Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки(№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА 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 та найменування спеціальності)

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

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

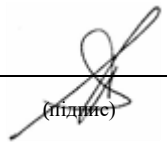
Розробник: Карпенко А.С., асистент

(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки

(назва кафедри)

Протокол № 1 від «30» 08 2023 р.

Завідувач кафедри д .т.н., професор  В. С. Харченко

(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 4,5</td><td rowspan="12">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека та захист інформації"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем,
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 4</td><td>2023/ 2024</td></tr>
<tr><td>Індивідуальне завдання – «Побудова таблиці Келі для групи точок еліптичної кривої над розширеним полем»</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 48*/135</td><td>4-й</td></tr>
<tr><td>Лекції 1)</td></tr>
<tr><td rowspan="6">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 5,5</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>87 годин</td><td>Вид контролю</td></tr>
<tr><td></td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *48/ 87.*

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

1. Мета вивчення: володіння навичками з виконання теоретико-числових та алгебраїчних перетворень, що виникають під час розрахунку параметрів та аналізу криптографічних алгоритмів і протоколів.

2. Завдання: формування знань і навичок щодо здійснювання базовових теоретико-числових та алгебраїчних перетворень; використовувати принципи доведення теоретико-числових та алгебраїчних теорем; класифікувати та аналізувати числові алгебраїчні системи.

3. Компетентності, які набуваються. Дисципліна має допомогти сформувати у студентів такі компетентності:

– (КЗ 1) здатність застосовувати знання у практичних ситуаціях;

– (КЗ 2) знання та розуміння предметної області та розуміння професії;

– (КЗ 4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– (КЗ 5) здатність до пошуку, оброблення та аналізу інформації.

– (КФ 1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;

– (КФ 4) здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

– (КФ 7) здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);

– (КФ 10) здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;

– (КФ 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.

4. Очікувані результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

– (ПРН 1) застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

– (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 6) критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

– (ПРН 19) застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

– (ПРН 31) застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

– (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.

5. Міждисциплінарні зв'язки. Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема (ОК 1) «Вища математика», (ОК 12) «Дискретна математика». Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін із циклу професійної підготовки, зокрема (ОК8) «Теорія інформації та кодування», (ОК15) «Курс на вибір 1. Захист інформації в інформаційно-комунікаційних системах», (ОК18) «Інформаційно-комунікаційні системи», (ОК23) «Прикладна криптологія».

Пререквізити – дисципліни (ОК1) «Вища математика», (ОК2) «Дискретна математика», (ОК6) «Фізика», (ВК5) «Соціально-гуманітарна дисципліна за вибором».

Кореквізити – дисципліни (ОК26) «Побудова та кібербезпека інтернету речей», (ОК22) «Безпечні вбудовані системи», (ОК20) «Теорія інформації і кодування».

3. Програма навчальної дисципліни

Модуль 1

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

Тема 1. Вступ до начальної дисципліни.

Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі (зв'язок даного курсу з іншими дисциплінами). Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Стислий екскурс в історію теорії чисел та теорії алгебраїчних систем.

Тема 2. Базові поняття елементарної теорії чисел.

Класифікація чисел як математичних об'єктів. Досконалі та дружні числа. Прості числа та їх властивості; теореми, що стосуються простих чисел. Прості числа спеціального типу: числа Мерсена та їх зв'язок з простими числами Мерсена, числа Ферма. Роль простих чисел у сучасній криптографії. Теорема про ділення з лишком. Основна теорема арифметики і факторизація. Найбільший спільний дільник (НСД) і найменше спільне кратне (НСК) та їх властивості. Взаємно-прості числа та деякі теореми з ними пов'язані. Способи обчислення НСД і НСК.

Тема 3. Основи теорії порівнянь.

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

Тема 4. Найважливіші функції і теореми елементарної теорії чисел

Мультипликативні функції та їх властивості. Приклади мультипликативних функцій: функція Мьобіуса, функція Ейлера, функція Кармайкла. Теорема Ейлера-Ферма. Теорема Кармайкла. Теорема Вільсона. Китайська теорема про лишки.

Модульний контроль

Змістовний модуль 2. Рішення систем порівнянь першого ступеню і основи теорії степінних лишків.

Тема 5. Рішення порівнянь першого ступеню та систем порівнянь першого ступеню.

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 6. Основи теорії квадратичних лишків.

Поняття про квадратичні лишки за даним модулем та їх властивості. Критерій Ейлера. Символи Лежандра та Якобі та їх властивості.

Тема 7. Основи теорії степінних лишків та індексів.

Поняття про степінь числа за заданим модулем, первообразні корені та індекси (дискретні логарифми). Застосування індексів до рішення порівнянь різного ступеня.

Модульний контроль

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

Тема 8. Основні поняття теорії алгебраїчних систем.

Поняття про алгебраїчні системи (структури) та їх компоненти (закони композиції об’єктів та аддитивне і мультипликативне представлення їх властивостей; регулярний, нейтральний та зворотній елементи). Класифікація алгебраїчних систем та їх приклади.

Тема 9. Основи теорії груп.

Поняття групи (група яка алгебраїчна система). Приклади груп. Групи підстановок, парні та непарні підстановки. Теорема Келі. Ізоморфізм груп. Циклічні групи та їх підгрупи. Ізоморфізм циклічних груп однакового порядку. Теорема Лагранжа та наслідки з неї. Нормальні дільники групи. Фактор-група. Ядро гомоморфізму та приклади гомоморфних відображень. Теорема про гомоморфні відображення.

Модульний контроль

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

Тема 10. Основи теорії кілець.

Поняття про кільце (кільце яка алгебраїчна система). Поняття про підкільце, ідеал. Дільник нуля, кільце цілісності. Приклади кілець та підкілець:

кільце цілих чисел, кільце лишків за даним модулем, кільце многочленів (поліномів).

Тема 11. Основи теорії полів.

Поняття про поле (поле яка алгебраїчна система). Приклади полів. Кінцеві поля (поля Галуа). Характеристика поля. Примітивний (породжуючий) елемент поля. 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 12. Основи теорії еліптичних кривих.

Поняття про еліптичні криві (ЕК). ЕК як алгебраїчна система. ЕК над простим кінцевим полем з перетвореннями в афінних координатах. ЕК над простим кінцевим полем з перетвореннями в проєктивних координатах. ЕК над розширеним кінцевим полем з перетвореннями в афінних координатах. ЕК над розширеним кінцевим полем з перетвореннями в проєктивних координатах.

Модульний контроль

4. Структура навчальної дисципліни

Назви модулів і тем	*Кількість годин*				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Модуль 1.					
Змістовний модуль 1. Основні поняття елементарної теорії чисел і основи теорії порівнянь.					
1. Вступ до навчальної дисципліни	1	1		-	-
2. Базові поняття елементарної теорії чисел.	16	4		2	10
3. Основи теорії порівнянь.	12	4		-	8
4. Найважливіші функції і теореми елементарної теорії чисел.	4	2		2	-
Модульний контроль	1			1	
Разом за змістовним модулем 1	***34***	***11***		***5***	***18***
Змістовний модуль 2. Рішення систем порівнянь першого ступеню і основи теорії степінних лишків.					
5. Рішення порівнянь першого ступеню та систем порівнянь першого ступеню.	12	4		-	8
6. Основи теорії квадратичних лишків.	12	2		2	8
7. Основи теорії степінних лишків та індексів.	13	2		3	8
Модульний контроль	1			1	
Разом за змістовним модулем 2	***38***	***8***		***6***	***24***

Змістовний модуль 3. Основні поняття теорії алгебраїчних систем і теорії груп.					
8. Основні поняття теорії алгебраїчних систем.	12	2		-	10
9. Основи теорії груп.	16	4		1	11
Модульний контроль	1			1	
Разом за змістовним модулем 3	***29***	***6***		***2***	***21***
Змістовний модуль 4. Основи теорії кілець, полів і еліптичних кривих.					
10. Основи теорії кілець.	10	2		-	8
11. Основи теорії полів.	8	2		-	6
12. Основи теорії еліптичних кривих.	11	3		2	6
Модульний контроль	1			1	
Разом за змістовним модулем 4	***30***	***7***		***3***	***20***
Модуль 2.					
Індивідуальне завдання	4				4
Усього годин	***135***	***32***		***16***	***87***

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
1	Не передбачено		
	Разом		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
1	Не передбачено		
	Разом		

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Рішення задач на тему «Подільність з лишком, ознаки подільності».	2
2	Рішення задач на тему «Прості і складові числа, найбільший спільний дільник і найменше спільне кратне».	2

№ з/п	Назва теми	Кількість годин
3	Рішення задач за темами «Властивості порівнянь», «Арифметичні застосування теорії порівнянь», «Функції і теореми теорії чисел».	2
4	Рішення порівнянь першого ступеню і систем порівнянь першого ступеню.	2
5	Рішення порівнянь другого ступеню. Обчислення символів Лежандра і Якобі.	2
6	Рішення задач за темою «Показники числа за заданим модулем, першообразні корені та індекси».	2
7	Рішення задач за темою «Основи теорії груп»	2
8	Розрахунок параметрів еліптичних кривих у простому та розширеному полях.	2
	Разом	**16**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Аксіома індукції. Аксіома Архімеда. Теореми, що стосуються натуральних чисел.	10
2	Застосування теорії ланцюгових дробів для вирішення порівнянь першого ступеня.	8
3	Порівняння другого ступеню за складовим модулем.	9
4	Першообразні корені та індекси за складовим модулем.	10
5	ЕК над простим кінцевим полем з перетвореннями в проєктивних координатах. ЕК над розширеним кінцевим полем з перетвореннями в проєктивних координатах.	8
6	Гомоморфізм та ізоморфізм груп. Ядро гомоморфізму та приклади гомоморфних відображень. Нормальні дільники групи. Фактор-група. Теорема про гомоморфні відображення. Автоморфізми груп.	12
7	Поняття про підкільце, ідеал. Дільник нуля, кільце цілісності. Факторіальність кільца многочленів і кільца цілих чисел. Ізоморфізм та гомоморфізми кілець. Китайська теорема про лишки та функція Ейлера з точки зору ізоморфізму кілець.	12
8	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.	12
9	Виконання розрахункової роботи	6
	Разом	**87**

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист лабораторних (практичних) робіт	3...5	3	9...15
Модульний контроль	5…10	1	5…10
Змістовний модуль 2			
Виконання і захист лабораторних (практичних) робіт	3...5	3	9...15
Модульний контроль	5…10	1	5…10
Змістовний модуль 3			
Виконання і захист лабораторних (практичних) робіт	3...5	1	3...5
Модульний контроль	5…10	1	5…10
Змістовний модуль 4			
Виконання і захист лабораторних (практичних) робіт	3...5	1	3...5
Модульний контроль	5…10	1	5…10
Усього за семестр			**60…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

знати базові поняття елементарної теорії чисел і теорії алгебраїчних систем;

- знати основи теорії порівнянь і теорії квадратичних лишків;
- знати основні методи рішення порівнянь та систем порівнянь першого ступеню;
- знати основи теорії груп, кілець, полів;
- знати основи теорії еліптичних кривих.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- уміти обчислювати основні функції елементарної теорії чисел;
- уміти вирішувати порівняння та системи порівнянь першого ступеня;
- уміти вирішувати квадратичні порівняння, а також символи Лежандра і Якобі;
- уміти вирішувати порівняння за допомогою індексів;
- уміти аналізувати алгебраїчні системи на предмет їх приналежності до того або іншого класу;
- уміти виконувати операції додавання і множення в групі точок еліптичних кривих.

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти обчислювати основні функції елементарної теорії чисел, вирішувати порівняння першого ступеню за допомогою обчислення функції Ейлера, уміти розраховувати символи Лежандра і Якобі, а також обчислювати індекси за даним модулем. Знати базові поняття теорії алгебраїчних систем та теорії груп. Уміти виконувати операції додавання и множення точок на число в групі точок еліптичних кривих.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань практичних занять. Уміти: вирішувати порівняння першого ступеню за допомогою розширеного алгоритму Евкліда, вирішувати квадратичні порівняння і системи порівнянь в тому числі за допомогою китайської теореми про лишки, виконувати операції додавання точок в групі точок еліптичних кривих в проективних координатах, вирішувати порівняння довільного ступеню за допомогою обчислення індексів.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх.

Шкала оцінювання: бальна і традиційна

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

13. Методичне забезпечення

1. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.

2. Дистанційний курс в системі дистанційного навчання Ментор, розташований за адресою: https://mentor.khai.edu/course/view.php?id=1636.

14. 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.

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.

15. 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.