим модулем та фактор-кільце многочленів як поле. Елементи алгебри двійкових многочленів над кінцевим полем. Кінцеве поле як векторний простір над підполем.

Самостійна робота здобувачів: Кільце лишків за простим модулем та фактор-кільце многочленів як поле. Елементи алгебри двійкових многочленів над кінцевим полем. Кінцеве поле як векторний простір над підполем, характеристика якого є просте число.

Тема 11. Основи теорії еліптичних кривих

Анотація: Розглядається поняття про еліптичні криві (ЕК) як алгебраїчну систему. Вивчаються ЕК над простим кінцевим полем та над розширеним кінцевим полем з перетвореннями в афінних та проєктивних координатах.

Тема лекції 1: Поняття про еліптичні криві. ЕК як алгебраїчна система. ЕК над простим кінцевим полем з перетвореннями в афінних координатах. ЕК над розширеним кінцевим полем з перетвореннями в афінних координатах.

Тема лабораторного заняття 1: Розрахунок параметрів еліптичних кривих у простому та розширеному полях.

Самостійна робота здобувачів: ЕК над простим кінцевим полем з перетвореннями в проєктивних координатах. ЕК над розширеним кінцевим полем з перетвореннями в проєктивних координатах. Виконання розрахункової роботи.

5. Індивідуальні завдання

Побудова таблиці Келі для груп точок еліптичної кривої над розширеним полем.

6. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

7. Методи контролю

Поточний контроль: опитування на лекційних та лабораторних заняттях з основних понять елементарної теорії чисел та алгебраїчних структур; аналіз та порівняння методів рішення порівнянь різного ступеню; виконання письмових контрольних робіт з окремих розділів курсу (подільність та прості числа, порівняння та їх властивості, функції теорії чисел, квадратичні та степінні лишки, теорія груп, кілець та полів, еліптичні криві); програмований контроль (тестування, онлайн-тести) з теоретичних основ та практичних аспектів криптології; оцінювання виконання індивідуальних лабораторних робіт з рішення задач на подільність, обчислення НСД і НСК, рішення порівнянь першого та другого ступеню, обчислення символів Лежандра і Якобі, роботи з первообразними коренями та індексами, розрахунку параметрів еліптичних кривих; перевірка звітів з лабораторних робіт та їх захист; оцінювання виконання індивідуальних розрахункових завдань з визначення параметрів криптографічних систем на основі теорії чисел та еліптичних кривих.

Модульний контроль: складання модульного контролю з змістового модуля 1 "Основні поняття елементарної теорії чисел і основи теорії порівнянь", змістового модуля 2 "Рішення систем порівнянь та основи теорії степінних лишків", змістового модуля 3 "Основні поняття теорії алгебраїчних систем і теорії груп" та змістового модуля 4 "Основи теорії кілець, полів і еліптичних кривих"; перевірка знань з теоретичних основ теорії чисел, властивостей порівнянь, функцій Ейлера та Кармайкла, теорем Ейлера-Ферма та Вільсона, Китайської теореми про лишки, квадратичних та степінних лишків, алгебраїчних структур, полів Галуа та еліптичних кривих; оцінювання практичних навичок роботи з числовими системами, рішення порівнянь та розрахунку параметрів криптографічних примітивів.

Підсумковий контроль: іспит, що включає теоретичні питання з усіх розділів курсу та практичні завдання з аналізу властивостей числових систем, рішення порівнянь різного ступеню, обчислення функцій теорії чисел, роботи

з алгебраїчними структурами та розрахунку параметрів еліптичних кривих для застосування у криптографічних алгоритмах.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1 Змістовний модуль 1			
Робота на лекціях	0...1	6	0...6
Лабораторні заняття	0...6	3	0...18
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	3	0...18
Модульний контроль	0…10	1	0…10
Модуль 2 Змістовний модуль 3			
Робота на лекціях	0...1	3	0...3
Лабораторні заняття	0...6	1	0...6
Модульний контроль	0…10	1	0...8
Змістовний модуль 4			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	1	0...6
Модульний контроль	0…10	1	0...7
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови здобувача освіти від балів підсумкового контролю. Під час складання семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.

Білет для заліку складається з двох теоретичних і одного практичного запитання. За теоретичні запитання студент отримує до 60 балів (до 30 балів за кожне) , за практичне – до 40 балів. Під час складання семестрового заліку здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав чотири модульні контрольні роботи. Знає основні визначення та термінологію в галузі теорії чисел та алгебраїчних структур. Розуміє класифікацію чисел як математичних об'єктів, властивості простих чисел та їх роль у криптографії. Знає теорему про ділення з лишком, основну теорему арифметики. Описує способи обчислення НСД і НСК, властивості взаємно-простих чисел. Розрізняє порівняння та їх властивості, повний та приведений набори лишків. Знає основні мультиплікативні функції: функцію Ейлера, Мьобіуса, Кармайкла. Пояснює теореми Ейлера-Ферма, Кармайкла, Вільсона та Китайську теорему про лишки. Описує базові принципи рішення порівнянь першого та другого ступеню. Знає поняття квадратичних лишків, символів Лежандра та Якобі. Розуміє основні поняття теорії груп, кілець та полів. Знає базові властивості еліптичних кривих. Виконує лабораторні роботи з рішення задач на подільність, обчислення порівнянь та параметрів алгебраїчних структур. Використовує стандартні методи теорії чисел для розв'язання базових задач.

Добре (75-89) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав чотири модульні контрольні роботи. Додатково до вимог на оцінку "задовільно": Проводить порівняльний аналіз методів рішення порівнянь (спосіб Ейлера, ланцюгові дроби, Китайська теорема про лишки), порівнює їх ефективність та область застосування. Самостійно аналізує та обчислює функції теорії чисел для конкретних параметрів криптосистем. Розраховує символи Лежандра та Якобі, застосовує критерій Ейлера для визначення квадратичних лишків. Самостійно знаходить первообразні корені та обчислює індекси (дискретні логарифми). Знає структуру та особливості алгебраїчних систем: груп, кілець та полів. Аналізує властивості циклічних груп, застосовує теорему Лагранжа. Розуміє принципи побудови кінцевих полів (полів Галуа) та їх застосування в криптографії. Виконує розрахунки параметрів еліптичних кривих у простому та розширеному полях. Порівнює різні алгебраїчні структури та обґрунтовує вибір оптимальних параметрів для криптографічних застосувань.

Відмінно (90-100) – здобувач має глибокі знання, навички та вміння для досягнення результатів навчання за програмою на високому рівні. Написав чотири модульні контрольні роботи на відмінно. Додатково до вимог на оцінку "добре": Вільно оперує термінологією теорії чисел та алгебраїчних структур. Самостійно доводить основні теореми курсу (Ейлера-Ферма, Вільсона, Лагранжа, Китайську теорему про лишки). Обґрунтовує вибір числових параметрів для конкретних криптографічних застосувань з урахуванням складності факторизації та дискретного логарифмування. Аналізує ізоморфізм та гомоморфізм алгебраїчних структур, застосовує теорему про гомоморфні

відображення. Проектує параметри кінцевих полів та еліптичних кривих з урахуванням вимог криптостійкості. Самостійно виконує перетворення на еліптичних кривих в афінних та проєктивних координатах. Демонструє творчий підхід до розв'язання нестандартних задач, пропонує оригінальні методи рішення порівнянь та обчислення параметрів алгебраїчних структур. Вільно захищає лабораторні роботи, демонструючи глибоке розуміння теоретичних основ та їх застосування в криптографії.

9. Політика навчального курсу

Відвідування занять. Обов'язкове відвідування лекційних та лабораторних занять з навчальної дисципліни "Теоретичні основи криптології" через їх інтерактивний характер та необхідність практичного освоєння методів теорії чисел, рішення порівнянь різного ступеню, роботи з алгебраїчними структурами та розрахунку параметрів еліптичних кривих для криптографічних застосувань. Здобувачі освіти, які не можуть регулярно відвідувати заняття, зобов'язані узгодити з викладачем протягом тижня графік відпрацювання пропущених занять. Пропущені заняття необхідно відпрацювати під час найближчої консультації протягом тижня з моменту пропуску, як правило, у формі усного опитування за попередньо визначеними питаннями з відповідних тем курсу. У деяких випадках допускається відпрацювання пропущених лабораторних занять у формі виконання письмових завдань з рішення порівнянь, обчислення функцій теорії чисел, аналізу властивостей алгебраїчних структур або розрахунку параметрів еліптичних кривих. Пропуск модульних контрольних робіт без поважної причини не допускається.

Дотримання вимог академічної доброчесності Здобувачі освіти зобов'язані дотримуватися загальних морально-етичних норм, а також вимог академічної доброчесності, викладених у "Положенні про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут»" (https://khal.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Роботи здобувачів освіти (звіти з лабораторних робіт, розрахункова робота, модульні контрольні роботи) повинні бути оригінальними. Прикладами порушення академічної доброчесності є відсутність посилань на джерела, вигадування джерел, плагіат, перешкоджання роботі інших здобувачів освіти. Виявлення ознак порушення академічної доброчесності в письмових роботах (звітах з лабораторних робіт, розрахунковій роботі, модульних контрольних роботах) призводить до оцінки "незадовільно" незалежно від масштабу плагіату або обману. Особлива увага приділяється оригінальності програмного коду, реалізованого під час лабораторних робіт з дослідження криптографічних алгоритмів та стеганографічних методів. Використання готових рішень без посилань на джерела та без власного аналізу та модифікації вважається порушенням академічної доброчесності.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khal.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор»: [Ел. ресурс]. https://mentor.khai.edu/course/view.php?id=1636.

11. Рекомендована література

Базова

1. Елементи теорії чисел: навч. посіб. / О. І. Оглобліна, Т.С. Сушко, Ю. В. Шрамко. – Суми: Сумський державний університет, 2015. – 186 с.
2. Стасюк, М., Елементи математичних основ криптографії : навчальний посібник / М. Стасюк – Львів: ЛДУ БЖД, 2021. – 216 с.
3. Лисенка, І.В. Основи елементарної теорії чисел [Текст]: навч. посібник з практ. заняттям/І.В. Лисенка. - Х.: Нац. аерокосм. ун-т ім. Н.Є. Жуковського «Харк. авіац. ін-т», 2017. - 42 с.
4. Лисенко, І.В. Математика еліптичних кривих та криптографія [Текст]: навч. посібник/І.В. Лисенка. - Х.: Нац. аерокосм. ун-т ім. Н.Є. Жуковського «Харк. авіац. ін-т», 2016. - 52 с.
5. Ковальчук Л.В., Маслова Н.О. Математичні методи криптографії. Електронний навчальний посібник. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 146с.: рис. 3, означень 147, теорем 29, бібліогр. 19.
6. 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.

Допоміжна

1. Повідайчик М.М. Професійна діяльність вчителя інформатики в сфері інформаційної безпеки / М.М. Повідайчик, І.Я. Шпонтак // Науковий

вісник УжНУ. Серія: Педагогіка. Соціальна робота. Вип. 1 (42). 2018. С. 179-182.
2. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: В-во УжНУ «Говерла», 2020. 28 с.
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
4. Крафт Д., An Introduction to Number Theory with Cryptography / Джеймс Крафт, Вашингтон Лоуренс // Taylor & Francis, 2018, 578.
5. Hoffstein J., An Introduction to Mathematical Cryptography / Jeffrey Hoffstein // Springer, 2008, 640 с.
6. Koblitz N., A Course in Number Theory and Cryptography / Neal Koblitz // Springer, 2012, 245.

12. Інформаційні ресурси

1. http://www.csn.khai.edu Кафедральний сайт.
2. http://www.dsszzi.gov.ua Державна служба спеціального зв'язку та захисту інформації України.
3. https://dlmf.nist.gov/27 NIST Functions of Number Theory.
4. https://cacr.uwaterloo.ca/hac/ Handbook of Applied Cryptography.