КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____О.М.Харитонов
«___» серпня 20__ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Алгебраїчна криптографія

для студентів

галузь знань	**11 «Математика та статистика»**
спеціальність	**112 «Статистика»**
освітній рівень	**перший (бакалавр)**
освітня програма	**«Статистика»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2020/2021**
Семестр	6
Кількість кредитів ECTS	3
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: Петравчук Анатолій Петрович, д.ф.-м.н., професор, завідувач кафедри алгебри і комп'ютерної математики

Пролонговано: на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)
на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)

КИЇВ – 2020

Розробник Петравчук А.П., д. ф.-м. н., професор, завідувач кафедри алгебри і комп'ютерної математики

ЗАТВЕДЖЕНО
Зав. кафедри алгебри і комп'ютерної математики
_____ Петравчук А.П.
(підпис)

Протокол № 1 від 11. 08. 2020 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "31" 08 2020 року № 1

Голова науково-методичної комісії _____професор, д.ф.-м.н. Олійник А.С.
(підпис)

1. Мета дисципліни – оволодіння сучасними методами, теоретичними положеннями та основними застосуваннями теорії кілець, теорії модулів над комутативними кільцями, теорії полів в різних задачах криптографії, а також ознайомлення із застосуваннями в теорії лінійних кодів, зокрема циклічних кодів

2. Попередні вимоги до опанування або вибору навчальної дисципліни
1. *Знати* основні поняття, факти і теореми лінійної алгебри, алгебри і теорії чисел, дискретної математики, теорії алгебраїчних структур, теорії ймовірностей, основні навички з програмування
2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Алгебраїчна криптографія».
3. *Володіти елементарними навичками* роботи з множинами, функціями, знаходити ймовірності подій, знати лінійну алгебру, основні поняття із теорії чисел, знати основні поняття із теорії кілець і теорії полів

3. Анотація навчальної дисципліни. В курсі «Алгебраїчна криптографія» висвітлюються базові відомості, поняття, факти теорії комутативних кілець, теорії модулів над такими кільцями, теорії скінченних полів. Зокрема розглядаються нетерові кільця і модулі над ними, елементи тензорної алгебри, тензорні добутки модулів, скінченні поля, основні результати про незвідні многочлени над скінченними полями, застосування теорії кілець і теорії полів в криптографії (еліптична криптографія, RSA)

Викладається у 2 семестрі 3 курсу в обсязі **90 год**. *(3* ***кредити ECTS***[1]*)* зокрема: *лекції – всього 26 год., практичні заняття 16, консультації 2 год., самостійна робота – 46 год.* У курсі передбачено 2 *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна **заліком** у другому семестрі 3-го курсу.

4. Завдання (навчальні цілі):

формування здатності розв'язувати складні задачі та практичні проблеми у математиці або у процесі навчання, що передбачає застосування теорій та методів математики, статистики й комп'ютерних технологій і характеризується комплексністю та невизначеністю умов; набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у математиці, відповідно до освітнього рівня «Бакалавр». Зокрема, професійне оволодіння компетентностями:
1) Здатність до абстрактного мислення, аналізу та синтезу;
2) Здатність застосовувати знання у практичних ситуаціях;
3) Знання й розуміння предметної області та професійної діяльності;
4) Здатність спілкуватися українською мовою як усно, так і письмово (ЗК-6).
5) Здатність вчитися і оволодівати сучасними знаннями;
6) Здатність до пошуку, обробки та аналізу інформації з різних джерел;
7) Здатність приймати обґрунтовані рішення;
8) Здатність працювати автономно;
9) Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків;
10) Здатність оцінювати та забезпечувати якість виконуваних робіт;
11) Здатність діяти на основі етичних міркувань (мотивів);
12) Здатність здійснювати логічні математичні міркування із чітким зазначенням припущень та висновків;
13) Здатність до математичного формулювання задач та вибору методів їх розв'язання;

[1] кредитів ECTS – кредит кратний 30 годинам.

14) Здатність до кількісно-статистичного мислення;
15) Здатність робити якісні висновки з кількісних даних;
16) Здатність проводити дослідження ймовірнісно-статистичних моделей та інтерпретувати одержані результати;
17) Здатність подавати статистичні процедури та результати їхнього застосування у формі, придатній для цільової аудиторії, до якої звертаються, як усно, так і письмово;
18) Здатність до аналізу основ і властивостей статистичних алгоритмів та розуміння переваг тих чи інших підходів, у тому числі до оцінки їх обґрунтованості й ефективності.

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**			
1.1	Знати: поняття ідеалу, фактор-кільця ніль-радикалу, радикалу Джекобсона . Модулі, операції над ними, точні послідовності, тензорні добутки модулів, тензорна алгебра векторного простору.	лекція, самостійне опрацювання	опитування під час лекції, модульна контрольна №1	10%
1.2	Знати: основні поняття кільця часток, локалізацію, та їїх застосувань в алгебраїчній геометрії. Нетерові кільця і модулі, теорема Гільберта про базис, примарний розклад нетерових кілець	лекція, самостійне опрацювання	опитування під час лекції, модульна контрольна №1	10%
1.3	Знати: характеризацію скінченних полів. Корені незвідних многочленів над скінченним полем. Функція Мьобіуса та кількість незвідних многочленів. Застосування скінченних полів в криптографії .	лекція самостійне опрацювання	опитування під час лекцій, модульна контрольна №2	10%
1.4	Автоморфізми та спряжені елементи. Сліди, норми та базиси. Лінійні та циклічні коди. Застосування до криптографії. Скінченні геометрії. Застосування до комбінаторики.	лекція, самостійне опрацювання	опитування під час лекцій, модульна контрольна №2	5%
2.1	Уміти знаходити ніль-радикал комутативного кільця, будувати кільце часток, обчислювати тензорні добутки, будувати локальні кільця. Задача дискретного логарифму в скінченних кільцях.	самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	15%
2.2	Уміти проводити обчислення в скінченних кільцях, застосовувати скінченні	самостійне опрацювання	перевірка індивідуальних завдань, самостійна	20%

	кільця при використанні циклічних кодів		аудиторна робота, модульна контрольна робота	
2.3	Уміти виконувати дії в скінченних полях, вміти будувати поле з заданою кількістю елементів, перевіряти, чи є множина (нормальним) базисом. Уміти з точками еліптичних кривих, дискретний логарифм для еліптичних кривих	самостійне опрацювання	перевірка індивідуальних завдань, самостійна робота, модульна контрольна робота	15%
2.4	Уміти: знаходити автоморфізми скінченного поля, застосовувати теорію скінченних полів в теорії кодування	самостійне опрацювання	перевірка індивідуальних завдань, самостійна робота	10%
3.1	Здатність обґрунтовувати власний погляд на задачу та формулювати робочі гіпотези, спілкуватися з колегами з питань застосування математичних методів та теорій	Лекція, самостійна робота	активна робота на лекції, усні відповіді	2.5%
3.2	Вироблення навиків командної роботи	Лекція, самостійна робота	активна робота на лекції, усні відповіді	2.5%

6. Співвідношення результатів навчання дисципліни з програмними результатами

Результати навчання дисципліни **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 1.4**	**РН 2.1**	**РН 2.2**	**РН 2.3**	**РН 2.4**	**РН 3.1**	**РН 3.2**
(*з опису освітньої програми*)										
РН-1 - Здійснювати професійну письмову й усну комунікацію українською мовою та, принаймні, однією з іноземних мов	+	+	+	+	+	+	+	+	+	+
РН-5 - Володіти базовими знаннями та вміннями з фундаментальних розділів математики: математичного аналізу, алгебри, аналітичної геометрії, диференціальних рівнянь, у тому числі в частинних похідних	+	+	+	+	+	+	+	+	+	+
РН-18 Вміти застосовувати ймовірнісно-статистичні моделі та методи для розв'язання прикладних проблем і задач			+		+		+			

7. Схема формування оцінки.

7.1. Форми оцінювання студентів:

- оцінювання впродовж навчального періоду:

1. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2, РН2.3, РН2.4 – 8 балів/4 бали

2. Модульна контрольна робота 1: РН1.1, РН1.2, РН2.1, РН2.2 – 20 балів/12 балів;

3. Модульна контрольна робота 2: РН1.3, РН1.4 РН2.3 –20 балів/12 балів;

4. Розв'язання задач на практичних заняттях: РН2.1, РН2.2, РН2.3, РН2.4, РН3.1, РН3.2, – 12 балів/7 бали;

Разом 60/35

- підсумкове оцінювання: залік.

- максимальна кількість балів, які можуть бути отримані: 40 балів;

- - результати навчання, які будуть оцінюватись:

Вміння формулювати і доводити основні теореми із викладеної в курсі теорії кілець, вміння знаходити ніль-радикал кільця, тензорні добутки модулів, розвязувати задачі про основні властивості нетерових кілець, здійснювати основні операції в скінченних кільцях, знаходити кількість незвідних многочленів над скінченними полями, знаходити норму і слід елемента поля, застосовувати отримані знання для кодування інформаційних векторів за допомогою циклічних кодів, застосовувати еліптичні криві в криптографії

РН2.2, РН2.3, РН2.4;

- форма проведення і види завдань: письмова робота.

7.2. Організація оцінювання:

Самостійна робота передбачає активну самостійну роботу по розвязанню задач і по формулюванню основних теоретичних положень під час практичних занять, при цьому кожен студент отримує індивідуальне завдання, яке він повинен виконати за невеликий проміжок часу (складність завдання пропорційно відведеному часу)

Критично-розрахунковий мінімум балів за навчання впродовж семестру становить **20** балів, рекомендований мінімум, розрахований з урахуванням специфіки дисципліни становить **35** балів. Студенти, які протягом семестру набрали сумарно меншу кількість балів ніж рекомендований мінімум **35** балів для підвищення балів отримують можливість написати додаткову контрольну роботу та доскласти домашні завдання. Мінімальна кількість балів, які додаються до семестрових – 20 балів, тобто, якщо оцінка студента на заліку є нижчою від мінімального порогового рівня (20 балів), то бали за залік не додаються до семестрової оцінки;

У випадку відсутності студента з поважних причин відпрацювання та перездачі форм контролю здійснюються у відповідності до „Положення про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка" (2018), http://www.univ.kiev.ua/pdfs/official/Organization-of-the-educational-process.pdf.

Форма заліку – письмово-усна. Білет складається із 5 завдань, перші два з яких є теоретичними, три інших – задачі. Кожне завдання оцінюються від 0 до 7 балів. Додатково від 0 до 5 балів студент отримує за усне опитування. Всього за залік можна отримати від 0 до 40 балів.

Терміни проведення форм оцінювання:

1. Модульна контрольна робота №1: на 3-му тижні 1 семестру.

2. Модульна контрольна робота №2: на 9-му тижні 1 семестру

3. Оцінювання завдань самостійної роботи за РН2.1 на 3-му тижні, за РН2.2 на 6 тижні, за РН2.3 на 12 тижні 1 семестру

7.3 Шкала відповідності оцінок

Зараховано/ Passed	60 – 100
Не зараховано/ Fail	0 – 34

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ

теми	Назва теми **І семестр**	Кількість годин				
		Лекції	Практичні заняття	Самост. робота	Модульна контрольна	Інші форми контролю
Змістовий модуль 1 „ Комутативні кільця і модулі над ними ”						
1	Кільця і модулі, основні операції над ними	6	4	12		
2	Нетерові кільця і модулі, їх застосування в криптографії	6	4	18	2	
Змістовий модуль 2 „ Скінченні поля і їх застосування ”						
3	Будова скінченних полів	6	4	8	2	
4	Автоморфізми та базиси. Застосування скінченних полів в криптографії	8	4	8		
Всього годин		26	16	46	4	

Загальний обсяг 90 годин, у тому числі:
лекції – 26 годин,
практичні заняття – 16 годин
консультації – 2 годин,
самостійна робота – 46 годин.

9. Рекомендовані джерела

Основні:

1. Э. Б. Винберг Курс алгебры, М.Факториал Пресс, 2002.
2. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х тт. — М.: Мир, 1988.
3. М.Атья, И. Макдональд «Введение в коммутативную алгебру", М.Мир, 1972.
4. Hoffstein J., Pipher J., Silverman J. An introduction to mathematical cryptography.Springer, 2008.

Додаткові:

1. H.Matsumura, «Commutative Ring Theory» Cambridge University Press, 1986
2. D.Eisenbud «Commutative Algebra with a view toward Algebraic Geometry», Springer Verlag, 1988
3. R.Bose, Information Theory, Coding Thepry and Cryptography, Third edition, McGraw Hill Education, 2008, 463p.
4. Вернер М. Основы кодирования, Техносфера. 2004, 286с.
5. Koblitz N. Algebraic aspects of cryptography. Algorithms and Computation in Mathematics, Berlin: Springer. 2004, 206 p.