КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____Харитонов О.М.
«30» серпня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Науковий семінар з алгебри та основ захисту інформації

для студентів

галузь знань	**11 «Математика та статистика»**
спеціальність	**111 «Математика»**
освітній рівень	**другий (магістр)**
освітньо-наукова програма	**«Математика»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**21 /22**
Семестр	**3**
Кількість кредитів ECTS	**3**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: Ганюшкін О.Г., кандидат фізико-математичних наук, доцент кафедри алгебри і комп'ютерної математики.

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

КИЇВ – 2021

Розробник: Ганюшкін О.Г., кандидат фізико-математичних наук, доцент кафедри алгебри і комп'ютерної математики

ЗАТВЕДЖЕНО
Зав. кафедри алгебри і комп'ютерної математики
_____Петравчук А.П.
(підпис)
Протокол № 1 від 30.08.2021 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "31" 08 2021 року № 1.

Голова науково-методичної комісії _____ д.ф.-м.н. Олійник А.С.

1. Мета дисципліни – оволодіння основними ідеями та методами, що використовуються при дослідженні різних алгебричних структур і застосовуються для побудови систем захисту інформації при її обробці й передачі.

2. Попередні вимоги до опанування або вибору навчальної дисципліни.

1. *Знати:* основні поняття, факти і теореми лінійної алгебри, загальної алгебри, дискретної математики, комбінаторного аналізу, теорії алгоритмів.

2. *Вміти:* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Науковий семінар з алгебри та основ захисту інформації».

3. *Володіти елементарними навичками:* аналіз будови та дослідження основних характеристик різних класів алгебричних структур, знання основних алгоритмів для роботи з дискретними структурами та великими натуральними числами, оцінювання ефективності алгоритмів, дослідження параметрів кодів та криптосистем.

3. Анотація навчальної дисципліни:

«Науковий семінар з алгебри та основ захисту інформації» є складовою освітньої програми підготовки фахівців за освітнім рівнем «магістр» галузі знань 11 математика та статистика зі *спеціальності* 111 математика освітньої програми «математика».

Дана дисципліна є вибірковою.

Викладається у **1** семестрі **2** курсу магістратури в обсязі **90 год**. ***(3 кредитів ECTS)*** зокрема: семінари *28 год., консультації 2 год., самостійна робота – 60 год.* У курсі передбачено 2 *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна **заліком.**

4. Завдання (навчальні цілі): формування здатності розв'язувати складні математичні задачі та практичні проблеми у професійній діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій і характеризується комплексністю та/або невизначеністю умов; набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у математиці та статистиці, відповідно до освітнього рівня «Магістр». Зокрема, професійне оволодіння компетентностями:

1) Здатність учитися, здобувати нові знання, уміння, у тому числі в галузях, відмінних від математики;
2) Здатність використовувати у професійній діяльності знання з галузей математичних, природничих, соціально-гуманітарних та економічних наук;
3) Здатність вирішувати проблеми у професійній діяльності на основі абстрактного мислення, аналізу, синтезу та прогнозу;
4) Здатність до пошуку, оброблення й аналізу інформації з різних джерел, необхідної для розв'язування наукових і професійних завдань;
5) Здатність генерувати нові ідеї;
6) Здатність спілкуватися державною мовою і усно, і письмово;
7) Здатність спілкуватися іноземною мовою;
8) Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування;
9) Здатність критично оцінювати та переосмислювати власний і чужий досвід, аналізувати свою професійну й соціальну діяльність;
10) Знання на рівні новітніх досягнень, необхідні для дослідницької та/або інноваційної діяльності у сфері математики та її практичних застосувань;
11) Спроможність розуміти проблеми та виділяти їхні суттєві риси;

12) Спроможність розробляти математичну модель ситуації з реального світу та переносити математичні знання у нематематичні контексти;
13) Здатність доводити знання та власні висновки до фахівців та нефахівців;
14) Здатність до розвитку нових та удосконалення існуючих математичних методів аналізу, моделювання, прогнозування, розв'язування нових проблем у нових галузях знань;
15) Здатність до самоосвіти та підвищення кваліфікації на основі інноваційних підходів у сфері математики.

5. Результати навчання за дисципліною:

Табл.1

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	**Результати навчання**			
РН1.1	Знати основні алгебричні структури та їх найпростіші властивості	*Семінарські заняття, консультації*	*Активна робота на семінарських заняттях, виконання завдань для самостійної роботи, залік*	7%
РН1.2	Знати основні принципи використання алгебричних структур для побудови систем кодування та криптосистем			7%
РН1.3	Знати основні конструкції, які використовуються для побудови алгебричних структур із заданими властивостями			7%
РН1.4	Знати основні принципи дослідження будови різних класів алгебричних структур			7%
РН1.5	Знати методи дослідження складних алгебричних структур за допомогою допоміжних дискретних і комбінаторних структур			17%
РН2.1	Вміти використовувати основні поняття теорії алгоритмів для дослідження складності та надійності криптосистем	*Семінарські заняття, консультації*	*Письмові модульні контрольні роботи 1 та 2 (60% правильних відповідей для кожної), оцінювання роботи на семінарських заняттях, оцінювання виконання завдань для самостійної роботи, залік*	15%
РН2.2	Вміти вивчати симетрію і часткову симетрію різних математичних і фізичних структур методами теорії груп та інверсних напівгруп			15%
РН2.3	Вміти проводити аналіз складності та надійності систем кодування та криптосистем			15%

РН3.1	Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування	*Семінарські заняття*		2,5 %
РН3.2	Вироблення навичок командної роботи	*Семінарські заняття*		2,5 %
РН4.1	Продемонструвати розуміння особистої/персональної відповідальності за професійні та/або управлінські рішення, які базуються на використанні математичних методів	*Лекція, самостійна робота*	*Залік, контрольні роботи*	*5%*

6. Співвідношення результатів навчання дисципліни з програмними результатами навчання

Табл.2

Результати навчання дисципліни **Програмні результати навчання**	**РН1.1**	**РН1.2**	**РН1.3**	**РН1.4**	**РН1.5**	**РН2.1**	**РН2.2**	**РН2.3**	**РН3.1**	**РН3.2**	**РН4.1**
ПРН-З-1-Знати та розуміти фундаментальні і прикладні аспекти наук у сфері математики	+	+	+	+	+	+	+	+			
ПРН-З-2-Відтворювати знання фундаментальних розділів математики в обсязі, необхідному для володіння математичним апаратом відповідної галузі знань і використання математичних методів у обраній професії	+	+	+	+	+	+	+	+	+		
ПРН-З-3-Володіти основами математичних дисциплін і теорій, зокрема тих, що вивчають моделі природничих і соціальних процесів	+	+	+	+	+	+	+	+			
ПРН-З-4-Володіти математичними методами аналізу, прогнозування та оцінки параметрів моделей, математичними способами інтерпретації числових даних та принципами функціонування природничих процесів	+	+	+	+	+	+	+	+			
ПРН-У-1-Уміти використовувати фундаментальні математичні закономірності у професійній діяльності	+	+	+	+	+	+	+	+	+		+
ПРН-У-2-Читати і розуміти	+	+	+	+	+	+	+	+	+		

фундаментальні розділи математичної літератури та демонструвати майстерність їх відтворення в аргументованій усній та/або письмовій доповіді											
ПРН-У-3-Доносити професійні знання, власні обґрунтування і висновки до фахівців і широкого загалу									+	+	+
ПРН-У-8-Бути наполегливим у досягненні мети під час вирішення математичної проблеми	+	+	+	+	+	+	+	+			
ПРН-У-10-Усно й письмово спілкуватися рідною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності із професійних питань; знаходити, аналізувати та використовувати інформацію з різних довідкових джерел	+	+	+	+	+	+	+	+	+	+	
ПРН-У-11-Використовувати раціональні способи пошуку та використання науково-технічної інформації, включаючи засоби електронних інформаційних мереж; застосовувати інформаційні ресурси, у тому числі електронні, для пошуку відповідних математичних моделей	+	+	+	+	+	+	+	+	+	+	
ПРН-У-12-Дотримуватися норм етичної поведінки стосовно інших людей, адаптуватися та комунікувати									+	+	+

7. Схема формування оцінки
7.1 Форми оцінювання студентів:

- оцінювання впродовж навчального періоду:
1. Активна робота на семінарських заняттях: РН1.1 – РН1.5, РН 2.1-РН2.3, РН 3.1,3.2– 10 балів/6 балів;
2. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2, РН 2.3, РН 3.1,3.2 – 10 балів/7 балів;
3. Контрольна робота 1: РН1.1-РН1.3, РН2.1, РН2.2, РН4.1 – 25 балів/11 балів;
4. Контрольна робота 2: РН1.4-РН1.6, РН2.3, РН4.1 – 25 балів/11 балів;
Разом має бути 60/35.

- підсумкове оцінювання: *залік.*
- *максимальна кількість балів, які можуть бути отримані:* 40 балів;
- *результати навчання, які будуть оцінюватись:* РН1.1 – РН1.5, РН 2.1-РН2.3, РН 3.1,3.2, РН4.1;
форма проведення і види завдань: письмова робота.

7.2. Організація оцінювання:
Активна робота на семінарських заняттях передбачає успішну доповідь на запропоновану тему, активну участь в обговоренні тем наукових доповідей одногрупників, відповіді на запитання аудиторії.
Самостійна робота передбачає самостійне опрацювання літератури на предмет теоретичного матеріалу, розв'язування задач, запропонованих для самостійного розв'язання.

Критично-розрахунковий мінімум балів за навчання становить **20** балів, рекомендований мінімум, розрахований з урахуванням специфіки дисципліни становить **35** балів. Студенти, які протягом навчання набрали сумарно меншу кількість балів ніж рекомендований мінімум **35** балів для підвищення балів отримують можливість написати додаткову контрольну роботу та доскласти домашні завдання. Студенти, які набрали впродовж навчання та за рахунок додаткових етапів оцінювання сумарно меншу кількість балів ніж критично-розрахунковий мінімум – **20** балів, до складання заліку не допускаються.

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 – письмова. Заліковий білет складається із 4 задач. Кожне завдання оцінюються від 0 до 10 балів. Всього за залік можна отримати від 0 до 40 балів. Мінімальна кількість балів, які додаються до отриманих під час навчання – 24 бали.

Терміни проведення форм оцінювання:
1. Модульна контрольна робота №1: на 6-му тижні 3 семестру.
2. Модульна контрольна робота №2: на 12-му тижні 3 семестру.
3. Оцінювання завдань самостійної роботи за РН2.1- РН2.2 на 6 тижні, за РН2.3 на 12 тижні 3 семестру

7.3. Шкала відповідності оцінок

Оцінка (за національною шкалою) / National grade	Рівень досягнень, % / Marks, %

Зараховано / Passed	60-100%
Не зараховано / Fail	0-59%

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

теми	Назва теми	Кількість годин				
		Лекції	Семінари	Самост. робота	Конс.	Інші форми контролю
Змістовий модуль 1. Основні структури сучасної алгебри						
1	Основні структури з однією бінарною дією (групи та напівгрупи)		4	10		
2	Основні структури з двома бінарними діями (кільця, поля, алгебри Лі)		4	10		
3	Сучасні методі дослідження алгебричних структур (гомологічна алгебра, теорія категорій)		5	10	1	
Змістовий модуль 2. Основні підходи до захисту інформації: захист від пошкодження та захист від несанкціонованого доступу.						
4	Основні принципи побудови кодів, що виправляють помилки, та дослідження їх характеристик		7	15		
5	Основні принципи побудови криптосистем із відкритим ключем та їх криптоаналіз		8	15	1	
Всього годин			28	60	2	

Загальний обсяг 90 годин, у тому числі:
семінарські заняття – 28 години.
консультації – 2 години,
самостійна робота – 60 годин.

9. Рекомендовані джерела

Основні:

1. Бахтурин Ю.А. Основные структуры современной алгебры. М., Наука, 1990.
2. Общая алгебра (СМБ). Т. 1, Т.2. М., Наука, 1990.
3. Шафаревич И.Р. Основные понятия алгебры (обзор). М., ВИНИТИ, 1990.
4. Dummit D.S., Foote R.M. Abstract Algebra. 3rd edition. John Wiley and Sons, Inc., 2004.
5. Lang S. Algebra. Rev. 3rd Edition. Springer-Verlag. 2002.
6. Goldreich O. Foundations of Cryptography – A Primer. Cambridge University Press, 2005.
7. Goldreich O. Foundations of Cryptography: Vol. 1. Basic Tools, Cambridge University Press, 2004.
8. Goldreich O. Foundations of Cryptography: Vol. 2. Basic Applications. Cambridge University Press, 2009.

Додаткові:

1. Awodey Steve. Category Theory. Oxford University Press. 2rd edition. 2010.
2. Дрозд Ю.А., Кириченко В.В. Конечномерные алгебры. Киев, 1980.
3. Ganyushkin O., Mazorchuk V. Classical finite transformation semigroups. An introduction. Springer-Verlag, 2009.
4. Ноден П., Китте К. Алгебраическая алгоритмика. М., Мир, 1999.
5. Mac Williams F.J. Sloane N.J.A. The Theory of Error-Correcting Codes. Parts I, II. (є рос. переклад: Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М., Связь, 1979.