КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ

Кафедра інтелектуальних програмних систем

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«____»_____2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗАГАЛЬНА АЛГЕБРА

для студентів

галузь знань **12 «Інформаційні технології»**
(шифр і назва)

спеціальність **121 «Інженерія програмного забезпечення»**
(шифр і назва спеціальності)

освітній рівень **бакалавр**
(молодший бакалавр, бакалавр, магістр)

освітня програма **«Програмна інженерія»**
(назва освітньої програми)

вид дисципліни обов'язкова

Форма навчання	**денна**
Навчальний рік	**2020/2021**
Семестр	**4**
Кількість кредитів ECTS	**5**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладач: **к.ф.-м.н. Ліндер Я.М.** (лекції, лабораторні заняття)

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2019

Розробник: Ліндер Ярослав Миколайович, асистент кафедри інтелектуальних програмних систем

ЗАТВЕРДЖЕНО
Завідувач кафедри інтелектуальних програмних систем _____
(Провотар О.І.)
(підпис) (прізвище та ініціали)

Протокол № __від «___»_____ 2019 р.

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

Протокол від «___» _____ 2019 року №___

Голова науково-методичної комісії _____ (Омельчук Л.Л.)
(підпис) (прізвище та ініціали)

«_____» _____ 20___ року

1. Мета дисципліни

Формування у студентів основ знань, необхідних для розуміння груп, кілець та полів, а також проведення їх аналізу; практичне використання набутих знань для побудови алгоритмів, які базуються на теорії груп, кілець та полів. До таких алгоритмів відносяться алгоритми модульної арифметики та чисельні алгоритми в групах, зокрема алгоритми обчислення дискретного логарифма, алгоритми криптографії на основі еліптичних кривих тощо.

2. Попередні вимоги до опанування або вибору навчальної дисципліни (за наявності):

Знати для вивчення курсу „Загальна алгебра" основи дискретної математики, які вивчаються на молодших курсах та основні поняття загальної алгебри.

Вміти досліджувати властивості скінченних груп, кілець та полів, обчислювати групові операції над елементами групи, проводити розширення скінченних груп, створювати та виконувати аналіз криптографічних систем, що базуються на властивостях груп лишків за модулем простого числа та груп на основі еліптичних кривих.

3. Анотація навчальної дисципліни

Навчальна дисципліна „Загальна алгебра" є складовою освітньо-професійної програми підготовки фахівців за першим (*бакалаврським*) рівнем вищої освіти *галузі знань* 12 „Інформаційні технології" зі *спеціальності 121* „Інженерія програмного забезпечення", *освітньо-професійної програми* „Програмна інженерія".

Дана дисципліна є обов'язковою навчальною дисципліною за ***програмою "Програмна інженерія"***. Викладається у **4** семестрі **2** курсу в **обсязі – 150 год.** ***(5 кредитів ECTS)*** зокрема: *лекції – 40 год., практичні – 20 год., консультації – 2 год., самостійна робота – 88 год.* У курсі передбачено **2** *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна – **іспитом в 4 семестрі.**

В результаті вивчення навчальної дисципліни студент повинен:

знати базові означення, факти, теореми та твердження теорії груп, кілець, полів; означення та елементарні властивості еліптичних кривих; основні алгоритми, які базуються на застосуванні теорії груп до задач криптографії, теорії складності та теорії чисел.

вміти проводити аналіз скінченних груп (пошук обернених елементів, знаходження порядку елемента групи), знаходити розширення груп, максимальних підгруп; застосовувати основні алгоритми до задач обчислення дискретного логарифма, криптографії на основі еліптичних кривих тощо.

Нормативна навчальна дисципліна „Загальна алгебра" є складовою циклу професійної підготовки фахівців освітньо-кваліфікаційного рівня „бакалавр". Для допуску до дисципліни „ Загальна алгебра " освітньо-професійної програми «Програмна інженерія» студент повинен опанувати компетентності та результати навчання, які надає дисципліна „Дискретна математика". Навчальна дисципліна „Загальна алгебра" є базовою для вивчення таких спеціальних дисциплін як "Математичні основи захисту інформації" та "Основи криптології".

4. Завдання (навчальні цілі):

Набуття знань, умінь та навичок (компетентностей) на рівні математичних основ загальної алгебри, відповідно до кваліфікації фахівець з інформаційних технологій. Зокрема, розвивати:

- здатність до абстрактного мислення, аналізу та синтезу (ЗК01);
- здатність застосовувати знання у практичних ситуаціях (ЗК02).
- здатність спілкуватися державною мовою як усно, так і письмово (ЗК03);
- здатність вчитися і оволодівати сучасними знаннями (ЗК05);
- здатність до пошуку, оброблення та аналізу інформації з різних джерел (ЗК06).
- здатність до алгоритмічного та логічного мислення (СК-14).

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		**Форми (та/або методи і технології) викладання і навчання**	**Методи оцінювання та пороговий критерій оцінювання (за необхідності)**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН1.1	*Знати базові означення, факти, теореми та твердження теорії груп, кілець, полів*	*Лекція, практичне заняття*	*Тест, 60% правильних відповідей, іспит*	15%
РН1.2	*Знати означення та елементарні властивості еліптичних кривих*	*Лекція, практичне заняття*	*Тест, 60% правильних відповідей, іспит*	20%
РН1.3	*Знати основні алгоритми, які базуються на застосуванні теорії груп до задач криптографії, теорії складності та теорії чисел.*	*Лекція, практичне заняття*	*Тест, 60% правильних відповідей, іспит*	15%
РН2.1	*Вміти проводити аналіз скінченних груп, знаходити розширення груп, максимальних підгруп тощо.*	*Практичне заняття, самостійна робота*	*Захист лабораторної роботи, іспит*	24%
РН3.1	*Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань проектування та розробки програм, складати письмові звіти*	*Практичне заняття*	*Поточне оцінювання, захист ЛР*	10%
РН4.1	*Організовувати свою самостійну роботу для досягнення результату*	*Самостійна робота*	*Поточне оцінювання, Захист лабораторної роботи*	8%
РН4.2	*Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість*	*Лабораторна робота*	*Захист лабораторної роботи*	8%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 2.1**	**РН 3.1**	**РН 4.1**	**РН 4.2**
(з опису освітньої програми)							
ПРН01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних	+	+	+	+	+	+	+

завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.							

7. Схема формування оцінки.

7.1. Форми оцінювання студентів:

- семестрове оцінювання:

1. Контрольна робота 1: РН 1.1, РН 1.2 — 20 балів/12 балів.

2. Контрольна робота 2: РН 1.2, РН1.3 — 20 балів/12 балів.

3. Лабораторна робота 1 (проект): РН 1.2, РН1.3– 10 балів/6 балів.

4. Лабораторна робота 2 (проект): РН1.2, РН1.3 – 10 балів/6 балів.

- підсумкове оцінювання (у формі іспиту):

- *максимальна кількість балів які можуть бути отримані студентом: 40 балів;*
- *результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3;*
- *форма проведення і види завдань: письмова.*

Види завдань: 5 письмових завдань.

Критерії оцінювання на іспиті

Завдання	**Тема завдання**	**Максимальний відсоток від 40 балів**	**Всього відсотків**
Завдання 1-5	Задачі на аналіз та дослідження груп, кілець та полів	По 20%	100%
			100%

Запитання для підготовки до іспиту

1) Означення групи. Властивості бінарної операції, що задає групу
2) Графічне та табличне представлення групи. Граф циклів та таблиця Келі
3) Групи малих порядків. Найменша неабелева група.
4) Порядок елемента групи.
5) Система твірних елементів групи. Циклічні групи.
6) Означення підгрупи. Клас суміжності за підгрупою. Теорема Лагранжа та її наслідки.
7) Теорема Силова. Побудова Силовських підгруп
8) Поняття гомоморфізму та ізоморфізму. Перша та друга теореми про гомоморфізм.
9) Класифікація скінченнопороджених абелевих груп.
10) Кільце многочленів над полем. Поняття ідеалу кільця многочленів однієї змінної. Опис ідеалів кільця многочленів однієї змінної.
11) Фактор-кільце кільця многочленів однієї змінної за ідеалом.
12) Означення поля. Приклади полів.
13) Поняття простого алгебраїчного розширення поля. Конструкція простого алгебраїчного розширення.
14) Поле розкладу многочлена. Існування та єдиність поля розкладу, з точністю до ізоморфізму.
15) Арифметичні операції в кільці лишків.
16) Китайська теорема про лишки.
17) Функція Ейлера та її властивості.
18) Функція Мьобіуса та формула обертання.
19) Квадратичні лишки. Символи Якобі та Лежандра.

20) Тести на простоту: тести Пратта, Соловея-Штрассена, Міллера-Рабіна.
21) Алгоритми факторизації Полларда та квадрат-решітки.
22) Поняття хеш-функції та алгоритм хешування MASH-1, SHA1.
23) Дискретний логарифм. Алгоритми обчислення дискретних логарифмів.
24) Найпростіші алгоритми шифрування: шифр підстановкою, шифр Вернама.
25) Криптосистема RSA.
26) Криптосистема Ель-Гамаля над полем GF(p) та GF(p^m).
27) Криптографічна система Рабіна.
28) Криптографія над еліптичними кривими.

7. 2. Організація оцінювання:

Терміни проведення форм оцінювання:

1. Контрольна робота : до 7 тижня семестру.
2. Контрольна робота : до 15 тижня семестру.
3. Лабораторна робота 1 (проект): до 7 тижня семестру.
4. Лабораторна робота 2 (проект): до 15 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.

Якщо впродовж семестру студент пропустив більше половини занять без поважних причин, не має оцінок за модульні контрольні роботи, у відповідних графах „Відомості обліку успішності КМСОНП" виставляються „0", а у графі заліку – відмітка про недопуск.

Студент допускається до складання заліку, якщо кількість набраних ним балів за семестр становить не менше 30 балів. Студент не допускається до іспиту, якщо під час семестру набрав менше ніж 24 балів. Студент допускається до іспиту за умови виконання 70% передбачених планом лабораторних робіт.

7.3 Шкала відповідності оцінок

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

8. Структура навчальної дисципліни. Тематичний план лекцій і лабораторних занять

№ Лекції	Назва лекції	Лекції	Практичні заняття	Самост. робота
ЧАСТИНА 1				
1	Предмет загальної алгебри. Бінарна операція. Напівгрупа. Група. Таблиця Келі групи.	2	2	4
2	Групи підстановок та їх властивості. Група симетрій	2	2	4
3	Циклічні групи. Система твірних елементів групи. Основні властивості таких груп.	2	2	4
4	Теореми Силова. Силовські підгрупи. Морфізми груп	2	2	4
5	Класи суміжності. Теорема Лагранжа та її наслідки.	2	2	4
Контрольна робота 1				
ЧАСТИНА 2				
6	Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення. Поле, характеристика поля та побудова скінченних полів.	2	2	5
7	Дільники нуля, дільники одиниці, оборотні та нільпотентні елементи. Знаходження обернених елементів у полі.	2	2	5
8	Алгебраїчні розширення полів. Числення над полем многочленів у розширеннях скінченних полів.	2	2	5
10	Кругові многочлени. Побудова незвідних многочленів заданого ступеня над скінченним полем.	2	2	5
11	Алгоритми розкладу многочлена над скінченним полем. Аналіз кількості коренів многочлена, та алгоритми їх знаходження.	2	2	5
Контрольна робота 2				
ЧАСТИНА 3				
1	Базові поняття криптографії. Криптографічні системи з відкритим та симетричним ключем.	2		4
2	Криптосистема RSA та проблема факторизації.	2		4
3	Криптосистема Ель-Гамаля. Алгоритми знаходження дискретного логарифма: ро-алгоритм Полларда, алгоритм «великий крок-малий крок».	2		4
4	Еліптичні криві над полем дійсних чисел.	2		4
5	Еліптичні криві над скінченними полями. Криптографія над еліптичними кривими.	2		4
ЧАСТИНА 4				
6	Однопараметричні групи перетворень. Рівняння Лі	2		4
7	Диференціальні інваріанти групи перетворень. Інфінітиземальний оператор групи.	2		4
8	Продовження оператору	2		5
9	Пошук групи, що допускається заданим диференціальним рівнянням.	2		5
10	Інтегрування диференціальних рівнянь та систем диференціальних рівнянь за допомогою диференціальних інваріантів	2		5
ВСЬОГО		**40**	**20**	**88**

Загальний обсяг 150 годин, в тому числі:

лекцій – 40 год., практичних занять – 20 год., самостійної роботи – 88 год., консультацій – 2 год.

9. Рекомендовані джерела

Основні:

1. *Apostol T.* Introduction to Analytic Number Theory. Springer-Verlag, 1976.
2. *Fraleigh J.* A First Course in Abstract Algebra, 3rd ed. Addison-Wesley Publishing, 1982.
3. Fulton W. Algebraic Curves, 3rd ed. Addison-Wesley Publishing Company, 2008.
4. Gilbert W.J., Nicholson W.K. Modern algebra with applications, 2ed., Wiley, 2004 347 с.
5. Washington L. C. Elliptic Curves: Number Theory and Cryptography, Second Edition (Discrete Mathematics and Its Applications) 2nd Edition, 2008, 531 с.
6. *Авдошин С.М., Набебин А.А.* Дискретная математика: модулярная алгебра, криптография, кодирование. М.: ДМК Пресс, 2017.
7. Ван дер Варден Б.Л. Алгебра. – М.: Наука, 1976.
8. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: МЦНМО. - 2003.- 328 с.
9. Головин С.В., Чесноков А.А. Групповой анализ дифференциальных уравнений, Новосибирск, 2009, 119 с.
10. Завало С.Т., Костарчук В.Н., Хацет Б.І . Алгебра і теорія чисел. В 2–х ч. –К.: Вища шк., 1974, 1977, 1980
11. Ибрагимов Н. Х. Азбука группового анализа, М.: «Знание», №8, 1989, 44 с.
12. Ибрагимов Н. Х. Опыт группового анализа, М.: «Знание», №7, 1991, 43 с.
13. *Кострикин А.И.* Сборник задач по алгебре, М: Физматлит 2001.
14. Курош А.Г. Лекции по общей алгебре. Издание 2-е, М.: Изд-во "Наука". 1973. - 400с.
15. Лидл Р., Нидеррайдер Г. Конечные поля: в 2-х т. Т. 1, М.:Мир, 1988. – 430 с.
16. Овсянников Л.В. Групповой анализ дифференциальных уравнений, М.: Наука, 1978, 339 с.
17. Олвер П. Приложения групп Ли к дифференциальным уравнениям. М.: Мир, 1989, 628 с.
18. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. М.: Наука, 1977.
19. Шапуков Б.Н. Задачи по группам Ли и их приложениям. М. НИЦ «Регулярная и хаотическая динамика», 2002, 256 с.

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.
5. Проскуряков И.В. Сборник задач по линейной алгебре. – М.: Наука, 1965.