Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра математичного аналізу та теорії ймовірностей

АЛГОРИТМІЧНА ТЕОРІЯ ЧИСЕЛ ТА КВАНТОВІ ОБЧИСЛЕННЯ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Третій (освітньо-науковий)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*111 Математика*
Освітня програма	*Математика*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*II курс, весняний семестр*
Обсяг дисципліни	*4 кредитів ЄКТС*
Семестровий контроль/ контрольні заходи	*іспит*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: д.ф.-м.н., професор Клесов Олег Іванович, klesov@matan.kpi.ua, Практичні / Семінарські: д.ф.-м.н., професор Клесов Олег Іванович, klesov@matan.kpi.ua*
Розміщення курсу	

Програма навчальної дисципліни

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

Цілі дисципліни	Метою навчальної дисципліни є формування у студентів здатностей: – до необхідної інтуїції та ерудиції у питаннях застосування математики, виховання у аспірантів прикладної математичної культури; – використовувати методи лінійної алгебри, математичного аналізу, теорії ймовірностей у задачах мікроекономіки; – уміння аналізувати одержані результати, здатності до узагальнення, постановки цілі та вибору шляхів її розв'язання, володіння культурою мислення; – самостійно використовувати і вивчати літературу з математики та мікроекономіки, здатності до розвитку гнучкості мислення, творчої самостійності та дій.
Предмет навчальної дисципліни	Алгоритми обчислень підвищеної точності, програмне забезпечення обчислень з підвищеною точністю, алгоритми перевірки цілих чисел на простоту, дискретні логарифми, квантові алгоритми, сучасні алгоритми для криптографічних систем
Компетентності	ЗК1: Здатність проводити критичний аналіз, оцінку і синтез нових та складних ідей ЗК3: Здатність креативно (творчо) мислити, розробляти та реалізовувати проєкти, включаючи власні дослідження ЗК5: Здатність до пошуку, оброблення та аналізу інформації з різних джерел ФК1: Здатність самостійно виконувати науково-дослідну діяльність у галузі математики та статистики з використанням сучасних теорій, методів та інформаційно-комунікаційних технологій і дотриманням належної академічної доброчесності ФК2: Здатність адаптувати і узагальнювати результати сучасних досліджень в галузі математики та статистики для вирішення наукових і практичних проблем ФК3: Здатність проводити теоретичні й експериментальні дослідження, математичне й комп'ютерне моделювання для перевірки математичних гіпотез та отримання результатів ФК4: Здатність до оцінки адекватності математичної моделі об'єкту за допомогою аналітичного дослідження та імітаційного моделювання;
Програмні результати навчання	РН12Уміти 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 РН13 Уміти організовувати і проводити науково-дослідну, інноваційну та освітню діяльність в обраній науковій спеціальності – математиці та статистиці РН14 Уміти розв'язувати теоретичні та прикладні математичні проблеми з використанням базових знань математики та статистики та базових загальних знань з різних природничих та соціальних наук РН15 Уміти приймати рішення у своїй професійній діяльності, демонструвати авторитетність, високий ступінь самостійності

	РН17 Уміти адаптувати, інтерпретувати та узагальнювати результати сучасних математичних та статистичних досліджень для розв'язання теоретичних та прикладних проблем РН18 Володіти сучасними інформаційними технологіями, методами обробки та аналізу інформації для розв'язання математичних та статистичних проблем і прийняття рішень, здійснювати математичне моделювання з використанням комп'ютерних технологій

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

Освітній компонент "*Алгоритмична теорія чисел та квантові обчислення*" є одним із завершальних курсів професійної підготовки докторів філософії спеціальності "Математика".

Дисципліні передує вивчення курсу «*Перетворення Фур'є та характеристичні функції* (ПО3) та «*Філософські засади наукової діяльності*» (ЗО 1) і передує вивченню «*Організації науково-інноваційної діяльності*» (ПО 4).

3. Зміст навчальної дисципліни

Кредитний модуль включає наступні теми

Розділ 1. Алгоритми обчислень підвищеної точності

Тема 1.1. Обчислення з великими цілими числами

Тема 1.2. Арифметичні операції, які виконуються на комп'ютері з підвищеною точністю

Тема 1.3. Операції модульної арифметики, які виконуються на комп'ютері з підвищеною точністю

Тема 1.4. Алгоритми швидкого множення

Розділ 2. Програмне забезпечення обчислень з підвищеною точністю

Тема 2.1. Математична система Sage

Тема 2.2. Система компьютерної алгебри PARI/GP

Розділ 3. Алгоритми перевірки цілих чисел на простоту

Тема 3.1. Алгоритм перевірки цілих чисел на простоту за допомогою еліптичних кривих

Тема 3.2. Алгоритм АКС

Розділ 4. Дискретні логарифми

Тема 4.1. Обчислення дискретних логарифмів за допомогою еліптичних кривих

Тема 4.2. Метод Поліга-Хеллмана

Розділ 5. Квантові алгоритми

Тема 5.1. Квантовий алгоритм факторизації цілих чисел

Тема 5.2. Квантовий алгоритм обчислення дискретних логарифмів

Тема 5.3. Квантовий алгоритм розв'язання рівняння Пелля

Тема 5.4. Квантовий алгоритм перевірки гіпотези Рімана

Розділ 6. Сучасні алгоритми для криптографічних систем

Тема 6.1. RSA криптосистема на базі еліптичних кривих

Тема 6.2. Криптографічна система на базі квантових алгоритмів

Тема 6.3. Криптографічна система на базі алгоритму біологічного DNA

Заплановано **практичні заняття** для поглибленого вивчення окремих розділів курсу. На практичних заняттях аспіранти навчаються розв'язувати задачі з відповідних тем курсу.

4. Навчальні матеріали та ресурси

1. О.Н.Василенко Теоретико-числовые алгоритмы в криптографии, МЦНМО,М.,2006, 334с.

2. R.B.Ash, A PARI/GP Tutorial, 2007, 20 pp.
3. C.Finch, Sage: Beginners Guide, PACKT Publishing, 2011, 504 pp.
4. A. Das, Computational number theory, CRC Press, New York, 2013.
5. S. Dasgupta, C.H.Papadimitriou, U.V.Vazirani, Algorithms, 2006, McGraw-Hill, New York.
6. Shoup V. A computational introduction to number theory and algebra, Cambridge University Press, Cambridge, 2005, 517 pp.
7. S.Y.Yang, Computational number theory and modern cryptography, Wiley, New York, 2012, 432pp.
8. S.Y.Yang, Quantum computational number theory, Springer, Cham, 2015, 259 pp.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних матеріалів, посилання на літературу)
1.1	Обчислення з великими цілими числами *Рекомендована література*: [6], глава 3.
1.2.	Арифметичні операції, які виконуються на комп'ютері з підвищеною точністю *Рекомендована література*: [1], розділи 10.1-10.3.
1.3.	Операції модульної арифметики, які виконуються на комп'ютері з підвищеною точністю *Рекомендована література*: [1], розділ 10.4.
1.4.	Алгоритми швидкого множения *Рекомендована література*: [4], розділ 1.1.3; [5], глава 2.
2.1.	Математична система Sage *Рекомендована література*: [3]
2.2.	Система компьютерної алгебри PARI/GP *Рекомендована література*: [2], розділ 11.
3.1.	Алгоритм перевірки цілих чисел на простоту за допомогою еліптичних кривих *Рекомендована література*: [7], розділ 3.3.
3.2.	Алгоритм АКС *Рекомендована література*: [7], розділ 3.4.
4.1.	Обчислення дискретних логарифмів за допомогою еліптичних кривих *Рекомендована література*: [7], розділ 5.5.
4.2.	Метод Поліга-Хеллмана *Рекомендована література*: [7], розділ 5.3.
5.1.	Квантовий алгоритм факторизації цілих чисел *Рекомендована література*: [7], розділ 10.2.
5.2.	Квантовий алгоритм обчислення дискретних логарифмів *Рекомендована література*: [7], розділ 10.3.
5.3.	Квантовий алгоритм розв'язання рівняння Пелля *Рекомендована література*: [8], розділ 6.1.
5.4.	Квантовий алгоритм перевірки гіпотези Рімана *Рекомендована література*: [8], розділ 6.2.
6.1.	RSA криптосистема на базі еліптичних кривих *Рекомендована література*: [7], розділ 9.5.
6.2.	Криптографічна система на базі квантових алгоритмів *Рекомендована література*: [7], розділ 11.3.

6.3.	Криптографічна система на базі DNA *Рекомендована література*: [7], розділ 11.4.

5. Практичні заняття.

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1.1-1.4	**Алгоритми обчислень півищеної точності**. Завдання СРС: [1], [4], [6]
2.1-2.2	**Програмне забезпечення обчислень з підвищеною точністю** Завдання СРС: [2], [3]
3.1-3.2	**Алгоритми перевірки цілих чисел на простоту** Завдання СРС: [7]
4.1-4.2	**Дискретні логарифми** Завдання СРС: [7]
5.1-5.4	**Квантові алгоритми** Завдання СРС: [7], [8]
6.1-6.3	**Сучасні алгоритми для криптографічних систем** Завдання СРС: [7]
	МКР

6. Самостійна робота студента/аспіранта

Вивчення дисципліни включає наступні види самостійної роботи:

- підготовка до лекційних та практичних занять занять,
- виконання розрахунково-графічної роботи,
- виконання модульної контрольної роботи.
- підготовка до МКР та екзамену

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Рекомендовані методи навчання: вивчення основної та допоміжної літератури за тематикою лекцій, розв'язування задач на практичних заняттях та при виконанні домашніх робіт
Аспіранту рекомендується вести докладний конспект лекцій. Важливим аспектом якісного засвоєння матеріалу, відпрацювання методів та алгоритмів вирішення основних завдань дисципліни є самостійна робота. Вона містить читання літератури, огляд літератури за темою, підготовку до занять та до іспиту.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

На першому занятті здобувачі ознайомлюються із рейтинговою системою оцінювання (РСО) дисципліни, яка побудована на основі Положення про систему оцінювання результатів навчання https://document.kpi.ua/files/2020_1-273.pdf

Зокрема, рейтинг здобувача з освітнього компонента формується як сума балів поточної успішності навчання – стартового рейтингу (максимально **50** балів) та екзаменаційних балів (максимально **50** балів).

Поточний контроль: фронтальний (усний\письмовий), МКР; індивідуальне задвдання.

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу результати якого відображаються в системі Електронний кампус https://campus.kpi.ua.

Рейтингова система оцінювання включає всі види тестування: контрольні роботи, виконання індивідуального завдання, відповідь на екзамені. Кожний здобувач отримує свій підсумковий рейтинг по дисципліні.

Рейтинг здобувача з кредитного модуля складається з балів, які він отримує за:
- роботу на практичних заняттях
- написання модульної контрольної роботи;
- виконання індивідуального завдання (РГР);
- відповіді на екзамені (письмової екзаменаційної роботи).

Відповіді під час практичних занять

Ваговий бал 1 (може бути відкорегований в залежності від кількості запланованих занять)

- якщо задача повністю розв'язана, то здобувач отримує максимальну кількість запланованих балів;
- якщо відповідь правильна, але у розв'язку є неточності, то здобувач отримує 0,5 запланованих балів;
- якщо незадовільна відповідь, метод розв'язування задачі неправильний – 0 балів;

Максимальний бал 10.

Модульна контрольна робота

Ваговий бал 20

Критерії оцінювання
- повна відповідь на всі завдання (більше 90% матеріалу) 18 – 20 балів;
- неповна відповідь на завдання (від 50 до 90% матеріалу) - 10 – 17 балів;
- відповідь містить менше 50 % необхідної інформації – 0-9 балів;

Максимальний бал 20

Індивідуальне завдання (Розрахунково-графічна робота)

Ваговий бал 20

Критерії оцінювання
- повна відповідь на всі завдання (більше 90% матеріалу) 18 – 20 балів;
- неповна відповідь на завдання (від 50 до 90% матеріалу) - 10 – 17 балів;
- відповідь містить менше 50 % необхідної інформації – 0-9 балів;

Виконання РГР може бути замінено на підготовку тез на наукову конференцію.

Максимальний бал 20

Умови допуску до екзамену.

Умовою допуску до екзамену є стартовий рейтинг не менше 30 балів. Здобувач, який в кінці навчального семестру мають менше балів до екзамену не допускаються і повинні виконати додаткові завдання до першого перескладання.

Форма семестрового контролю – іспит

На екзамені студенти виконують письмову контрольну роботу. Кожне завдання містить два теоретичних запитання (завдання) і одне практичне. Кожне теоретичне запитання (завдання) оцінюється у 15 балів, а практичне у 20 балів за такими критеріями:

– «відмінно», повна відповідь, не менше 90% потрібної інформації, що виконана згідно з вимогами до рівня «умінь», (повне, безпомилкове розв'язування завдання) – 14-15; 18-20 балів;

– «добре», достатньо повна відповідь, не менше 75% потрібної інформації, що виконана згідно з вимогами до рівня «умінь» або є незначні неточності (повне розв'язування завдання з незначними неточностями) – 11-13; 16-17 балів;
– «задовільно», неповна відповідь, не менше 60% потрібної інформації, що виконана згідно з вимогами до рівня «умінь» та деякі помилки (завдання виконане з певними недоліками) – 9-10; 10-15 балів
– «незадовільно», відповідь не відповідає умовам до «задовільно» – 0 балів.

Сума стартових балів та балів за екзамен переводиться до екзаменаційної оцінки згідно з таблицею:

100…95	Відмінно
94…85	Дуже добре
84…75	Добре
74…65	Задовільно
64…60	Достатньо
Менше 60	Незадовільно
Стартовий рейтинг менше 30 балів	Не допущено

У випадку дистанційної форми навчання у РСО відбуваються наступні зміни:

- Контрольні заходи проводяться дистанційно із застосуванням електронної пошти, Telegram, Zoom та освітньої платформи Moodle, зокрема у вигляді тестових контрольних робіт.
- Максимальну суму вагових балів контрольних заходів протягом семестру R_C встановлюється на рівні 50 балів.
- Допусковий бал до екзамену R_D встановлюється на рівні 30 балів.
- Сума балів R_I, набрана протягом семестру згідно затвердженого РСО, повідомляється на останньому практичному занятті.
- У разі не отримання студентом допускового балу, йому надається можливість підвищити R_I шляхом проведення додаткових контрольних заходів до допускового
- Рівень набуття передбачених навчальною програмою компетентностей визначається на підставі проведених заходів поточного контролю.
- Екзаменаційна оцінка може бути виставлена «автоматом» за формулою шляхом перерахунку стартових балів за 100-бальною шкалою:

$$R = 60 + \frac{40(R_I - R_D)}{R_C - R_D}.$$

Переводиться до екзаменаційної оцінки згідно з таблицею

100…95	Відмінно
94…85	Дуже добре
84…75	Добре
74…65	Задовільно
64…60	Достатньо
Менше 60	Незадовільно

Робочу програму навчальної дисципліни (силабус):

Складено проф. Клесовим О.І.

Ухвалено кафедрою математичного аналізу та теорії ймовірностей (протокол № 1 від 27.08.2020 р.)

Погоджено Методичною комісією ФМФ (протокол № 1 від 02.09.2020 р.)