Інститут телекомунікацій і глобального інформаційного простору НАН України

Відділ інформаційної безпеки

Математичні моделі дискретної математики та їх застосування

Робоча програма навчальної дисципліни (силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Третій (освітньо-науковий)***
Галузь знань	*Галузь F Інформаційні технології*
Спеціальність	*F3 – Комп'ютерні науки*
Освітньо-наукова програма	*Інформаційні технології*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна), заочна*
Рік підготовки, семестр	*2 курс, весняний семестр*
Обсяг дисципліни	*90 годин / 3 кредити ЄКТС* *(лекції – 20 год., практичні заняття – 10 год., СРС – 60 год.)*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*2 год лекційних та 1 год практичних занять на тиждень*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лекції та практичні заняття проводить: *д.ф.-м.н., професор, Устименко Василь Олександрович*
Розміщення курсу	https://classroom.google.com/c/ODQzMjEwMzYxMjUx?cjc=uhxrouaw

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна «Математичні моделі дискретної математики та їх застосування» *впроваджує математичний апарат необхідний для побудови та аналізу алгоритмів і розв'язання задач моделювання процесів та об'єктів. Лекції складаються з елементів комбінаторики, теорії графів, теорії чисел і прикладної алгебри, теорії алгоритмів, математичної логіки, теорії скінченних геометрій, елементів теоретичної криптографії та теорії кодування. Курс знайомить слухачів з новітніми проблемами постквантової та квантової криптографії та сучасними методами для їх розв'язання, методами використання штучного інтелекту в прикладних комп'ютерних алгоритмах. Ці методи можуть бути використані для розв'язання задач дисертаційного дослідження.*

Мета: *формування в аспірантів загальних та фахових компетентностей, навчити аспірантів застосовувати методи дискретної математики, методи моделювання в інформаційних технологіях та дослідженнях з прикладної математики*

Предмет вивчення – *є дискретна математики вцілому, що об'єднує різні математичні методи, які використовуються* ***в*** *інформатиці та комп'ютерних науках.*

Програмні результати навчання: *оволодіння методами дискретної математики, що поєднують використання теорії чисел, комбінаторики, алгебри та математичної логіки, застосування цих методів у дослідженнях з прикладної математики, розробках комп'ютерних алгоритмів, моделюванні різноманітних процесів математичними методами.*

Загальні компетентності

ЗК 01 Здатність до абстрактного мислення, аналізу та синтезу.
ЗК 02 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК04 Здатність розв'язувати комплексні проблеми комп'ютерних наук на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.
ЗК 06 Здатність до набуття концептуальних та методологічних знань в галузі чи на межі галузей знань або професійної діяльності, використання спеціалізованих умінь/навичок і методів, необхідних для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики, безперервного саморозвитку та самовдосконалення.

Фахові компетентності

СК01 Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей.
СК 02 Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.
СК 03 Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень.
СК 06 Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій.
СК 08 Здатність дотримуватись академічної та професійної доброчесності, морально-етичних правил поведінки, етики досліджень в академічному середовищі.

Програмні результати навчання

ПРН 01 Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.
ПРН 03 Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.
ПРН 04 Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямах.
ПРН05 Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.
ПРН 06 Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.
ПРН 10 Відшуковувати, оцінювати та критично аналізувати інформацію щодо поточного стану та трендів розвитку, інструментів та методів досліджень, наукових та інноваційних проєктів з комп'ютерних наук.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

*Дисципліна **«Математичні моделі дискретної математики та їх застосування»** вивчається у зимовому (четвертому) семестрі другого курсу, тому для успішного засвоєння дисципліни необхідні знання з дисциплін: Лінійна алгебра, Логіка числення висловлювань, Комбінаторні методи, Елементи теорії ймовірностей, Алгебраїчні методи. Для вивчення дисципліни «Математичні моделі дискретної математики та їх застосування» аспірант має бути знайомий з основами постановки задач та методами математичного моделювання, обчислювальними методами, методикою проведення чисельних експериментів та оброблення даних, розробляти комп'ютерні моделі та реалізовувати їх в спеціалізованих середовищах та створювати власні розробки використовуючи сучасні мови програмування, розробляти, аналізувати та застосовувати знання з різних предметних.*

Як результат курсу слухач повинен володіти методами дискретної математики, дискретного математичного моделювання для використання дисертаційних досліджень комп'ютерних науках та прикладної математики.

3. Зміст навчальної дисципліни

Тема 1. *Предмет дискретної математики, зв'язки з алгеброю, теорію чисел. Математична індукція та рекурсія.*

Тема 2. *Підстановки та розбиття.*

Тема 3. *Породжуючі функції.*

Тема 4. *Елементи теорії чисел.*

Тема 5. *Модулярна арифметика. Булеві кільця та їх застосування.*

Тема 6. *Основні поняття теорії графів.*

Тема 7. *Дерева і цикли, цикли Ейлера і Гамільтона, алгоритми на графах. Графи задані рівняннями та їх застосування.*

Тема 8. *Напівгрупи, групи та їх властивості.*

Тема 9. *Застосування теорії груп у задачах переліку комбінаторних об'єктів, теорії кодування та криптографії.*

Тема 10. *Скінченні поля. Графи задані рівняннями над скінченими полями та кільцями.*

Тема 11. *Застосування алгебри та алгебраїчних графів у сучасній криптографії.*

Тема 12. *Скінченні геометрії та системи інциденції і їх застосування.*

Тема 13. *Теорії першого порядку, аксіоматика теорії чисел та теорії груп.*

Тема 14. *Постквантова та некомутативна криптографія та символьні обчислення.*

Тема 15. *Елементи теорії кодування, схеми відношень та класичні метрики, графи та коди LDPC.*

Тема 16. *Елементи теорії алгоритмів, машина Тюрінга, квантовий комп'ютер та символьні обчислення.*

4. Навчальні матеріали та ресурси

Базова література

1. V. Ustimenko, Graphs in terms of Algebraic Geometry, symbol is computations and secure communications in Post-Quantum world, Wydawnictwo University of Maria-Curie Sklodowska, Lublin, 2022, 212pp. https://www.researchgate.net/publication/359045063
2. V. Ustimenko, On Schubert cells of Lie geometries and public keys of multivariate cryptography, Contemporary Mathematics, Volume 830, 2025, https://doi.org/10.1090/conm/830/1656.
3. V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023), https://doi.org/10.1007/s40879-023-00685.
4. V. Ustimenko, On the restoration of historical Matsumoto - Imai cryptosystem and other schemes in terms of Noncommutative Cryptography, FTC-2024, Future Technologies Conference, 14-15, November 2024, London, In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2024, Volume 2. FTC 2024. Lecture Notes in Networks and Systems, vol 1155. Springer, Cham. https://doi.org/10.1007/978-3-031-73122-8_7
5. V. Ustimenko, On Schubert cells of Lie geometries and public keys of multivariate cryptography, Contemporary Mathematics, Volume 830, 2025 https://doi.org/10.1090/conm/830/16568
6. Mendelson, Introduction to Mathematical Logic, Sam Buss August 14, 2023, 302 p.

Додаткова література

1. Michiel Hazewinkel, Nadiya Gubareni, V.V. Kirichenko, Algebras, Rings and Modules Non-commutative Algebras and Rings, CRC Press, 2021
2. V. Ustimenko, Algebraic graphs and security of digital communications, Institute ofComputer Science, University of Maria Curie Sklodowska in Lublin, 2011, 151 p.
3. V. Ustimenko, U. Romanczuk, Finite geometries, LDPC codes and Cryptography, Lublin, Publication UMCS, 2012.
4. 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.
5. N. Gubareni. Introduction to Modern Algebra and Its Applications. CRC Press, 2021.
6. Kenneth H. Rozen, Discrete Mathematics and Its Applications, Published by McGraw-Hill, 2012, 1072 p.
7. Vasyl Ustymenko: On computations with Double Schubert Automaton and stable maps of multivariate cryptography. FedCSIS (Position Papers) 2021: 123-130 DOI:10.15439/2021F67

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання, для проведення практичних занять використовується дослідницький метод навчання: викладач ставить перед аспірантами проблему, і ті вирішують її самостійно або під керівництвом викладача.

За дистанційної форми навчання заняття проводять за допомогою платформи для

проведення онлайн-зустрічей Zoom

№ п/п	Змістові модулі / теми	Кількість годин, відведених на:			Термін виконання
		лекції	практичні заняття	сам. робота.	
1	2	3	4	5	6
T1	*Тема 1 Предмет дискретної математики, зв'язки з алгеброю, теорію чисел. Математична індукція та рекурсія.*	2	2	2	1-й, 2-й тиждень
T2	*Тема 2: Підстановки та розбиття.*	2	2	2	3-й, 4-й тиждень
T3	*Тема 3: Породжуючі функції.*	1	1	4	5-й, 6-й тиждень
T4	*Тема 4: Елементи теорії чисел.*	1	2	3	7-й, 8-й тиждень
T5	*Тема 5: Модулярна арифметика. Булеві кільця та їх застосування.*	2	1	3	9-й, 10-й тиждень
T6	*Тема 6: Основні поняття теорії графів.*	2	2	2	9-й, 10-й тиждень
T7	*Тема 7: Дерева і цикли, цикли Ейлера і Гамільтона, алгоритми на графах. Графи задані рівняннями та їх застосування.*	1	1	3	9-й, 10-й тиждень
T8	*Тема 8: Напівгрупи, групи та їх властивості.*	1	2	2	10-й, 11-й тиждень
T9	*Тема 9: Застосування теорії груп у задачах переліку комбінаторних об'єктів, теорії кодування та криптографії.*	1	1	3	10-й, 11-й тиждень
T10	*Тема 10: Скінченні поля. Графи задані рівняннями над скінченими полями та кільцями.*	1	1	3	10-й, 11-й тиждень
T11	*Тема 11: Застосування алгебри та алгебраїчних графів у сучасній криптографії.*	1	1	3	12-й, 13-й тиждень
T12	*Тема 12: Скінченні геометрії та системи інциденції і їх застосування. Прості скінченні групи та їх геометрії.*	1	1	3	12-й, 13-й тиждень
T13	*Тема 13: Теорії першого порядку, аксіоматика теорії чисел та теорії груп.*	1	1	3	12-й, 13-й тиждень
T14	*Тема 14: Постквантова та некомутативна криптографія та символьні обчислення.*	1	1	3	14-й, 15-й тиждень
T15	*Тема 15: Елементи теорії кодування, схеми відношень та класичні метрики, графи та коди LDPC*	1	1	3	14-й, 15-й тиждень
T16	*Тема 16: Елементи теорії алгоритмів, машина Тюрінга, квантовий комп'ютер та символьні обчислення.*	1	1	3	14-й, 15-й тиждень
	Всього модуль	**20**	**21**	**45**	

5.1. Лекції

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на інформаційні джерела)
Тема 1 Предмет дискретної математики, зв'язки з алгеброю, теорію чисел. Математична індукція та рекурсія.	
1	***Лекція 1. Предмет дискретної математики*** *Основні питання: основні розділи дискретної математики; приклади моделей дискретної математики; застосування дискретної математики у теорії комунікацій*
	Лекція 2. Математична індукція та рекурсія. *Основні питання: приклади доведень методом математичної індукції; приклади рекуренційних співвідношень у теорії чисел; поняття рекурсивних функцій.*
Тема 2 Підстановки та розбиття.	
2	***Лекція 3. Елементи теорії груп підстановок.*** *Основні питання: парні та непарні підстановки і теорія визначників; підгрупи симетричної групи, дії на множині; примітивні та імпримітивні групи підстановок.*
	Лекція 4. Розбиття та відношення еквівалентності. *Основні питання: розбиття скінченної множини; подібність матриць, інші відношення еквівалентності; фактор множини та факторизація алгебраїчних систем.*
Тема 3 Породжуючі функції.	
3	***Лекція 5. Породжуючі функції.*** *Основні питання: включення та виключення; приклади породжуючих функцій, застосування методу включення та виключення.*
Тема 4 Елементи теорії чисел.	
4	***Лекція 6. Елементи теорії чисел.*** *Основні питання: подільність та модулярна арифметика; представлення цілих чисел в пам'яті комп'ютера та алгоритми; прості числа та найбільший спільний дільник; лишки за модулем m, діафантові рівняння.*
Тема 5 Модулярна арифметика. Булеві кільця та їх застосування.	
5	***Лекція 7. Лишки за модулем m та багатозначна логіка.*** *Основні питання: Булеві функції та функції багатозначної логіки; представлення булевих функцій; логічні брамки та мінімізація Булевих функцій.*
	Лекція 8. Булеві функції та скінченні автомати. *Основні питання: задача класифікації Булевих функцій від n змінних; Булеві кільця та їх застосування у комп'ютерних обчисленнях; графи визначені над Булевими кільцями та їх застосування.*
Тема 6 Основні поняття теорії графів.	
Лекція 9. Графи і моделі у термінах графів. *Основні питання: представлення графів, ізоморфізм графів; найкоротша стежка у графі та алгоритм її знаходження; розфарбування графів.*	
Лекція 10. Спеціальні типи графів. *Основні питання: зв'язні графи, діаметр; Ойлерівські та Гамільтонівські стежки; планарні графи.*	
Тема 7 Дерева і цикли, цикли Ейлера і Гамільтона, алгоритми на графах. Графи задані рівняннями та їх застосування.	

7	***Лекція 11. Дерева, цикли у графах, алгоритми на графах.*** *Основні питання: теорема про кількість ребер у дереві; нескінченні регулярні дерева, їх задання квадратичними рівняннями на векторних просторах; апроксимація нескінченного дерева сім'єю графів великого обгорту.*
	Лекція 12. Графи задані рівняннями та їх застосування. *Основні питання: лінгвістичні графи; лінгвістичні графи та нелінійні перетворення векторних просторів; криптографічні застосування лінгвістичних графів.*

Тема 8 Напівгрупи, групи та їх властивості.	
8	***Лекція 13. Способи задання груп та напівгруп.*** *Основні питання: комбінаторна теорія груп та напівгруп; групи та напівгрупи матриць; операції на групах та напівгрупах.*
	Лекція 14. Гомоморфізми груп та напівгруп, нормальні дільники у групах. *Основні питання: класи суміжності, теорема Лагранжа; прості некомутативні групи; алгебри Лі та групи.*
Тема 9 Застосування теорії груп у задачах переліку комбінаторних об’єктів, теорії кодування та криптографії.	
9	***Лекція 15. Застосування теорії груп та перелік комбінаторних об'єктів.*** *Основні питання: теорема Пойя; задача обчислення кількості класів еквівалентності; вивчення орбіт симетричної групи, що діє на множині многочленів.*
	Лекція 16. Застосування теорії груп до кодування та криптографії. *Основні питання: застосування груп Коксетера у теорії кодування; застосування простих груп теорії Лі у теорії кодування; застосування простих груп теорії Лі у криптографії.*
Тема 10 Скінченні поля. Графи задані рівняннями над скінченими полями та кільцями.	
10	***Лекція 17. Скінченні поля.*** *Основні питання: розширення Кронекера; класифікація скінченних полів; застосування скінченних полів у комп'ютерних науках.*
	Лекція 18. Графи задані рівняннями над скінченими полями та кільцями. *Основні питання: лінгвістичні графи над скінченними полями та клітини Шуберта геометрій простих груп типу Лі; узагальнення простих геометрій типу Лі визначених над кільцями; застосування алгебраїчних графів визначених над полями та кільцями у криптографії.*
Тема 11 Застосування алгебри та алгебраїчних графів у сучасній криптографії.	
11	***Лекція 19. Застосування алгебри та алгебраїчних графів у сучасній криптографії.*** *Основні питання: криптографія від багатьох змінних; некомутативна криптографія; алгебраїчні графи та алгоритми шифрування.*
Тема 12 Скінченні геометрії та системи інциденції і їх застосування. Прості скінченні групи та їх геометрії.	
12	***Лекція 20. Скінченні геометрії та системи інциденції і їх застосування.*** *Основні питання: теорема класифікації простих скінченних груп; геометрії простих груп типу Лі і BN пари; застосування BN пар у теорії кодування і криптографії.*
Тема 13 Теорії першого порядку, аксіоматика теорії чисел та теорії груп.	
13	***Лекція 21. Теорії першого порядку, аксіоматика теорії чисел та теорії груп.*** *Основні питання: числення предикатів; приклади теорій першого порядку та їх інтерпретація; системи аксіом теорії чисел та теорії груп.*
Тема 14 Постквантова та некомутативна криптографія та символьні обчислення.	

14	***Лекція 22. Постквантова та некомутативна криптографія та символьні обчислення.*** *Основні питання: основні напрямки Постквантової криптографії з публічними ключами; використання граток та інших комбінаторних об'єктів у Постквантовій криптографії; некомутативна криптографія у термінах символьних обчислень.*
Тема 15 Елементи теорії кодування, схеми відношень та класичні метрики, графи та коди LDPC	
15	***Лекція 23. Елементи теорії кодування, схеми відношень та класичні метрики, графи та коди LDPC*** *Основні питання: схеми відношень теорії кодування побудовані через орбітали груп Коксетера; схеми відношень теорії кодування побудовані через орбітали класичних груп типу Лі; LDPC та графи Таннера.*
Тема 16 Елементи теорії алгоритмів, машина Тюрінга, квантовий комп'ютер та символьні обчислення.	
16	***Лекція 24. Елементи теорії алгоритмів, машина Тюрінга, квантовий комп'ютер та символьні обчислення.*** *Основні питання: скінченні автомати та машина Тюрінга; складність детерміністичних алгоритмів та алгоритмів реалізованих на квантовому комп'ютері; складність алгоритмів визначених у термінах символьних обчислень.*

5.2 Практичні роботи

Практичні заняття

№ з/п	*Назва теми заняття та перелік основних питань*
1	*Практичне заняття №1. Приклади математичних моделей дискретної математики.* *Основні питання заняття: скінченні автомати; алгебраїчні системи у пам'яті ЕОМ; моделювання потоків у мережах.*
2	*Практичне заняття №2. Розбір прикладів доведень методом математичної індукції, псевдовипадкові послідовності задані рекурсійно.* *Основні питання: числа Фібоначчі; приклади рекуренційно заданих мереж; приклади примітивно-рекурсійних функцій.*
3	*Практичне заняття №3. Операції над підстановками та групами підстановок* *Основні питання: обчислення суперпозиції підстановок; спряжені елементи у симетричній групі; цикловий індекс підстановки.*
4	*Практичне заняття №4. Приклади відношення еквівалентності.* *Основні питання: розбір прикладів відношення еквівалентності у теорії чисел; еквівалентність у пропозиційній логіці; приклади трансвесалей на класах еквівалентності.*
5	*Практичне заняття №5. Перелік комбінаторних об'єктів та породжуючих функцій* *Основні питання: перелік дерев; приклади розв'язання задач переліку комбінаторних об'єктів за допомогою породжуючих функцій.*
6	*Практичне заняття №6. Застосування лишків за модулем т.* *Основні питання: задача дискретного логарифму у кільці Z_p ; класичний протокол обміну ключів Діффі-Хеллмана; фунція Ейлера та алгоритм RSA.*

7	*Практичне заняття №7. Застосування малої теореми Ферма та теореми Ейлера* *Основні питання: критерій Рабіна-Мілера простоти цілого числа; застосування мультиплікативних груп кільця лишків Z_n.*
8	*Практичне заняття №8. Криптографічні алгоритми з використанням Булевих кілець* *Основні питання: потокові алгоритми шифрування; алгоритми з публічним ключем; криптографічні протоколи визначених над Булевими кільцями.*
9	*Практичне заняття №9. Спектри графів* *Основні питання: приклади графів-експандерів; узагальнені многокутники; спектри графів Хемінга та Джонсона*
10	*Практичне заняття №10. Приклади графів з екстремальними властивостями*

	Основні питання: графи малого світу; графи великого обгорту; графи Мура та функція V(k,j)
11	*Практичне заняття №11. Потокові алгоритми шифрування визначені за апроксимізацією дерев.* *Основні питання: шляхи на графах та гасла алгоритму шифрування; комбінація кодування за графами з лінійними перетвореннями; вимоги до алгоритмів шифрування, рівень безпеки*
12	*Практичне заняття №12. Приклади груп заданих генераторами та співвідношеннями.* *Основні питання: циклічні групи та моногінні напівгрупи, період та індекс; скінченні групи Коксетера; приклади нескінченних груп Коксетера.*
13	*Практичне заняття №13. Напівгрупа Кремони, її піднапівгрупи та підгрупи.* *Основні питання: приклади ендоморфізмів кілець від багатьох змінних; стандартна форма задання нелінійного перетворення; приклади стабільних елементів та стабільних підгруп групи Кремони.*
14	*Практичне заняття №14. Застосування теорії груп у некомутативній криптографії.* *Основні питання: логічні схеми протоколів обміну ключів визначених у термінах теорії груп; приклади платформ алгоритмів некомутативної криптографії; символьне обчислення та платформи некомутативної криптографії.*
15	*Практичне заняття №15. Криптографічні алгоритми визначені над полями та кільцями.* *Основні питання: потокові алгоритми шифрування визначені за алгебраїчними графами; публічні ключі визначені за алгебраїчними графами; алгоритми некомутативної криптографії визначені за алгебраїчними графами.*
16	*Практичне заняття №16. Приклади криптосистем алгебраїчної криптографії.* *Основні питання: публічний ключ Імао-Мацумото; підкручений протокол Діффі-Хелмана і його імплементація на платформах символьних обчислень; потокові алгоритми шифрування визначені за графами D(n,q).*
17	*Практичне заняття №17. Класичні групи Шевальє на діаграмами A_n, B_n, C_n, D_n та їх застосування.* *Основні питання: класичні прості групи та схеми відношень теорії кодування; клітини Шуберта скінченної проективної геометрії та їх застосування у криптографії; геометрія групи A_n (F_q) та генерація стабільних підгруп у групах Кремони.*
18	*Практичне заняття №18. Елементи числення предикатів* *Основні питання: приклади правильно побудованих формул у числення предикатів; підрахунок кількості інтерпретацій формули на скінченній множині; логічна дедукція у теоріях першого порядку, приклади.*

19	*Практичне заняття №19. Приклади криптосистем та протоколів Постквантової криптографії.* *Основні питання: приклади криптосистем з публічним ключем від багатьох змінних; приклади протоколів некомутативної криптографії побудовані у термінах теорії символьних обчислень; алгоритми типу Ель-Гамаля некомутативної криптографії.*
20	*Практичне заняття №20. Вивчення властивостей LDPC кодів побудованих за екстремальними графами.* *Основні питання: LDPC коди визначені за графами Келі-Рамануджан; LDPC коди визначені за графами D(n,q); LDPC коди визначені за графами A(n,q).*
21	*Практичне заняття №21. Приклади детерміністичних та недетерміністичних алгоритмів.*

	Основні питання: проблема дискретного логарифму, її розв'язок у термінах квантових обчислень; проблема факторизації цілих чисел, її розв'язок у термінах квантових обчислень; проблема спряження з потенціюванням у напівгрупи Кремони символьних перетворень

5.3 Самостійна робота студента/аспіранта

№	Вид самостійної роботи	Кількість годин (орієнтовно)
1.	Підготовка до аудиторних занять	15
2.	Дослідження реальних задач	5
3.	Проведення розрахунків	10
4	Прогнозування	5
5	Формування звіту за результатами дослідження	10
	Всього	**45**

Політика та контроль

8 Політика навчальної дисципліни (освітнього компонента)

Вимоги, яких має дотримуватися студент в рамках даної дисципліни:

- правила відвідування занять: відвідування лекцій та практичних занять, а також відсутність на них, не оцінюється. Однак, студентам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання семестрового індивідуального завдання та проводяться контрольні заходи (тести) з поточної оцінки самостійної роботи студентів з засвоєння поточного матеріалу. Останні є складовою частиною поточного рейтингу і проводяться тільки у день проведення відповідних лекцій та практичних занять. Система оцінювання орієнтована на отримання балів за своєчасність виконання студентами практичних та контрольних робіт, а також виконання завдань, які здатні розвинути практичні уміння та навички;
- правила поведінки на заняттях: студент повинен брати участь у розв’язку задач, готувати короткі доповіді;
- захист практичних – захист відбувається у визначені терміні під час аудиторних занять;
- політика щодо академічної доброчесності– політика та принципи академічної доброчесності визначені у Етичному кодексі вченого Інституту телекомунікацій та глобального інформаційного простору НАН України.

9 Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Семестровий контроль - залік. Рейтингова система оцінювання результатів навчання передбачає оцінювання заходів поточного контролю з дисципліни впродовж семестру. Рейтингова оцінка здобувача складається з балів, отриманих здобувачем за результатами заходів поточного контролю. Рейтингова оцінка доводиться до здобувачів на передостанньому занятті з дисципліни в семестрі. Здобувачі, які виконали всі умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань

Зі здобувачами, які виконали всі умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить семестровий контроль у вигляді залікової контрольної роботи.

Для посилення зацікавленості здобувачів у якісному виконанні індивідуальних семестрових завдань, передбачених індивідуальним навчальним планом здобувача, рейтингову оцінку, у разі виконання залікової контрольної роботи, можна визначати як суму балів за залікову контрольну роботу та балів за індивідуальне семестрове завдання. У цьому випадку розмір шкали оцінювання

залікової контрольної роботи зменшується на максимальне значення балів, передбачених за виконання відповідного індивідуального семестрового завдання.

Після виконання залікової контрольної роботи, якщо оцінка за залікову контрольну роботу більша ніж за рейтингом, здобувач отримує оцінку за результатами залікової контрольної роботи. Якщо оцінка за залікову контрольну роботу менша ніж за рейтингом, то здобувач отримує більшу з оцінок, що отримані за результатами залікової контрольної роботи або за рейтингом.

До відомості семестрового контролю викладач заносить рейтингові бали, отримані здобувачем у семестрі або за результатами виконання залікової контрольної роботи, та оцінку відповідно до цих балів

Критерії нарахування балів:

1. Практичні заняття оцінюються виходячи з максимальної кількості балів - 20 бали кожне:

- «відмінно» – 95 відсотків максимального балу;
- «добре» –75-95 відсотків максимального балу;
- «задовільно» – 60-75 відсотків максимального балу;
- «достатньо» – 50 відсотків – робота виконана, але не захищена.

Умови допуску до підсумкового контролю є зарахування усіх практичних робіт.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

– виконання практичних (лабораторних) робіт;

– виконання самостійної роботи.

За період вивчення дисципліни студент може набрати 100 балів. Їх розподіл між видами робіт наведено в таблиці 1

Таблиця 1

Бали за виконання	Номер практичної роботи або теми					Разом
	1	2	3	4	5	
Практичної роботи	10	10	10	10	10	100
Самостійної роботи	10	10	10	10	10	

2. Залікова контрольна робота оцінюється за такими критеріями:

- «відмінно» – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд;
- «добре» – достатньо повна відповідь (не менше 75% потрібної інформації), що виконана згідно з вимогами до рівня «умінь», або незначні неточності);
- «задовільно» – неповна відповідь (не менше 60% потрібної інформації. що виконана згідно з вимогами до «стереотипного» рівня та деякі помилки);
- «незадовільно» – незадовільна відповідь – 0 балів.

Залікова контрольна робота передбачається у вигляді тесту, критерії оцінювання тесту:

Кількість правильних відповідей	*Відсоток правильних відповідей*	*Оцінка за національною шкалою*	*Оцінка за шкалою ECTS*
48-50	*95-100*	*Відмінно*	*A*
41-47	*82-94*	*Дуже добре*	*B*
37-40	*75-81*	*Добре*	*C*
34-36	*69-74*	*Задовільно*	*D*
30-33	*60-68*	*Достатньо*	*E*
5-29	*10-13*	*Не задовільно*	*FX*

Відповідність рейтингових балів оцінкам за шкалою Інституту та *шкалою ECTS*

Рейтингова оцінка	*Оцінка за національною шкалою*	*Оцінка за шкалою ECTS*
90-100	*Відмінно*	*A*
82-89	*Дуже добре*	*B*
75-81	*Добре*	*C*
69-74	*Задовільно*	*D*
60-68	*Достатньо*	*E*
45-59	*Не задовільно*	*FX*
Невиконання умов допуску до семестрового контролю	*Не допущено*	

10 Додаткова інформація з дисципліни (освітнього компонента)

- *перелік питань, які виносяться на семестровий контроль у додатку*
- є можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів Coursera за відповідною тематикою – зараховується додатково до 10 балів до загального рейтингу студента, якщо студент набрав не менше 75 балів за період вивчення курсу та отримав відповідний сертифікат.

Робочу програму навчальної дисципліни (силабус):

Склав: д.ф.-м.н., професор Устименко Василь Олександрович

Затверджено:

Вченою радою Інституту телекомунікацій
і глобального інформаційного простору
НАН України Протокол № 10 від 13 серпня 2026 р.

Введено в дію:

Наказом директора
Наказ від 14 серпня 2026 р. № 12

Перелік питань до заліку з дисципліни

1. Definition of Symmetric group on the set, examples of its subgroups. Означення симетричної групи на множині та прикладі її підгруп
2. Cyclic index of a permutation on the finite set, conjugated elements of symmetric group. Цикловий індекс підстановки на скінченій множині, спряжені елементи симетричної групи.
3. Systems of distinct representatives of the family of subsets, Системи різних представників для сімейства підмножин. Теорема Хола-Коніга.
4. Lagrange Theorem of Group Theory. Theorems on homomorphisms. Теорема Лагранжа теорії груп. Теореми про гомоморфізми.
5. Cayley Theorem on action of groups on sets. Transitive permutation groups. Primitivity and imprimitivity. Теорема Келі про дію груп на множинах. Транзитивні групи перестановок. Примітивність та імпримітивність.
6. Polya Theorem. Renumerations of combinatorial objects. Examples. Теорема Пойя. Перенумерації комбінаторних об'єктів. Приклади.
7. Divisibility in arithmetics, Residues. Подільність в арифметиці, Лишки за модулем.

8. Little Fermat Theorem. Discrete logarithm problem. Application to Cryptography. Мала Теорема Ферма. Проблема дискретного логарифмування. Застосування до криптографії.

9. Diffie-Hellman protocol of key exchange. Протокол обміну ключами Діффі-Хеллмана.

9. Main Theorem of Arithmetics. Euler function. Основна теорема арифметики. Функція Ейлера,

10. Euler Theorem and RSA algorithm. Public keys in Cryptography. Теорема Ейлера та алгоритм RSA. Відкриті ключі в криптографії.

11. Commutative rings, ideals and homomorphisms. Комутативні кільця, ідеали та гомоморфізми.

12. Eucledian algorithm of finding the greatest common divisors and Eucledian rings. Евклідів алгоритм знаходження найбільших спільних дільників, Евклідові кільця.

13 Polynomial rings. Gilbert Theorem on basis. Кільця многочленів, теорема Гілберта про базис.

14. Systems of polynomial equations, complexity. Grobner bazis. Системи поліноміальних рівнянь, складність. Базис Грьобнера.

15. The definition of fields. Examples. Визначення полів. Приклади.

16. Kronecker extensions. Structure of finite fields. Розширення Кронекера. Структура скінченних полів

17. Multivariate Cryptography. Matsumoto-Imai Cryptosystems and its restorations. Криптографія від багатьох змінних. Мацумото-Імаї Криптосистеми та їх реставрації.

18. Basic definitions of graph theory. Finite and infinite trees. Основні визначення теорії графів. Скінченні та нескінченні дерева.

19. Regular graphs. Spectral Graph Theory. Expanders. Регулярні графи. Спектральна теорія графів. Графи-експандери.

20, Association schemes of Coding Theory. Distance regular and distance transitive graphs. Схеми відношень теорії кодування. Дистанційно регулярні та дистанційно-транзитивні графи.

21. Turan type problems of Extemal Graph Theory. Erdos Even Circuits Theorem. Проблеми типу Турана Екстемальної теорії графів. Теорема парного циклу Ердоша.

22. Graph Based Cryptography. Examples of public keys and key establishment protocols. Криптографія на основі графів. Приклади відкритих ключів та протоколів встановлення ключів.

23. Finite simple groups, their geometries, groups of Lie type and Tits geometries. Скінченні прості групи, їх геометрії, групи типу Лі та геометрії Тітса.

24. Small and Large Schubert cells on Lie Geometries, appplications of Lie geometries to Multivariate and Noncommutative Cryptoraphies, Малі та великі комірки Шуберта на геометріях Лі, застосування геометрій Лі до криптографії від багатьох змінних та некомутативної криптографії,

26. Propositional logic and Boolean Functions. Логіка висловлювань та Булеві функції.

27. Calculus of predicates and axiomatization of Arithmetics. Числення предикатів та аксіоматизація арифметики.

28. Turing machine and Quantum Computer. Examples of Turing machines. Quantum and Postquantum Cryptography. Машина Тюрінга та квантовий комп'ютер. Приклади машин Тюрінга. Квантова та постквантова криптографія.