

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
КАФЕДРА ДОСЛІДЖЕННЯ ОПЕРАЦІЙ

«ЗАТВЕРДЖУЮ»
Заступник декана з навчальної роботи
Олена КАШПУР
2021 року



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

АЛГЕБРАЇЧНІ СТРУКТУРИ, КРИПТОГРАФІЯ
ТА ЗАХИСТ ІНФОРМАЦІЇ

для студентів

галузі знань 12 – "Інформаційні технології"
спеціальність 122 – «Комп'ютерні науки»
освітній рівень бакалавр
освітня програма "Інформатика"
вид дисципліни обов'язкова

Форма навчання	денна
Навчальний рік	2022/2023
Семестр	5
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	іспит

Викладачі: доцент Маринич О.В., д.ф.м.н. (лекції, практичні заняття)

Пролонговано: на 20 /20 н.р. () « » 20 р.
на 20 /20 н.р. () « » 20 р.

КИЇВ – 2021

Розробник: **Олександр МАРИНИЧ**, д.ф.м.н., доцент кафедри дослідження операцій

Робочу програму дисципліни «Алгебраїчні структури, криптографія та захист інформації» затверджено на засіданні кафедри дослідження операцій

Мар

Завідувач кафедри «Дослідження операцій»

[підпис] Олександр ІКСАНОВ
(підпис)

« 27 » 04 2021 року

Протокол № 10 від « 27 » 04 2021 року

Схвалено гарантом освітньо-професійної програми першого (бакалаврського) рівня вищої освіти «Інформатика» *[підпис]* Людмила ОМЕЛЬЧУК

« 6 » травня 2021 року

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від « 6 » травня 2021 року № 10

Голова науково-методичної комісії *[підпис]* Людмила ОМЕЛЬЧУК
(підпис)

« 6 » травня 2021 року

1. Мета дисципліни: ознайомлення з базовими поняттями та методами теорії груп, кілець, полів та їх розширень, основами теорії чисел та теорії еліптичних кривих, а також застосування вказаного математичного апарату в криптографії та захисті інформації.

2. Попередні вимоги до опанування або вибору навчальної дисципліни

Для успішного опанування курсу «Алгебраїчні структури, криптографія та захист інформації» студент має вільно володіти матеріалом нормативного курсу «Алгебра та геометрія». Зокрема, вміти виконувати базові операції з матрицями та поліномами, знати основні поняття теорії лінійних просторів (лінійна залежність, базис, лінійний оператор) та теорії бінарних відношень (еквівалентність, частковий порядок, факторизація по відношенню еквівалентності). Також студент має *володіти елементарними навичками* програмування.

3. Анотація навчальної дисципліни: Метою навчальної дисципліни «Алгебраїчні структури, криптографія та захист інформації» є ознайомлення студентів з основними типами алгебраїчних структур (групи, кільця, поля та їх розширення) та основами теорії чисел, з метою їх подальшого застосування у криптографії та захисті інформації. Навчальна дисципліна «Алгебраїчні структури, криптографія та захист інформації» є базовою для вивчення дисципліни «Основи криптографії» та ін. Дисципліна є логічним продовженням курсу «Алгебра та геометрія». Навчальна дисципліна «Алгебраїчні структури, криптографія та захист інформації» є складовою освітньо-професійної програми підготовки фахівців за першим (бакалаврським) рівнем вищої освіти *галузі знань* 12 «Інформаційні технології» зі спеціальності 122 «Комп'ютерні науки», *освітньо-професійної програми* – «Інформатика». Дана дисципліна є обов'язковою за *програмою «Інформатика»*.

Викладається у 5 семестрі 3 курсу в **обсязі – 120 год.**

5 кредитів ECTS, зокрема: *лекції – 42 год., практичні заняття – 14 год., консультації – 2 год., самостійна робота – 62 год.*

У курсі передбачено **2 частини**. Завершується дисципліна – **іспитом в 5 семестрі**.

4. Завдання (навчальні цілі): набуття знань, умінь та навичок (компетенцій) на рівні новітніх досягнень у програмуванні, відповідно до освітньої кваліфікації «Бакалавр з комп'ютерних наук». Зокрема, розвивати:

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

5. Результати навчання за дисципліною:

Результат навчання (РН) (1. знати; 2. вміти; 3. комунікація [□] ; 4. автономність та відповідальність [□])	Результат навчання	Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код				
РН 1.1	Знати базові означення, факти, теореми та твердження теорії груп, кілець, полів	<i>Лекція, практичне заняття</i>	<i>Контрольна робота, 60% правильних відповідей, іспит</i>	20%
РН 1.2	Знати базові твердження теорії лишків, квадратичних лишків та теорії арифметичних функцій			
РН 1.3	Знати основні алгоритми факторизації, знаходження дискретного логарифма та	<i>Лекція, самостійна робота</i>		20%

	знаходження квадратичних лишків			
PH 1.4	Знати основні алгоритми криптографії з відкритим ключем			
PH 1.5	Знати означення та елементарні властивості еліптичних кривих			
PH 2.1	Вміти перевіряти, чи є задана структура групою, кільцем, полем	<i>Лекція, практичне заняття</i>	<i>Контрольна робота, 60% правильних відповідей, іспит</i>	30%
PH 2.2	Вміти знаходити розширення скінченного поля			
PH 2.3	Вміти розв'язувати порівняння першого порядку та їх системи			
PH 2.4	Вміти застосовувати символи Лежандра та Якобі для знаходження квадратичних лишків			
PH 2.5	Вміти програмувати основні криптографічні алгоритми	<i>Лекція, самостійна робота</i>	<i>Захист лабораторної роботи</i>	30%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни Програмні результати навчання	PH 1.1	PH 1.2	PH 1.3	PH 1.4	PH 1.5	PH 2.1	PH 2.2	PH 2.3	PH 2.4	PH 2.5
<i>(з опису освітньої програми)</i>										
ПРН16. Демонструвати знання концепції інформаційної безпеки, принципів безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	+	+	+	+	+	+	+	+	+	+

7. Схеми формування оцінки.

7.1 Форми оцінювання студентів:

- **семестрове оцінювання:**

1. Контрольна робота 1: PH 1.1, PH 1.2 – 15 балів / 9 балів
2. Контрольна робота 2: PH 2.1, PH 2.2, PH 2.3, PH 2.4 – 15 балів / 9 балів
3. Лабораторна робота: PH 1.3, PH 1.4, PH 1.5, PH 2.5 – 30 балів / 18 балів

- **підсумкове оцінювання (у формі іспиту):**

максимальна кількість балів, які можуть бути отримані студентом: 40 балів

результати навчання, які будуть оцінюватись: PH 1.1, PH 1.2, PH 1.3, PH 1.4, PH 1.5, PH 2.1, PH 2.2, PH 2.3, PH 2.4

форма проведення: письмова робота.

види завдань: 2 теоретичних запитання, 2 задачі.

Критерії оцінювання на іспиті

Завдання	Тема завдання	Максимальний відсоток від 40 балів	Всього відсотків
Завдання 1	Письмове запитання з теорії алгебраїчних структур або теорії чисел	20%	20%
Завдання 2	Письмове запитання з криптографії	20%	20%

Завдання 3	Задача з теорії алгебраїчних структур або теорії чисел	30%	30%
Завдання 4	Задача з криптографії	30%	30%
			100%

Запитання для підготовки до іспиту

- 1) Означення групи. Приклади груп.
- 2) Означення підгрупи. Клас суміжності за підгрупою. Теорема Лагранжа та її наслідки.
- 3) Поняття нормальної підгрупи. Фактор-група за нормальною підгрупою: коректність означення добутку суміжних класів
- 4) Групи малих порядків. Найменша неабелева група.
- 5) Поняття гомоморфізму та ізоморфізму. Перша та друга теореми про гомоморфізм.
- 6) Класифікація скінченнопороджених абелевих груп.
- 7) Кільце многочленів над полем. Поняття ідеалу кільця многочленів однієї змінної. Опис ідеалів кільця многочленів однієї змінної.
- 8) Фактор-кільце кільця многочленів однієї змінної за ідеалом.
- 9) Означення поля. Приклади полів.
- 10) Поняття простого алгебраїчного розширення поля. Конструкція простого алгебраїчного розширення.
- 11) Поле розкладу многочлена. Існування та єдиність поля розкладу, з точністю до ізоморфізму.
- 12) Арифметичні операції в кільці лишків.
- 13) Китайська теорема про лишки.
- 14) Функція Ейлера та її властивості.
- 15) Функція Мьобіуса та формула обертання.
- 16) Квадратичні лишки. Символи Якобі та Лежандра.
- 17) Тести на простоту: тести Пратта, Соловея-Штрассена, Міллера-Рабіна.
- 18) Алгоритми факторизації Полларда та квадрат-решітки.
- 19) Поняття хеш-функції та алгоритм хешування MASH-1, SHA1.
- 20) Дискретний логарифм. Алгоритми обчислення дискретних логарифмів.
- 21) Найпростіші алгоритми шифрування: шифр підстановкою, шифр Вернама.
- 22) Криптосистема RSA.
- 23) Криптосистема Ель-Гамала над полем $GF(p)$ та $GF(p^m)$.
- 24) Криптографічна система Рабіна.
- 25) Криптографія над еліптичними кривими.

7.2. Організація оцінювання:

• Терміни проведення оцінювання:

Модульна контрольна робота 1 – до 7 тижня семестру

Модульна контрольна робота 2 – до 14 тижня семестру

Лабораторна робота – до 14 тижня семестру

Якщо студент з поважних причин, які підтверджено документально, був відсутній при написанні модульної контрольної роботи, він має право на одне перескладання з можливістю отримання максимальної кількості балів. Термін перескладання визначається викладачем.

У разі неякісного виконання лабораторної роботи, викладач має право не зарахувати лабораторну роботу, або знизити за неї бали.

Студент має право здавати лабораторні роботи після закінчення визначеного для них терміну, але з втратою одного балу за кожний тиждень, який пройшов з моменту закінчення терміну її здачі.

Якщо впродовж семестру студент не з'являвся на заняття (не залежно від причин), не має модульних оцінок, у відповідних графах „Відомості обліку успішності КМСОНП” виставляються „0”, а у графі іспиту – відмітка про недопуск.

Студент допускається до складання іспиту, якщо кількість набраних ним балів за семестр становить не менше 20 балів.

Іспит вважається не зданим, якщо сумарна кількість балів з дисципліни складає менше 60 балів

7.3. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

8. Структура навчальної дисципліни. Тематичний план занять

№ п/п	Номер і назва теми	Кількість годин		
		лекції	Практичні заняття	Самостійна робота
Частина 1. Алгебраїчні структури та основи теорії чисел				
1	Тема 1. Означення групи, приклади груп. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2	1	2
2	Тема 2. Підгрупа, нормальна підгрупа, фактор-група. Теорема Ферма. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2		2
3	Тема 3. Поняття ізоморфізму, гомоморфізму. Теорема про ізоморфізм. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2	1	2
4	Тема 4. Ряди груп. Теорема Шраєра. <i>Самостійна робота: Опрацювання лекційного матеріалу. Теорема Жордана-Гьолдера.</i>	2		2
5	Тема 5. Кільця та області цілісності. <i>Самостійна робота: Опрацювання лекційного матеріалу. Теорема Ейлера.</i>	2	1	2
6	Тема 6. Поля. <i>Самостійна робота: Опрацювання лекційного матеріалу.. Виконання лабораторної роботи 1.</i>	2		2
7	Тема 7. Алгебраїчні розширення полів. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>			2
8	Тема 8. Основні арифметичні функції. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2	1	2
9	Тема 9. Функції Ейлера та Мьобіуса. Формула обернення. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2		2
10	Тема 10. Порівняння та їх системи. Китайська теорема про лишки. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2	1	2
11	Тема 11. Порівняння другого степеня. Символи Лежандра та Якобі. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 1</i>	2		2
	Контрольна робота 1		1	
Частина 2. Основні алгоритми криптографії, криптосистеми з відкритим ключем, криптографія над еліптичними кривими				

1 2	Тема 12. Базові поняття криптографії. Криптографічні системи з відкритим та симетричним ключем. <i>Самостійна робота: Опрацювання лекційного матеріалу. Шифрування підстановками. Виконання лабораторної роботи 2.</i>	2		3
1 3	Тема 13. Протокол Діффі-Гелмана та проблема дискретного логарифма. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>	2	1	3
1 4	Тема 14. Алгоритми знаходження дискретного логарифма: ро-алгоритм Полларда, алгоритм «великий крок-малий крок». <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>	2		3
1 5	Тема 15. Криптосистема RSA та проблема факторизації. <i>Самостійна робота: Опрацювання лекційного матеріалу. Алгоритм решета числового поля для факторизації. Виконання лабораторної роботи 2.</i>	2		3
1 6	Тема 16. Алгоритми факторизації: ро-алгоритм Полларда, метод Ферма, алгоритм квадратичного решета. <i>Самостійна робота: Опрацювання лекційного матеріалу. Алгоритм решета числового поля для факторизації. Виконання лабораторної роботи 2.</i>	2	2	4
1 7	Тема 17. Криптосистема Ель-Гамала. <i>Самостійна робота: Опрацювання лекційного матеріалу. Алгоритм решета числового поля для факторизації.. Виконання лабораторної роботи 2.</i>	2		3
1 8	Тема 18. Криптосистема Рабіна для проблема квадратичного лишка. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>	2	1	4
1 9	Тема 19. Тест чисел на простоту. Тест Соловея-Штрассена та Міллера-Рабіна. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>	2		4
2 0	Тема 20. Проективна площина та однорідні координати. Алгебраїчні криві у проективній площині. <i>Самостійна робота: Опрацювання лекційного матеріалу. Застосування однорідних координат в комп'ютерній графіці. Виконання лабораторної роботи 2.</i>	2		3
2 1	Тема 21. Еліптичні криві над полем дійсних чисел. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>	2	1	3
2 2	Тема 22. Еліптичні криві над скінченними полями. <i>Самостійна робота: Опрацювання лекційного матеріалу. Виконання лабораторної роботи 2.</i>			3
2 3	Тема 23. Криптографія над еліптичними кривими. Криптосистема Ель-Гамала над еліптичною кривою. <i>Самостійна робота: Опрацювання лекційного матеріалу. Алгоритм факторизації Ленстри. Виконання лабораторної роботи 2.</i>	2		4
	Контрольна робота 2		1	
	Контроль за підсумками лабораторної роботи		2	

Загальний обсяг – 120 год., в тому числі:

Лекцій - **42 год.**

Практичні заняття - **14 год.**

Самостійна робота - **62 год.**

Умова лабораторної роботи:

Лабораторна робота. Довга арифметика з імплементацією основних теоретико-числових функцій: розв'язування порівнянь та їх систем, обчислення функцій Ейлера та Мьобіуса, символів Лежандра та Якобі. Реалізація основних криптосистем та алгоритмів з використанням довгої арифметики.

Умови можна знайти на веб-сторінці кафедри:

<http://do.unicyb.kiev.ua/index.php/uk/2015-01-22-11-29-43/239-2017-08-21-11-28-43>

9. Рекомендовані джерела:

Основні:

1. *Apostol T.* Introduction to Analytic Number Theory. Springer-Verlag, 1976.
2. *Fraleigh J.* A First Course in Abstract Algebra, 7th ed. Addison-Wesley Publishing, 2003.
3. *Авдошин С.М., Набєбин А.А.* Дискретная математика: модулярная алгебра, криптография, кодирование. М.: ДМК Пресс, 2017.
4. *Клесов О.І.* Елементарна теорія чисел та елементи криптографії. К.: ТВіМС, 2016.
5. *Кострикин А.И.* Сборник задач по алгебре, М: Физматлит 2001.

Додаткові:

1. *Ахо Альфред В., Хопкрофт Джон, Ульман Джеффри Д.* Структуры данных и алгоритмы: Уч.пос. – СПб.: Издательский дом «Вильямс», 2010.
2. *Кнут Д.* Искусство программирования: В 3 т.– М.: Мир; Том 1, 1976; Том 3, 1978.
3. *Кострикин А.И.* Введение в алгебру, М: Физматлит, 2000.
4. *Вельшенбах М.* Криптография на С и С++ в действии. М.: Триумф, 2003.

Інтернет-ресурси:

1. *Goldwasser S., Bellare M.* Lecture Notes on Cryptography. <https://cseweb.ucsd.edu/~mihir/papers/gb.pdf>
2. *Маринич О.В.* Алгебраїчні структури, криптографія та захист інформації: Електронний навчальний посібник.
<http://do.unicyb.kiev.ua/marinych/wpcontent/uploads/2020/09/AlgStructCrypto.pdf>