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

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

ЗАТВЕРДЖУЮ

Голова НМК
_____ М.С. Зряхов
(підпис) (ініціали та прізвище)
«30» 08 2019 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"
(код та найменування спеціальності)

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

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2019 рік

Робоча програма Теоретичні основи криптології
(назва дисципліни)

для студентів за спеціальністю 125 "Кібербезпека"
освітньою програмою Безпека інформаційних і комунікаційних систем
освітньою програмою Кібербезпека індустріальних систем

«27» 08 2019 р., – 12 с.

Розробник: Лисенко І.В., доцент, к.т.н., доцент
(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 «29» 08 2019 р.

Завідувач кафедри д.т.н., професор (підпис) В. С. Харченко
(науковий ступінь та вчене звання) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</th><th>Характеристика навчальної дисципліни
(денна форма навчання)</th></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="10">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем, Кібербезпека індустріальних систем
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Цикл загальної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td>2019/ 2020</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 – 64*/120</td><td>3-й</td></tr>
<tr><td>Лекції 1)</td></tr>
<tr><td rowspan="6">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td>32 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>56 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *64/ 56.*

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: ознайомлення тих, хто навчається, з базовими поняттями, теоремамі і алгоритми елементарної теорії чисел і теорії алгебраїчних систем, що використовуються у сучасній прикладної криптології, а також – в придбанні навичок з виконання відповідних теоретико-числових та алгебраїчних розрахунків та перетворень.

Завдання:

- вивчити базові поняття елементарної теорії чисел і теорії алгебраїчних систем;
- вивчити основи теорії порівнянь і теорії квадратичних лишків;
- вивчити основи методи рішення порівнянь та систем порівнянь першого ступеню;
- вивчити основи теорії груп, кілець, полів;
- вивчити основи теорії еліптичних кривих.

Результати навчання: в результаті вивчення дисципліни студенти повинні бути здатними до виконання основних теоретико-числових та алгебраїчних перетворень.

Міждисциплінарні зв'язки: у частині вивчення основних понять елементарної теорії чисел дисципліна базується на деяких поняттях шкільної математики і сама є підґрунтям для вивчення дисципліни «Прикладна криптологія».

3. Програма навчальної дисципліни

Модуль 1

Змістовий 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

Змістовий 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

Змістовий 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

Змістовий 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.					
Змістовий модуль 1. Основні поняття елементарної теорії чисел і основи теорії порівнянь.					
1. Вступ до навчальної дисципліни	1	1	-		-
2. Базові поняття елементарної теорії чисел.	12	4	4		4
3. Основи теорії порівнянь.	8	4	4		-
4. Найважливіші функції і теореми елементарної теорії чисел.	5	2	3		-
Модульний контроль	1		1		
Разом за змістовим модулем 1	27	11	12		4
Змістовий модуль 2. Рішення систем порівнянь першого ступеню і основи теорії степінних лишків.					
5. Рішення порівнянь першого ступеню та систем порівнянь першого ступеню.	11	4	3		4
6. Основи теорії квадратичних лишків.	10	2	4		4
7. Основи теорії степінних лишків та індексів.	10	2	4		4
Модульний контроль	1		1		
Разом за змістовим модулем 2	32	8	12		12
Змістовий модуль 3. Основні поняття теорії алгебраїчних систем і теорії груп.					
8. Основні поняття теорії алгебраїчних систем.	2	2	-		
9. Основи теорії груп.	15	4	3		8
Модульний контроль	1		1		
Разом за змістовим модулем 3	18	6	4		8
Змістовий модуль 4. Основи теорії кілець, полів і еліптичних кривих.					
10. Основи теорії кілець.	12	2	-		10
11. Основи теорії полів.	12	2	-		10
12. Основи теорії еліптичних кривих.	12	3	3		6
Модульний контроль	1		1		
Разом за змістовим модулем 4	37	7	4		26
Модуль 2.					
Індивідуальне завдання	6				6
Усього годин	**120**	**32**	**32**		**56**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
1			
2			
	Разом		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Рішення задач на тему «Подільність з лишком, ознаки подільності».	4
2	Рішення задач на тему «Прості і складові числа, найбільший спільний дільник і найменше спільне кратне».	4
3	Рішення задач за темами «Властивості порівнянь», «Арифметичні застосування теорії порівнянь», «Функції і теореми теорії чисел».	4
4	Рішення порівнянь першого ступеню і систем порівнянь першого ступеню.	4
5	Рішення порівнянь другого ступеню. Обчислення символів Лежандра і Якобі.	4
6	Рішення задач за темою «Показники числа за заданим модулем, першообразні корені та індекси».	4
7	Рішення задач за темою «Основи теорії груп»	4
8	Розрахунок параметрів еліптичних кривих у простому та розширеному полях.	4
	Разом	**32**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
1			
2			
	Разом		

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Аксіома індукції. Аксіома Архімеда. Теореми, що стосуються натуральних чисел.	4
2	Застосування теорії ланцюгових дробів для вирішення порівнянь першого ступеня.	4
3	Порівняння другого ступеню за складовим модулем.	4
4	Першообразні корені та індекси за складовим модулем.	4
5	ЕК над простим кінцевим полем з перетвореннями в проєктивних координатах. ЕК над розширеним кінцевим полем з перетвореннями в проєктивних координатах.	6
6	Гомоморфізм та ізоморфізм груп. Ядро гомоморфізму та приклади гомоморфних відображень. Нормальні дільники групи. Фактор-група. Теорема про гомоморфні відображення. Автоморфізми груп.	8
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.	10
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.	10
9	Виконання розрахункової роботи	6
	Разом	**56**

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
Змістовий модуль 1			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	3...5	3	9...15
Модульний контроль	5…10	1	5…10
Змістовий модуль 2			
Робота на лекціях	0…1	3	0…3
Виконання і захист лабораторних (практичних) робіт	3...5	3	9...15
Модульний контроль	5…10	1	5…10
Змістовий модуль 3			
Робота на лекціях	0…1	3	0…3
Виконання і захист лабораторних (практичних) робіт	3...5	1	3...5
Модульний контроль	5…10	1	5…10
Змістовий модуль 4			
Робота на лекціях	0…1	4	0…3
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. Лысенко, И.В. Основы элементарной теории чисел [Текст] : учеб. пособие по практ. занятиям / И.В. Лысенко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк. авиац. ин-т», 2017. – 42 с.

2. Лысенко, И.В. Математика эллиптических кривых и криптография [Текст]: учеб. пособие / И.В. Лысенко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк. авиац. ин-т», 2016. – 52 с.

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

14. Рекомендована література

Базова

1. Бухштаб, А. А. Теория чисел [Текст] / А. А. Бухштаб. – М. : Просвещение, 1966. – 386 с.

2. Сушкевич, А. К. Теория чисел. Элементарный курс [Текст] / А. К. Сушкевич. – Х. : Изд-во Харьковского университета, 1956. – 204 с.

3. Курош, А. Г. Курс высшей алгебры [Текст] / А. Г. Курош. – 9-е изд. – М. : Наука, Гл. ред. физ.-мат. лит., 1968. – 431 с.

4. Александров, П. С. Введение в теорию групп [Текст] / П. С. Александров. – М. : Наука, Гл. ред. физ.-мат. лит., 1980. – 144 с.

5. Ершова, Т. И. Введение в теорию алгебраических систем [Текст] : учебно-методич. пособие / Н. И. Смирнова, И. Л. Хмельницкий. – Екатеринбург : Урал. гос. пед. ун-т, 2007. – 100 с.

Допоміжна

1. Оре, О. Приглашение в теорию чисел / Пер. с англ. Л.А.Савиной и А.П. Савина, М.: Наука. Гл. редакция физико-математической литературы, 1980. – 128 с. – (Библиотечка "Квант". Вып. 3).

2. Сизый, С. В. Лекции по теории чисел [Текст] : учеб. пособие для студентов вузов / С. В. Сизый. – 2-е изд., испр. – М. : ФИЗМАТЛИТ, 2008. – 192 с.

3. Каргаполов, М. И. Основы теории групп [Текст] / М. И. Каргаполов, Ю. И. Мерзляков. – 3-е изд., перераб. и доп. – М. : Наука, 1982. – 288 с.

4. Жданов, О. Н. Эллиптические кривые и их применение в криптографии [Текст] : учеб. пособие / О. Н. Жданов, В. А. Чалкин. – Красноярск : Сиб. гос. аэрокосмич. ун-т, 2011. – 105 с.

5. Ишмухаметов, И. Т. Методы факторизации натуральных чисел [Текст] : учеб. пособие / И. Т. Ишмухаметов. – Казань : Казан. ун-т, 2001. – 190 с.

6. Крэндалл, Р., Померанс, К. Простые числа. Криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс. – М. : УРСС, Книжный дом «Либроком», 2011. – 664 с.

15. Інформаційні ресурси

1. Вікіпедія – свободна енціклопедія [Електронний ресурс]. – Режим доступу: http://www. ru.wikipedia.org/.

2. Бібліотека видань з математики [Електронний ресурс]. – Режим доступу: http://www.math.ru/lib/cat/numbers.