Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра комп'ютерної фізики

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

_____ Олександр ГОЛОВКО

"30" серпня 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНТЕРАКТИВНІ ДОКАЗИ ТА КВАНТОВІ ОБЧИСЛЕННЯ

рівень вищої освіти	другий (магістерський)
галузь знань	10 Природничі науки
спеціальність	105 Прикладна фізика та наноматеріали
освітня програма	«Комп'ютерна фізика»
вид дисципліни	обов'язкова

навчально – науковий інститут комп'ютерної фізики та енергетики

2022 / 2023 навчальний рік

Програму рекомендовано до затвердження вченою радою навчально-наукового інституту комп'ютерної фізики та енергетики

26 серпня 2022 року, протокол № 8/22

РОЗРОБНИКИ ПРОГРАМИ:
Лісін Денис Олександрович, к.т.н., доцент каф. комп'ютерної фізики

Програму схвалено на засіданні кафедри комп'ютерної фізики

Протокол від 26 серпня 2022 року № 8/22

Завідувач кафедри комп'ютерної фізики

_____ Костянтин НЄМЧЕНКО

Програму погоджено з гарантом освітньо-наукової програми «Комп'ютерна фізика»

Гарант освітньо-наукової програми «Комп'ютерна фізика»

_____ Костянтин НЄМЧЕНКО

Програму погоджено науково-методичною комісією
навчально-наукового інституту комп'ютерної фізики та енергетики

Протокол від 26 серпня 2022 року № 8/22

Голова науково-методичної комісії
навчально-наукового інституту комп'ютерної фізики та енергетики

_____ _____ Ольга ЛІСІНА

ВСТУП

Програма навчальної дисципліни «Інтерактивні докази та квантові обчислення» складена відповідно до освітньо-наукової програми підготовки магістрів

спеціальності 105 Прикладна фізика та наноматеріали

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є дати уявлення про основні сучасні підходи до квантових обчислень, систем інтерактивних доказів, систем ймовірносно перевіряємих доказів.

1.2. Основні завдання вивчення дисципліни

- вивчення основних підходів до квантових обчислень, систем інтерактивних доказів, систем ймовірносно перевіряємих доказів;
- практичне застосування основних методів і алгоритмів, які використовуються у цих підходах.

1.3. Кількість кредитів 5

1.4. Загальна кількість годин 150 год.

1.5. Характеристика навчальної дисципліни	
Обов’язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	-й
Семестр	
1-й	-й
Лекції	
32 год.	год.
Практичні, семінарські заняття	
32 год.	год.
Лабораторні заняття	
0 год.	год.
Самостійна робота	
86 год.	год.
у тому числі індивідуальні завдання	
0 год.	

1.6. Заплановані результати навчання

Згідно з вимогами освітньо-наукової програми, студенти мають досягти таких результатів навчання:

знати:

- основні класи, які стосуються систем інтерактивних доказів, систем ймовірносно перевіряємих доказів, квантових обчислень;
- основні алгоритми, які використовуються у вищеозначених системах

вміти:

- формувати системи інтерактивних доказів, ймовірносно перевіряємих доказів тощо для заданих задач

- створювати базові квантові алгоритми

Програмні результати навчання за освітньою програмою:

1. ПРН1. Використовувати знання в галузі прикладної фізики, математики, електроніки та інформаційних технологій для виконання наукових досліджень та розв'язання виробничих задач.
2. ПРН3. Обговорювати та знаходити прогресивні та інноваційні рішення проблем і завдань при виконанні науково-технічних та виробничих проектів.
3. ПРН8. Вміти розроблювати гіпотези та запропоновувати способи їх перевірки за допомогою відповідних аналітичних, експериментальних та чисельних інструментів

2. Тематичний план навчальної дисципліни

Розділ 1. Ймовірнісні обчислення

Тема 1. Методи Монте-Карло, Лас Вегас. Ймовірнісні класи. Ампліфікація. Теорема Ейдельмана. Теорема Гача-Сіпсера. Проблема P=?BPP

Тема 2. Дерандомізація. Метод умовних математичних очікувань. Проблеми MAXCUT та MAX3SAT. Метод попарно незалежних випадкових величин. Теорема Hardness vs Randomness.

Тема 3. Задачі підрахунку. Теорема про зв'язок рівностей P=PP та FP=#P. #P – повнота. Задача про перманент. Теорема Веліанта.

Розділ 2. Системи інтерактивних доказів

Тема 4. Клас IP. Інтерактивна система для неізоморфізма графів. Загальні монетки та клас AM. Деякі властивості IP та AM.

Тема 5. IP=PSPACE. Арифметизація. Інтерактивний протокол для #SATD. Протокол перевірки суми. Інтерактивний протокол для TQBF.

Тема 6. Системи інтерактивних доказів з нульовим розголошенням. Класи ZKP, CZKP,PZKP,SZKP.

Тема 7. Раціональні інтерактивні докази.Одноразундові докази. Багатораундові докази.

Розділ 3. Ймовірносно перевіряємі докази

Тема 8. Клас PCP. Наближений розв'язок NP-складних задач. PCP-теорема. Трибітна теорема Хестеда.

Тема 9. Експоненційна PCP-теорема. Коди Уолша-Адамара.

Розділ 4. Квантові обчислення

Тема 10. Квантова механіка. Квантова заплутаність. ЕПР-парадокс. Квантові обчислення. Криптографія.

Тема 11. Квантові алгоритми. Алгоритм Шора. Алгоритм Гровера.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Ймовірнісні обчислення												
Тема 1. Методи Монте-Карло, Лас Вегас. Ймовірнісні	16	3	3			10						

класи. Ампліфікація. Теорема Ейдельмана. Теорема Гача-Сіпсера. Проблема P=?BPP												
Тема 2. Дерандомізація. Метод умовних математичних очікувань. Проблеми MAXCUT та MAX3SAT. Метод попарно незалежних випадкових величин. Теорема Hardness vs Randomness.	16	3	3			10						
Тема 3. Задачі підрахунку. Теорема про зв'язок рівностей P=PP та FP=#P. #P – повнота. Задача про перманент. Теорема Веліанта.	14	2	2			10						
Разом за розділом 1	46	8	8			30						
Розділ 2. Системи інтерактивних доказів												
Тема 4. Клас IP. Інтерактивна система для неізоморфізма графів. Загальні монетки та клас AM. Деякі властивості IP та AM.	11	2	2			7						
Тема 5. IP=PSPACE. Арифметизація. Інтерактивний протокол для $\#SAT_D$. Протокол перевірки суми. Інтерактивний протокол для TQBF.	11	2	2			7						
Тема 6. Раціональні інтерактивні докази.Одноразундові докази. Багаторазундові докази.	12	2	2			7						
Тема 7. Раціональні інтерактивні докази.Одноразундові докази.	12	3	3			7						

Багатораундові докази.												
Разом за розділом 2	46	9	9			28						
Розділ 3. Ймовірносно перевіряємі докази												
Тема 8. Клас PCP. Наближений розв'язок NP-складних задач. PCP-теорема. Трибітна теорема Хестеда.	15	4	4			7						
Тема 9. Експоненційна PCP-теорема. Коди Уолша-Адамара.	15	4	4			7						
Разом за розділом 3	30	8	8			14						
Розділ 4. Квантові обчислення												
Тема 10. Квантова механіка. Квантова заплутаність. ЕПР-парадокс. Квантові обчислення. Криптографія.	11	3	3			6						
Тема 11. Квантові алгоритми. Алгоритм Шора. Алгоритм Гровера.	15	4	4			6						
Разом за розділом 4	28	7	7			14						
Усього годин	150	32	32			86						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Методи Монте-Карло, Лас Вегас.	4
2	Метод попарно незалежних випадкових величин.	4
3	Інтерактивна система для неізоморфізма графів.	4
4	Інтерактивний протокол для TQBF.	4
5	Системи інтерактивних доказів з нульовим розголошенням.	4
6	Раціональні інтерактивні докази.	4
7	Наближений розв'язок NP-складних задач.	4
8	Алгоритм Шора. Алгоритм Гровера.	4
	Разом	32

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Вивчити методи Монте-Карло, Лас Вегас. Ймовірнісні класи. Ампліфікація.	5

2	Ознайомитись з теоремою Ейдельмана, теорема Гача-Сіпсера. Проблемою P=?BPP	5
3	Опрацювати розділи:Дерандомізація. Метод умовних математичних очікувань. Проблеми MAXCUT та MAX3SAT.	5
4	Вивчити метод попарно незалежних випадкових величин та теорему Hardness vs Randomness.	5
5	Опрацювати розділи:Задачі підрахунку. Теорема про зв'язок рівностей P=PP та FP=#P.	6
6	Опрацювати розділи: #P – повнота. Задача про перманент. Теорема Веліанта.	6
7	Опрацювати розділи: Клас IP. Інтерактивна система для неізоморфізма графів. Загальні монетки та клас AM. Деякі властивості IP та AM.	6
8	Опрацювати розділи: IP=PSPACE. Арифметизація. Інтерактивний протокол для #SATD.	6
9	Ознайомитись із протоколом перевірки суми та інтерактивним протоколом для TQBF.	6
10	Опрацювати розділи: Системи інтерактивних доказів з нульовим розголошенням. Класи ZKP, CZKP,PZKP,SZKP.	6
11	Опрацювати розділи: Раціональні інтерактивні докази.Одноразундові докази. Багатораундові докази.	6
12	Опрацювати розділи: Клас PCP. Наближений розв'язок NP-складних задач. PCP-теорема. Трибітна теорема Хестеда.	6
13	Опрацювати розділи: Експоненційна PCP-теорема. Коди Уолша-Адамара.	6
14	Опрацювати розділи: Квантова механіка. Квантова заплутаність. EPR-парадокс. Квантові обчислення. Криптографія.	6
15	Опрацювати розділи: Квантові алгоритми. Алгоритм Шора. Алгоритм Гровера.	6
	Разом	86

6. Індивідуальні завдання

Не передбачено

7. Методи навчання

Лекції викладаються методом проблемного викладення. Використовуючи будь-які джерела й засоби, лектор, перш ніж викладати матеріал, ставить проблему, формулює пізнавальне завдання, а потім, розкриваючи систему доведень, порівнюючи погляди, різні підходи, показує спосіб розв'язання поставленого завдання. Студенти стають ніби свідками і співучасниками наукового пошуку. Лабораторні заняття ведуться дослідницьким методом.

Лекції викладаються методом проблемного викладення. Використовуючи будь-які джерела й засоби, лектор, перш ніж викладати матеріал, ставить проблему, формулює пізнавальне завдання, а потім, розкриваючи систему доведень, порівнюючи погляди, різні підходи, показує спосіб розв'язання поставленого завдання. Студенти стають ніби свідками і співучасниками наукового пошуку. Лабораторні заняття ведуться дослідницьким методом.

- Пояснювально-ілюстративний метод (викладання лекційного, пояснювального практичного матеріалів, Zoom-конференції);
- Проблемні методи (розв'язання проблемних задач, дискусії, самостійне вивчення літератури студентами, Zoom-конференції);
- Репродуктивний метод (виконання завдань на базі зразка, система Moodle).

8. Методи контролю

На заняттях – опитування, програмування у системі MATLAB. По закінченні модуля – модульний контроль. Форма підсумкового контролю знань – іспит.

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання					Іспит	Сума
Р1	Р2	Р3	Р4	Контрольні роботи, передбачені навчальним планом		
10	10	10	10	2*10	40	100

Р1, Р2, Р3 – теми розділів.

Передбачаються бали за:

- експрес-контроль на лекції – 10;
- виконання контрольних робіт – 20;
- виконання практичних робіт - 30
- іспит – 40 балів.

Критерії оцінювання навчальних досягнень

Загальна максимальна бальна оцінка за екзамен складатиме 40 балів. Мінімальний підсумковий бал складатиме 50 балів, а максимальний – 100 балів. Підсумкова оцінка визначається шляхом переводу підсумкового балу з дисципліни у традиційну академічну оцінку національної шкали ("відмінно", "добре", "задовільно", "незадовільно" за шкалою, що наведено у попередньому пункті робочої програми.

Загальна максимальна бальна оцінка за екзамен складатиме 40 балів. Мінімальний підсумковий бал складатиме 50 балів, а максимальний – 100 балів. Підсумкова оцінка визначається шляхом переводу підсумкового балу з дисципліни у традиційну академічну оцінку національної шкали ("відмінно", "добре", "задовільно", "незадовільно" за шкалою:

— “відмінно" (90 та вище балів) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії;

— “добре" (82-89 балів) заслуговує студент, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності;

— "добре" (70-81 балів) заслуговує студент, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності;

— "задовільно" (61-69 балів) заслуговує студент, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка “задовільно” виставляється студентам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;

— "задовільно" (50-60 балів) заслуговує студент, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка "достатньо" виставляється студентам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача.
— "незадовільно" (40-49 балів) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.
— "незадовільно" (1-39 балів) виставляється студенту коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.
При виставленні оцінки можуть враховуватися результати навчальної роботи студента протягом семестру.

Схема нарахування балів на іспиті.

Кожне питання екзаменаційного білету оцінюється наступним чином (максимальна кількість балів за питання - 5):

5 балів – студент повністю відповів на питання;
4 балів – у загалому правильна відповідь, робота з певною кількістю помилок ;
3 балів - відповів на питання, але з великою кількістю недоліків;
2 балів – допущені грубі помилки у відповіді, але студент частково володіє необхідними знаннями;
1 балів - студент відповів на питання з грубими помилками та продемонстрував відсутність володіння базовими знаннями;
0 балів – студент зовсім не відповів на питання.

Кожна задача екзаменаційного білету оцінюється наступним чином (максимальна кількість балів за питання - 15):

15 балів – студент повністю розв'язав задачу без помилок;
10 балів – у загальному правильний розв'язок з певною кількістю незначних помилок ;
5 балів – розв'язав задачу за правильним алгоритмов, але з великою кількістю недоліків;
1 балів – студент позначив хід розв'язання задачі, але не вирішив її;
0 балів – студент зовсім не розв'язав задачу.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	не зараховано

10. Рекомендована література

Наочні матеріали надаються з використанням ПЕОМ та проекційного устаткування у спеціально обладнаних аудиторіях.

Основна література

1. Arora, Sanjeev; Barak, Boaz - Computational Complexity: A Modern Approach
2. Christos H. Papadimitriou. Computatational Complexity. Addison-Wesley, Reading, Mass., 1994
3. Russell Impagliazzo. A personal view of average-case complexity. In Structure in Complexity Theory Conference, pages 134–147, 1995.
4. S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In S. Micali, editor, Randomness and Computation. JAI Press, Greenwich, CT, 1987. Extended Abstract in Proc. 18th ACM Symp. on Theory of Computing, 1986.
5. Oded Goldreich. Computational Complexity: A Conceptual Perspective

11. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Мережа Internet.
2. Бібліотеки ХНУ ім. В.Н.Каразіна.