Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра інформаційних технологій в фізико-енергетичних системах

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

_____ Антон ПАНТЕЛЕЙМОНОВ

"___" _____ 2021 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 нанометаріали
освітня програма	«Прикладна фізика енергетичних систем»
вид дисципліни	за вибором
ННІ	комп'ютерної фізики та енергетики

2021 / 2022 навчальний рік

ВСТУП

Програма навчальної дисципліни «Інтерактивні докази та квантові обчислення» складена відповідно до освітніх програм підготовки **магістрів**

спеціальність: 105 Прикладна фізика та наноматеріали

освітні програми: «Прикладна фізика енергетичних систем»

1. Опис навчальної дисципліни

1.1. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни є дати уявлення про основні сучасні підходи до квантових обчислень, систем інтерактивних доказів, систем ймовірносно перевіряємих доказів. Курс охоплює такі розділи комп'ютерних та математичних наук: складність обчислень, теорія обчислюваності, теорія графів, теорія ймовірності, обчислення у скінчених полях.

1.2. Основними завданнями вивчення дисципліни є:
- 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

2. Опис навчальної дисципліни

1.5. Характеристика навчальної дисципліни	
за вибором	
Вид кінцевого контролю : семестровий екзамен	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	-й
Семестр	
1-й	-й
Лекції	
16 год.	год.
Практичні, семінарські заняття	
16 год.	год.

Лабораторні заняття	
год.	год.
Самостійна робота	
118 год.	год.
у тому числі індивідуальні завдання	
год.	

1.6. Заплановані результати навчання. Згідно з вимогами освітньо-професійної 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

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 $\#SAT_D$. 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.Однораундові 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 змістових модулів 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
Змістовий модуль 1. Ймовірнісні обчислення												
Тема 1. Методи Монте-Карло, Лас Вегас. Ймовірнісні класи. Ампліфікація. Теорема Ейдельмана. Теорема Гача-Сіпсера. Проблема P=?BPP		2	2			17						
Тема 2. Дерандомізація. Метод умовних математичних очікувань. Проблеми MAXCUT та MAX3SAT. Метод попарно незалежних випадкових величин. Теорема Hardness vs Randomness.		2	2			17						
Разом за розділом 1	42	4	4			34			-	-	-	
Розділ 2. Системи інтерактивних доказів												
Тема 3. Клас IP. Інтерактивна система для неізоморфізма графів. Загальні монетки та клас AM. Деякі властивості IP та AM.		2	2			17						
Тема 4. IP=PSPACE. Арифметизація. Інтерактивний протокол для $\#SAT_D$. Протокол перевірки суми. Інтерактивний протокол для TQBF.		2	2			17						
Тема 5. Раціональні інтерактивні докази.Одноразундові докази. Багатораундові докази.		2	2			17						

Разом за розділом 2	63	6	6			51			-	-	-	
Розділ 3. Квантові обчислення												
Тема 6. Квантова механіка. Квантова заплутаність. ЕПР-парадокс. Квантові обчислення. Криптографія.		3	3			17						
Тема 7. Квантові алгоритми. Алгоритм Шора. Алгоритм Гровера.		3	3			16						
Разом за розділом 3	45	6	6			33			-	-	-	
Усього годин	150	16	16			118						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Методи Монте-Карло, Лас Вегас.	**2**
2	Метод попарно незалежних випадкових величин.	**2**
3	Інтерактивна система для неізоморфізма графів.	**2**
4	Інтерактивний протокол для TQBF.	**2**
5	Системи інтерактивних доказів з нульовим розголошенням.	**2**
6	Раціональні інтерактивні докази.	**2**
7	Наближений розв’язок NP-складних задач.	**2**
8	Алгоритм Шора. Алгоритм Гровера.	**2**
Усього		**16**

5. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Вивчити методи Монте-Карло, Лас Вегас. Ймовірнісні класи. Ампліфікація.	**8**
2	Ознайомитись з теоремою Ейдельмана, теорема Гача-Сіпсера. Проблемою P=?BPP	**8**
3	Опрацювати розділи:Дерандомізація. Метод умовних математичних очікувань. Проблеми MAXCUT та MAX3SAT.	**8**
4	Вивчити метод попарно незалежних випадкових величин та теорему Hardness vs Randomness.	**8**
5	Опрацювати розділи:Задачі підрахунку. Теорема про зв’язок рівностей P=PP та FP=#P.	**8**
6	Опрацювати розділи: #P – повнота. Задача про перманент. Теорема Веліанта.	**8**
7	Опрацювати розділи: Клас IP. Інтерактивна система для неізоморфізма графів. Загальні монетки та клас AM. Деякі властивості IP та AM.	**8**
8	Опрацювати розділи: IP=PSPACE. Арифметизація. Інтерактивний протокол для $\#SAT_D$.	**8**
9	Ознайомитись із протоколом перевірки суми та інтерактивним протоколом для TQBF.	**8**

10	Опрацювати розділи: Системи інтерактивних доказів з нульовим розголошенням. Класи ZKP, CZKP,PZKP,SZKP.	**8**
11	Опрацювати розділи: Раціональні інтерактивні докази.Одноразундові докази. Багатораундові докази.	**8**
12	Опрацювати розділи: Клас PCP. Наближений розв'язок NP-складних задач. PCP-теорема. Трибітна теорема Хестеда.	**8**
13	Опрацювати розділи: Експоненційна PCP-теорема. Коди Уолша-Адамара.	**8**
14	Опрацювати розділи: Квантова механіка. Квантова заплутаність. EPR-парадокс. Квантові обчислення. Криптографія.	**8**
15	Опрацювати розділи: Квантові алгоритми. Алгоритм Шора. Алгоритм Гровера.	**6**
Усього		**118**

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).

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.

Передбачаються бали за:

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

Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

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	Контрольні роботи, передбачені навчальним планом		
10	15	15	2*10	40	100

Р1, Р2, Р3 – теми розділів.

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 за національною шкалою	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	не зараховано

9. Рекомендована література

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

Базова література

1. Берж К. Теория графов и ее применения. --- М.: Изд-во иностр. лит., 1962.
2. Зыков А.А. Основы теории графов. --- М.: Наука, 1984.
3. Кнут Д. Искусство программирования для ЭВМ. Т. 3. Сортировка и поиск. --- М.: Мир, 1978.
4. Кристофидес Н. Теория графов. Алгоритмический подход. --- М.: Мир, 1978.
5. Оре О. Теория графов. --- М.: Наука, 1968.
6. Скворцов А.В. Триангуляция Делоне и ее применение. --- Издательство Томского университета, 2002.
7. Препарата Ф., Шеймос М. Вычислительная геометрия: Введение / Пер. с англ. М.: Мир, 1989. 478 с.
8. Роджерс Д., Адамс Дж. Математические основы машинной графики / Пер. с англ. М.: Машиностроение, 1980. 204 с.

Інформаційні ресурси

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