Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

ЗАТВЕРДЖУЮ
Директор Інституту телекомунікацій
і глобального інформаційного
простору НАН України,
Член-кор. НАНУ, д.т.н., професор

О.М.Трофимчук
Наказ від 21.07.2023 №19 -с

СИЛАБУС

навчальної дисципліни

Математичні моделі дискретної математики та їх застосування

113 – Прикладна математика
(спеціальність)

Київ-2023

Силабус з дисципліни **Математичні моделі дискретної математики та їх застосування**

(назва навчальної дисципліни)

Для аспірантів за галуззю знань - 11 Математика та статистика
Спеціальність – 113 Прикладна математика

Розробник:

Устименко В.М., д.ф.-м.н., професор
(прізвище та ініціали, науковий ступінь, вчене звання)

(підпис)

Робоча програма затверджена на засіданні вченої ради Інституту телекомунікацій і глобального інформаційного простору НАН України (протокол №7 від 12 червня 2023р.)

Голова вченої ради

Олександр ТРОФИМЧУК
(прізвище та ініціали)

Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

СИЛАБУС (SYLLABUS)

1. Опис навчальної дисципліни

Дисципліна	Математичні моделі дискретної математики та їх застосування
Освітній ступінь	Третій (освітньо-науковий)
Галузь знань	Математика та статистика
Спеціальність	Прикладна математика
Загальна характеристика дисципліни	Кількість годин - 60 Кількість кредитів – 2 Форма підсумкового контролю – залік Курс –2 Відділ досліджень навколишнього середовища
Пререквізити	Теорія чисел, Лінійна алгебра, Математична логіка
Анотація	Курс впроваджує математичний апарат необхідний для побудови і аналізу алгоритмів та розв'язання задач моделювання процесів та об'єктів. Лекції складаються з елементів комбінаторики, теорії графів, теорії чисел. прикладної алгебри,комбінаторики, теорії графів, теорії чисел і прикладної алгебри, теорії алгоритмів, математичної логіки,теорії скінченних геометрій, елементів теоретичної криптографії та теорії кодування.
Методи навчання	лекція (оглядова/тематична); семінарські/практичні (презентація/дискусія)
Результати навчання (компетентності	Здатність розуміння сутності та значення дискретної математики у розвитку сучасної комп'ютерної науки та інформатики; використовувати основні результати та методи дискретної математики у прикладних задачах моделювання в інформатиці.
Мова викладання	українська
Форма викладання	Денна, заочна

2. Інформація про викладача

Викладач	Устименко Василь Олександрович
Науковий ступінь	Доктор фізико-математичних наук
Посада	Завідувач відділу онтологічних систем та прикладної алгебраїчної комбінаторики
Адреса закладу	03186, м.Київ, Чоколівський бульвар,13,
E-mail	itelua@kv.ukrtel.net
Контактний телефон	(044) 245-8797

3. Календарно-тематичний план (схема вивчення курсу)

Назви тем	Кількість навчальних годин				Форми контролю
	Усього годин (кредитів)	Лекції	Практичні (семінарські) заняття	Самостійна робота студентів	
	60 год	*30 год*	*15 год*	*15 год*	
Тема 1(2 год.)	Математична індукція, рекуренція	Застосування математична індукції, залежності рекуренцій, залежності числа Фібоначі	Приклади застосування індукції	Розвязання рекуренційних рівнянь	Участь у дискусії, тестування
Тема2 (4 год.)	Підстановки та розбиття	Розклад підстановки на цикли, циклові числа Стірлінга	Приклади груп підстановок та їх застосування	Приклади застосуванн я теореми Холла-Кьонінга	Участь у дискусії, тестування
Тема 3 (2 год.)	Породжуючі функції	Породжуючі функції у задачах переліку комбінаторних об'єктів	Породжуючі функції і розвязання рекуренційн их рівнянь	Числа Каталана	Участь у дискусії, тестування
Тема 4 (4год.)	Теорія числа	Подільність, НСД, НСК, прості числа	Алгоритм Евкліда розклад на прості множники	Густина простих чисел	Участь у дискусії, тестування
Тема 5 (2 год.)	Модулярна арифметика	Теорема Ферма та Ейлера,	Китайська теорема про решту	Системи діамантових рівнянь	Участь у дискусії, тестування

		функція Мобіуса			
Тема 6 (4 год.)	Основні поняття теорії графів	Прості та дводольні графи	Сеті та сетеві потоки, теорема Форда-Фалкерсона	Алгоритм Форда-Фалкерсона	Участь у дискусії, тестування
Тема 7 (4 год.)	Дерева і цикли, цикли Ейлера і Гамільтона, алгоритми на графах	Планарність графів, теорема Куратовського	Розфарбування графів	Матриця сусідства графу, власні числа, матриця інциденції	Участь у дискусії, тестування
Тема 8 (4 год.)	Елементи теорії груп:	Означення групи, теорема Лагранжа	Циклічні групи, порядок елементу групи, вільна група	Групи симетрії многокутників	Участь у дискусії, тестування
Тема 9 (4 год.)	Застосування теорії груп у задачах переліку комбінаторних об'єктів	Дія групи на множині, теорема, Теорема Поля	Застосування теореми Поля у задачах перерахунку об'єктів	Групи матриць та їх дії на векторних просторах та інших многовидах	Участь у дискусії, тестування
Тема 10 (6 год.)	Скінченні поля	Кільця многочленів	Конструкція скінченних полів	Однозначність скінченного поля	Участь у дискусії, тестування
Тема 11 (4 год.)	Застосування алгебри і теорії чисел у криптографії	Криптосистема RSA, тест простоти Ферма та тест простоти Міллера-Рабіна	Приклади потокових і блокових алгоритмів симетричної криптографії	Криптографія від багатьох змінних	Участь у дискусії, тестування
Тема 12 (4 год.)	Скінченні геометрії та системи інциденції	Визначення геометрії за Ф. Клейном, Д. Гільбертом та Б. Ріманом	Групи Косетера та геометрії	Обчислення у скінченних геометріях	Участь у дискусії, тестування
Тема 13 (4 год.)	Прості скінченні групи та геометрії	Алгебра Лі та геометрії	Обчислення у геометрія класичних груп	Спорадичні прості групи та	Участь у дискусії, тестування

		простих груп типу Лі		геометрії Бюкенхо-Тіца	
Тема 14 (4 год.)	Постквантова та некомутативна геометрії	Основні напрямки пост квантової криптографії	Криптосистема Імай-Мацумото та її крипто аналіз	Потокові алгоритми шифрування визначені за графами	Участь у дискусії, тестування
Тема 15 (2 год.)	Елементи теорії кодування	Алгебраїчний підхід до відношень теорії кодування	Лінійні та BChX коди	Коди у схемах Хеммінга, код Голея	Участь у дискусії, тестування
Тема 16 (6 год.)	Елементи теорії алгоритмів	Машини Поста і Тюрінга, скінченні автомати	Обчислювальні та частково рекурсивні функції	Моделі алгоритмів і програм	Участь у дискусії, тестування

4. Перелік навчальних робіт та їх оцінка

Види робіт	Форми контролю	Оцінювання
Тема 1	Тест	Залік
Тема 2	Тест	Залік
Тема 3	Тест	Залік
Тема 4	Тест	Залік
Тема 5	Тест	Залік
Тема 6	Тест	Залік
Тема 7	Тест	Залік
Тема 8	Тест	Залік
Тема 9	Тест	Залік
Тема 10	Тест	Залік
Тема 11	Тест	Залік
Тема 12	Тест	Залік
Тема 13	Тест	Залік
Тема 14	Тест	Залік
Тема 15	Тест	Залік
Тема 16	Тест	Залік

Література.

1. Ю. В. Капітонова, С.А. Кривий, О. А. Летічевський, Г.М.Луцький, М. К. Печурін, Основи дискретної математики,Київ, Наукова думка, 2002, 579 с
2. В. І Андрійчук, М. Я. Комарницький, Ю. Б. Іщук, Вступ до дискретної математики, Київ, 2004, 254.
3. Г. Биркгоф, М.Барти., Современная прикладная алгебра, М., 1977.

4. Г. В. Гаврилов, А. А. Сапожников, Сборник задач по дискретной математике, М., 1977.
5. С. Т. Завало, Алгебра та теорія чисел, Практікум, У 2-х частинах, К., 1983.
М. Й. Ядренко, А. Я. Оленко, Дискретна математика, Навч. посібник, К., 1995.
7. О. В. Вербіцькій. Вступ до криптології, В НТЛ, Львів, 1998.
8.Р. Лиддл, Г. Нидеррайтер, Конечние поля, В 2-х томах, М.1988.
9. Л. А. Калужнин, Введение в общую алгебру, М.Наука, 1973.
10. Е. Менделсон, Введение в математическую логику,М. Мир, 1988.
11. Л. А. Скорняков, Теория структур, М. Мир, 1982.
12. М. Холл, Комбинаторика, М . Мир, 1970.
13. V. Ustimenko, Algebraic graphs and security of digital communications, Institute ofComputer Science, University of Maria CurieSklodowska in Lublin, 2011, 151 p.
14. V. Ustimenko, U. Romanczuk, Finite geometries, LDPC codes and Cryptography, Lublin, Publication UMCS, 2012.
15. P. Delsart, Algebraic approach to association schemes of coding theory,Philips Res. Rep. Suppl. 10 (1973).
16.N.Koblitz, Algebraic Aspects of Cryptography, Springer, 1998, 198 p.
17. T. Shaska , W C Huffman, D. Joyner, V Ustimenko (Editors), Advances in Coding Theory and Crytography (Series on Coding Theory and Cryptology) World Scientific Publishing Company, 2007.
18. H. Wielandt, Finite permutation groups, Acad. Press, New York, 1964, 312p.
19. R. Ore, Graph theory, Wiley, London, 1971.
20. R. W. Carter, Simple Groups of Lie Type, Wiley, New York (1972).
21. F. Buekenhout (Editor), Handbook on Incidence Geometry, North Holland, Amsterdam, 1995.
21. T. Richardson, R. Urbanke, Modern Coding Theory, Cambridge University Press, 2008.
22. K. Ross. C. Wright, Discrete Mathematics, World Scientific, 1992.
23. V.Ustimenko, M.Klisowski. On Noncommutative Cryptography with cubical multivariate maps of predictable density, In "Intelligent Computing'', Proceedings of the 2019 Computing Conference, Londone, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 998, Springer, pp. 654-674
DOI:10.1007/978-3-030-22868-2_47
24. Vasyl Ustymenko: On computations with Double Schubert Automaton and stable maps of multivariate cryptography. FedCSIS (Position Papers) 2021: 123-130
DOI:10.15439/2021F67
25. V. Ustimenko, On small world non-Sunada twins and cellular Voronoi diagrams, Algebra and Discrete Mathematics, vol. 30, No1 (2020). Pp 118-142.
DOI: http://dx.doi.org/10.12958/adm1343