МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра фундаментальной и прикладной математики

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КВАНТОВАЯ КРИПТОГРАФИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Математика информационных сред

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КВАНТОВАЯ КРИПТОГРАФИЯ
Рабочая программа дисциплины

Составитель:
Канд. физ.-мат.наук, доцент кафедры фундаментальной и прикладной математики
Викторова Н.Б.

УТВЕРЖДЕНО
Протокол заседания кафедры
фундаментальной и прикладной математики
№ 10 от 05.04.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: овладение студентами-математиками основами квантовой механики и квантовых вычислений, и умением применять такие знания для решения задач практических вычислений.
Задачи дисциплины: научить применять знания по основам квантовой механике для решения задач практических вычислений.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-3. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей	ПК-3.2. Рассматривает социотехнические системы как сложные информационные системы для создания моделей разного типа.	*Знать:* основы нерелятивистской квантовой теории одной и нескольких частиц, принципы вычислений и обработки информации, содержащихся в квантовых ансамблях; *Уметь:* построить алгоритм, реализующий стандартные информационные процессы над квантовыми ансамблями (унитарная эволюция, измерение и частичное измерение, вычисление запутанности, телепортация, квантовые вентили), реализовать компьютерную модель этого процесса и оценить его сложность, построить математическую и программную модель реального процесса для нескольких заряженных частиц во внешнем потенциале, в частности, реализующую стандартные квантовые вентили, и сделать практические выводы по ней (время срабатывания, добротность, возможность масштабирования); *Владеть:* реализацией вычислительных алгоритмов с применением стандартных квантовых вентилей, вычислением стандартных физических величин (энергии, координат, импульса, момента), а также вероятностных распределений для заданных квантовых состояний простых ансамблей из нескольких частиц во внешнем потенциале
	ПК-3.3. Выделяет информационные потоки, определяет точки бифуркаций.	*Знать:* основы нерелятивистской квантовой теории одной и нескольких частиц, принципы вычислений и обработки информации, содержащихся в квантовых ансамблях; *Уметь:* построить алгоритм, реализующий стандартные информационные процессы над квантовыми ансамблями (унитарная эволюция, измерение и частичное измерение, вычисление запутанности, телепортация, квантовые вентили), реализовать компьютерную модель этого процесса и оценить его сложность, построить математическую и программную модель реального процесса для нескольких заряженных частиц во внешнем потенциале, в частности,

		реализующую стандартные квантовые вентили, и сделать практические выводы по ней (время срабатывания, добротность, возможность масштабирования); *Владеть:* реализацией вычислительных алгоритмов с применением стандартных квантовых вентилей, вычислением стандартных физических величин (энергии, координат, импульса, момента), а также вероятностных распределений для заданных квантовых состояний простых ансамблей из нескольких частиц во внешнем потенциале
	ПК-3.4. Строит математические модели различных типов, исследует их.	*Знать:* основы нерелятивистской квантовой теории одной и нескольких частиц, принципы вычислений и обработки информации, содержащихся в квантовых ансамблях; *Уметь:* построить алгоритм, реализующий стандартные информационные процессы над квантовыми ансамблями (унитарная эволюция, измерение и частичное измерение, вычисление запутанности, телепортация, квантовые вентили), реализовать компьютерную модель этого процесса и оценить его сложность, построить математическую и программную модель реального процесса для нескольких заряженных частиц во внешнем потенциале, в частности, реализующую стандартные квантовые вентили, и сделать практические выводы по ней (время срабатывания, добротность, возможность масштабирования); *Владеть:* реализацией вычислительных алгоритмов с применением стандартных квантовых вентилей, вычислением стандартных физических величин (энергии, координат, импульса, момента), а также вероятностных распределений для заданных квантовых состояний простых ансамблей из нескольких частиц во внешнем потенциале

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Квантовые вычисления и квантовая криптография» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Линейная алгебра», «Дифференциальное и интегральное исчисление», «Теория вероятностей», «Общая алгебра и теория чисел», «Функциональный анализ», «Математические основы современной физики».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Теория кодирования», «Конечные поля и их приложения к криптографии», «Элементы p-адического анализа и его приложения к криптографии», Производственная практика (Научно-исследовательская работа).

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа (ов).

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**24**
7	Практические занятия	**32**
	Всего:	**56**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 88 академических часа(ов).

3. Содержание дисциплины

Раздел 1. Обзор математических методов квантовой физики

Тема 1. Обзор основных экспериментов по квантовой механике

Предмет квантовой механики. Корпускулярно-волновой дуализм при определении света. Эксперимент с пулеметной стрельбой. Эксперимент с волнами. Дифракция. Эксперимент с электронами. Корпускулярно-волновой дуализм в поведении электрона. Интерференция. Наблюдение за электроном. Принцип неопределенности Гейзенберга.

Тема 2. Обзор математического аппарата квантовой механики

Свет. Частота света. Фотоны. Фотоумножитель, как пример того, что свет состоит из частиц. Частичное отражение света от поверхности стекла. Амплитуда вероятности. Метод стрелок. Результирующая стрелка. Интерференция амплитуд. Вероятность события как квадрат длины амплитуды. Отражение света от зеркала. Прохождение света из воздуха в воду. Фокусирующая линза. Электроны и их взаимодействие. Амплитуда фотона P(a-b). Амплитуда электрона E(a-b). Амплитуда того, что электрон испустит или поглотит фотон. Рассеяние света. Античастицы. Принцип запрета.

Раздел 2. Алгебраический аппарат квантовой информатики

Тема 3. **Элементы линейной алгебры**

Векторное пространство. Координаты вектора в разных базисах. Матрица перехода.

Евклидово пространство. Унитарное пространство. Линейные операторы. Матрица линейного оператора. Формула преобразования матрицы оператора при преобразовании базиса. Собственное число и собственный вектор линейного оператора**.** Линейный оператор в комплексном пространстве со скалярным произведением. Сопряженный оператор. Матрица сопряженного оператора. Самосопряженный оператор. Эрмитова матрица. Унитарный оператор. Унитарная матрица. Свойства самосопряженного оператора. Свойства унитарного оператора. Приведение матрицы линейного оператора к диагональному виду. Приведение произвольной эрмитовой матрицы к диагональному виду с помощью унитарной матрицы перехода. Теорема о связи унитарной матрицы U и эрмитовой матрицы H (U=exp(iH)). Тензорное произведение линейных пространств. Тензорное произведение операторов. Тензорное произведение матриц. Оператор Уолша - Адамара.

Раздел 3. Элементы квантовой механики.

Тема 4. Эволюция вектора квантового состояния

Пространство классических состояний. Пространство квантовых состояний. Дискретное представление пространства состояний. Дискретное представление волнового вектора. Виды эволюции вектора состояния: унитарная динамика и измерение. Понятие коллапса волнового вектора. Измерение квантового состояния. Правило Макса Борна. Кет-вектор |Ψ> и бра-вектор <Ψ| (символика Дирака). Унитарная динамика. Уравнение Шредингера относительно вектора |Ψ>. Решение уравнения Шредингера - эволюция вектора состояния во времени |Ψ(t) >=exp(-iHt) |Ψ(0)>. Линейность эволюции. Решение уравнение Шредингера для одномерных потенциалов, одно- и двух- ямного потенциала,. Матрица плотности Ландау. Частичное измерение и частичная матрица плотности. Смешанные состояния. Проекторы. Открытые квантовые системы. Декогерентность.

Тема 5. Применение тензорного произведения

Тензорное произведение пространств, квантовых состояний и операторов. Незапутанные и запутанные состояния. Физический смысл запутанности и ее связь со сложностью вычислений.

Тема 6. Соответствие физических величин эрмитовым операторам.

Операторы координат, импульса, энергии, момента импульса. Собственные значения и допустимые значения физической величины. Собственные состояния. Примеры: координаты, импульс, энергия, момент. Дельта-функция Дирака и координатный базис.

Раздел 4. Квантовый компьютер

Тема 7. Квантовый компьютер

Вычисление с оракулом на классическом компьютере. Квантовый компьютер и квантовое вычисление. Квантовый оракул. Пример: задача перебора. Квантовые вентили: однокубитные, CNOT, Toffoli, фазовращатель. Квантовые схемы из функциональных элементов. Методы работы с анциллами. Квантовая чистка анцилл. Понятие квантового ускорения. Алгоритм Гровера для переборной задачи. Геометрический смысл алгоритма Гровера. Типичность гроверовского ускорения. Понятие о нижних оценках квантовой сложности. NP- задачи и квантовые вычисления. Алгоритм Залки-Визнера моделирования унитарной квантовой динамики. Понятие о квантовом моделировании систем многих частиц. Приложения квантовых вычислений: схема телепортации неизвестного квантового состояния. Запрет на клонирование квантовых состояний.

Раздел 5. Элементы квантовой криптографии

Тема 8. Элементы квантовой криптографии

О задаче секретной передачи данных. Задача распространения секретного ключа. Исторические способы шифрования данных. Криптографические протоколы. Симметричные шифры. Стойкость криптосистемы. Теорема Шеннона. Использование псевдослучайных генераторов. Криптосистемы с открытым ключом. Алгоритм RSA. Алгоритм Шора факторизации больших чисел. Квантовые коды коррекции ошибок. Протокол BB84.

4. Образовательные технологии

Для проведения *занятий лекционного типа* по дисциплине применяются такие образовательные технологии как лекция-дискуссия.

Для проведения *практических занятий* используются такие образовательные технологии как: дискуссия, решение и обсуждение вопросов и задач.

В рамках *самостоятельной работы* студентов проводится консультирование и проверка домашних заданий посредством электронной почты.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и

дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- опрос	1 балл	22 балла
- теоретический коллоквиум 1	38 баллов	38 баллов
Промежуточная аттестация – зачет с оценкой (коллоквиум 2)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне –

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		«высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Примерные вопросы к теоретическому коллоквиуму 1

1. Конфигурационное и гильбертово пространство состояний квантовой системы.

2. Координатный и импульсный базисы гильбертова пространства состояний. Дельта- функция Дирака.

3. Измерение волнового вектора. Матрица плотности Ландау. Частичная матрица плотности и ее вычисление. Дискретный и непрерывный варианты.

4. Операторы координат, энергии, импульса, момента импульса. Соответствующие им наблюдаемые и их эрмитовость. Унитарный оператор эволюции. Пример: координата и импульс.

5. Уравнение Шредингера и его общее решение. Проблема квантового компьютера. Решение уравнения Шредингера для одномерного случая (одна и две ямы). Атом водорода.

Промежуточная аттестация (зачет с оценкой)

Примерные вопросы для коллоквиума 2

1. Пространство волновых функций. Квантовое состояние. Обозначения Дирака.
2. Бит. Кубит.
3. Правило Борна. Измерение.
4. Уравнение Шредингера.
5. Тензорное произведение.
6. Запутанные и незапутанные квантовые состояния.
7. Квантовые вентили.
8. Матрица плотности Ландау.
9. Оператор координаты и импульса.
10. Одновременно измеримые физические величины
11. Преобразование Фурье.
12. Квантовый компьютер. Абстрактная схема.
13. Квантовое вычисление. Оракул и его квантовый вариант.
14. Сложность квантового вычисления. Квантовое ускорение и его примеры.
15. Алгоритм Гровера для решения переборной задачи. Инверсии относительно нуля и целевого состояния. Геометрический смысл.

Примерные задачи для коллоквиума 2

1. а) найти тензорное произведение операторов Паули сигма-x и сигма-z.
   б) вычислить экспоненту оператора Паули сигма-y.
   в) найти собственные состояния оператора импульса.

2. а) найти частичную матрицу плотности первого кубита для состояния |00> - |01> - |10> +|11>.
   б) решить уравнение Шредингера для гамильтониана, равного матрице Адамара.
   в) можно ли одновременно с одинаковой точностью измерить наблюдаемые: проекция момента на ось x и импульс. Ответ обосновать.

3. а) реализовать алгоритм Гровера, используя только однокубитные вентили и оператор Toffoli.
   б) выписать последовательные шаги алгоритма Гровера при работе над функцией f(x,y) = xy.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Хренников А. Ю. Введение в квантовую теорию информации / А. Ю. Хренников. - М.: Физматлит, 2008. - 283 с.

2. Фейнман Ричард П. Дюжина лекций: шесть попроще и шесть посложнее / Р. Фейнман; пер. англ. Е. В. Фалева и В. А. Носенко. - 6-е изд. - Москва: БИНОМ, Лаб. знаний, 2015. - 318 с.

Дополнительная

1. Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.

2. Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 64 с.

3. Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая криптография: учебное пособие./ МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 111 с.

4. Фейнман Ричард П. Фейнмановские лекции по физике: [учебное пособие]. Вып. 8-9: Квантовая механика / Р. Фейнман, Р. Лейтон, М. Сэндс; пер. с англ. Г. И. Копылова; под ред. Я. А. Смородинского. - Изд. 8-е. - Москва: URSS: Либроком, 2014. - 523 с.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Архив статей по квантовой информатике - http://xxx.lanl.gov/, раздел quant-ph
Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Тема 1. Обзор математических методов квантовой физики.

Цель занятия: сделать обзор математических методов квантовой физики:
1. Рассмотреть явление частичного отражения света от поверхности стекла;
2. Рассмотреть метод стрелок для описания амплитуды нахождения частицы в некоторой точке;
3. Изучить отражение света от зеркала;
4. Изучить принцип работы фокусирующей линзы;
5. Рассмотреть эксперимент с электронной пушкой.

Контрольные вопросы:
1. В чем проявляется корпускулярно-волновой дуализм света?
2. Опишите эксперимент с пулеметной стрельбой, с волнами и с электронами.
3. В чем проявляется корпускулярно-волновой дуализм в поведении электрона?
4. Что такое интерференция?
5. Что происходит, если в опыте с электронной пушкой за электроном "наблюдать"?
6. В чем проявляется принцип неопределенности Гейзенберга?
7. В чем заключается главный закон Природы?
8. Из чего образуется результирующая стрелка?
9. Как свет отражается от зеркала?
10. Как свет проходит через 2 поверхности стекла?
11. Почему по мере утолщения стекла величина отраженного света колеблется от 0% до 16%?
12. Объясните действие фокусирующей линзы.
13. Как в атоме водорода протон удерживает электрон?

Тема 2. Алгебраический аппарат квантовой информатики.

Цель занятия: вспомнить материал линейной алгебры, необходимый для понимания основ квантовой механики.

Примерный тип задач, который необходимо разобрать на занятиях для дальнейшего понимания материала:
1. Найти координаты вектора в заданном базисе.
2. Найти матрицу линейного оператора в заданном базисе.
3. Найти собственное число и собственный вектор линейного оператора**.**
4. Доказать свойства унитарного оператора.
5. Доказать свойства самосопряженного оператора.
6. Привести матрицы линейного оператора к диагональному виду.
7. Доказать теорему о связи унитарной матрицы U и эрмитовой матрицы H (U=exp(iH)).
8. Разобрать задачу 3.2, 3.4, 3.7 (стр.9, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.)

Указания по выполнению задания: необходимо вспомнить определения унитарных и эрмитовых матриц.

Разобрать задачу 4.1, 4.2, 4.3 (стр.11 Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.)

Указания по выполнению задания: необходимо вспомнить определение f(A).
9. Найти тензорное произведение матриц A и B.
10. Найти n-ую тензорную степень оператора W Уолша Адамара.

Указания по выполнению задания: необходимо разложить числа i и j в двоичной системе.

11. Разобрать задачу 1.3, 1.4 (стр.14, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.)

Указания по выполнению задания: необходимо воспользоваться определением тензорного произведения пространств

12. Разобрать задачу 2.2 (стр.17, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.)
Указания по выполнению задания: необходимо вспомнить определение тензорного произведения операторов.
13. Разобрать задачу 2.4, 2.3, 2.5 (стр.17, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 55с.).
Указания по выполнению задания: необходимо вспомнить свойства определителей и определение следа матрицы
14. Найти собственные значения и собственные векторы операторов Паули (задача 8, стр.40, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 64 с.)
15.Доказать, что матрицы Паули образуют базис в пространстве эрмитовых матриц.
Контрольные вопросы:
1. Дайте определение векторного пространства.
2. Как найти координаты вектора в некотором заданном базисе?
3. Как определить матрицу перехода между двумя базисами?
4. Как определяется евклидово пространство и унитарное пространство?
5. Дайте определение линейного оператора и его матрицы.
6. Как преобразуется матрица оператора при преобразовании базиса?
7. Дайте определение собственного значения и собственного вектора линейного оператора.
8. Дайте определение сопряженного оператора.
9. Какая матрица у сопряженного оператора?
10. Дайте определение самосопряженного оператора?
11. Дайте определение эрмитовой матрицы?
12. Дайте определение унитарного оператора?
13. Какая матрица у унитарной матрицы?
14. Перечислите свойства самосопряженного оператора.
15. Перечислите свойства унитарного оператора.
16. Каким образом можно привести матрицу линейного оператора к диагональному виду?
17. Как связаны между собой унитарная матрица U и эрмитова матрицы H? (U=exp(iH)).
18. Как определяется тензорное произведение пространств?
19. Как найти тензорное произведение матриц?
20. Как определить экспоненту от матрицы?
21. Как найти производную от exp(At).
Список литературы:
Дополнительная
1. Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Алгебраический аппарат квантовой информатики: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - С. 7-38.
2. Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. – С.40.

Тема 3. Эволюция вектора квантового состояния.

Цель занятия: разобраться в том, каким образом может происходить эволюция квантового состояния во времени
Решить задачи:
1. № 5, стр.39, № 6, № 10, № 11, стр.40, №№ 12,14,16, стр.41, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им.

М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 64 с.)

2. Найти проекцию заданного состояния Ψ на второй кубит.

Указания по выполнению задания: следует измерить состояние Ψ, когда первый кубит перейдет в состояние | 0 >, а потом, когда первый кубит перейдет в состояние | 1 >.

Контрольные вопросы:

1. Что называется пространством классических состояний?
2. Как определяется пространство квантовых состояний?
3. Как называется элемент пространства квантовых состояний?
4. Что такое волновая функция?
5. От каких переменных зависит волновая функция?
6. Какова размерность пространства квантовых состояний?
7. Какова размерность пространства классических состояний?
8. Что имеют в виду под зерном пространственно-временного разрешения?
9. В чем проявляется дискретное представление пространства состояний, т.е. каким образом происходит процесс перехода от волновой функции к конечному вектору (эта процедура еще называется переходом к кубитовому представлению волновой функции)?
10. Какие бывают виды эволюции вектора состояния?
11. Как определяется амплитуда в некоторый точке в следующий момент времени, если мы знаем амплитуды во всех точках в предыдущий момент и знаем амплитуды перехода из этих точек в исходную?
12. В чем заключается унитарная динамика вектора состояния?
13. Как определяется измерение квантового состояния?
14. Что такое коллапс волнового вектора?
15. В чем заключается Правило Макса Борна (основной закон Природы)?
16. Как определяются кет-вектор |Ψ> и бра-вектор <Ψ| (символика Дирака)?
17. Как записывается общий вид однокубитного состояния?
18. Как записывается общий вид двухкубитного состояния?
19. Запишите уравнение Шредингера относительно вектора |Ψ>.
20. Как называется H в уравнении Шредингера?
21. Чему равняется H в простейшем случае частицы в потенциальном поле?
22. Запишите решение уравнения Шредингера как эволюцию вектора состояния во времени (|Ψ(t) >=exp(-iHt) |Ψ(0)>) (в случае постоянства потенциальной энергии во времени).
23. Почему говорят о линейности эволюции?
24. Запишите уравнение Шредингера для атома водорода.
25. Запишите уравнение Шредингера для молекулы водорода.
26. Запишите уравнение Шредингера для одномерных потенциалов.
27. Запишите общий вид решения уравнения Шредингера.
28. Как определяется матрица плотности?
29. Чему равняется ранг матрицы плотности?
30. Как определяется матрица плотности смешанного состояния?
31. Чем отличается чистое состояние от смешанного?
32. Какое состояние называется некогерентным?

Список литературы:

Основная

Хренников А. Ю. Введение в квантовую теорию информации / А. Ю. Хренников. - М.: Физматлит, 2008. – С. 6-60.

Дополнительная

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011– С.39-41.

Тема 4. Применение тензорного произведения.

Цель занятия: рассмотреть различные применения тензорного произведения.
Задачи:
1. Является ли состояние GHZ запутанным?
2. Является ли состояние W запутанным?
3. Являются ли операторы CNOT, Toffoli, SWAP запутывающими? Написать матрицы операторов. Выяснить, представимы ли матрицы в виде тензорного произведения некоторых матриц.
4. Задачи 34, 35, 36, 37, 38, 39, стр.47, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер.

Контрольные вопросы:
1. Что называется тензорным произведением пространств?
2. Что называется тензорным произведением квантовых состояний?
3. Что называется тензорным произведением операторов?
4. Дайте определение незапутанных и запутанных состояний?
5. Приведите пример запутанного квантового состояния?
6. В чем проявляется физический смысл запутанности и ее связь со сложностью вычислений.

Список литературы:
Дополнительная
Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011– С.47.

Тема 5. Соответствие физических величин эрмитовым операторам.

Цель занятия: разобраться в соответствие между физическими величинами и эрмитовыми операторами.
Задачи:
1. Найти собственное значение и собственный вектор оператора координаты.
2. Найти собственное значение и собственный вектор оператора импульса.
3. Найти собственное значение и собственный вектор оператора кинетической энергии.
4. Доказать, что оператор импульса эрмитов.
5. Доказать, что оператор координаты эрмитов.
6. Доказать, что оператор энергии эрмитов.
7. Доказать, что оператор градиента не является эрмитовым.
8. Написать, как действует оператор момента импульса

Указания по выполнению задания: необходимо вспомнить определение векторного произведения.
9. Решить стационарную задачу для свободной частицы.
10. Найти матрицу оператора отражения вдоль вектора $|a\rangle$. Доказать, что он унитарен (задача № 42, стр.50, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 64 с.)
11. Реализовать на квантовом компьютере оператор отражения вдоль вектора $|0\rangle$.

Указания по выполнению задания: сканировать кубиты аргумента слева направо, одновременно с нулевой анцилой, нужной для сбора мусора, а результат выявления хотя бы одной единицы накапливать в специальном кубите res, который после сканирования нужно использоваться для изменения знака (задача 44, Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. - 64 с.).

Контрольные вопросы:
1. Как определяется оператор координаты?

2. Как определяется оператор импульса?
3. Как определяется оператор энергии?
4. Как определяется оператор момента?
5. Как записывается импульсное представление волновой функции (преобразование Фурье от волновой функции)?
6. Как получается оператор энергии из выражения для классической энергии?
7. Как связаны между собой классические значения физической величины и собственные значения соответствующего эрмитова оператора?
8. Можно ли измерить одновременно координату и импульс вдоль одной координатной оси?
9. А если рассмотреть координату x, а импульс вдоль другой оси?
10. В каком смысле понимается одновременное измерение?

Список литературы:

Дополнительная

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая информатика и квантовый компьютер: учебное пособие. МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. – С.50.

Тема 6. Квантовый компьютер.

Цель занятия: изучить абстрактную модель квантового компьютера.

Задачи:

1. Физически реализовать NOT .
2. Физически реализовать CNOT .
3. Реализовать Gate Toffoli в виде Quantum Gate Array с использованием оператора Адамара, NOT и CNOT.

Контрольные вопросы:

1. Опишите абстрактную схему квантового компьютера.
2. Опишите, в чем заключается квантовое вычисление.
3. Опишите вычисление с оракулом на классическом компьютере.
4. Что такое квантовый оракул?
5. Опишите задачу перебора.
6. Что такое квантовые вентили?
7. Какие однокубитные квантовые вентили вы знаете?
8. Какие двухкубитные квантовые вентили вы знаете?
9. Какие трехкубитные квантовые вентили вы знаете?
10. Как составляются квантовые схемы из функциональных элементов?
11. Что такое анцилла?
12. Зачем вводится анцилла при р*еализации на квантовом компьютере оператора отражения вдоль вектора* | 0 >?
13. Зачем производится квантовая чистка анцилл?
14. Что такое квантовое ускорение?
15. В чем заключается алгоритм Гровера для переборной задачи?
16. Объясните геометрический смысл алгоритма Гровера.
17. В чем заключается типичность гроверовского ускорения?
18. Что вы можете сказать о нижних оценках квантовой сложности?
19. Как соотносятся NP- задачи и квантовые вычисления?
20. Какие вы знаете алгоритмы квантового моделирования систем многих частиц?
21. В чем заключается схема телепортации неизвестного квантового состояния?
22. Что имеется в виду под запретом на клонирование квантовых состояний?

Тема 7. Элементы квантовой криптографии.

Цель занятия: познакомиться с основными положениями квантовой криптографии

Контрольные вопросы:

1. К какому году относится рождение квантовой криптографии?
2. В чем заключается главное преимущество квантовой криптографии перед классической?
3. В чем заключается задача секретной передачи данных?
4. В чем заключается задача распространения секретного ключа?
5. Какие вы знаете исторические способы шифрования данных?
6. Каковы интересы Алисы (Alice),Боба (Bob) и Евы (Eve)?
7. Что такое криптографический протокол?
8. Что такое симметричные шифры?
9. Дайте определение стойкости криптосистемы.
10. Сформулируйте теорему Шеннона.
11. В чем проявляется использование псевдослучайных генераторов?
12. Как связан вопрос о псевдослучайных генераторах с нерешенной проблемой о равенстве P и NP проблемы?
13. Что такое криптосистема с открытым ключом?
14. Опишите схему алгоритма RSA.
15. Алгоритм Шора факторизации больших чисел. Квантовые коды коррекции ошибок. Протокол BB84.

Список литературы:

Дополнительная

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский. Квантовая криптография: учебное пособие./ МГУ им. М.В. Ломоносова, Фак. вычисл. математики и кибернетики. - Москва: МАКС Пресс, 2011. – С. 9-25.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Квантовые вычисления и квантовая криптография реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.

Цель дисциплины: овладение студентами - математиками основами квантовой механики и квантовых вычислений, и умением применять такие знания для решения задач практических вычислений. Задачи: научить применять знания по основам квантовой механике для решения задач практических вычислений.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей.

В результате освоения дисциплины обучающийся должен:

Знать: основы нерелятивистской квантовой теории одной и нескольких частиц, принципы вычислений и обработки информации, содержащихся в квантовых ансамблях;

Уметь: построить алгоритм, реализующий стандартные информационные процессы над квантовыми ансамблями (унитарная эволюция, измерение и частичное измерение, вычисление запутанности, телепортация, квантовые вентили), реализовать компьютерную модель этого процесса и оценить его сложность, построить математическую и программную модель реального процесса для нескольких заряженных частиц во внешнем потенциале, в частности, реализующую стандартные квантовые вентили, и сделать практические выводы по ней (время срабатывания, добротность, возможность масштабирования);

Владеть: реализацией вычислительных алгоритмов с применением стандартных квантовых вентилей, вычислением стандартных физических величин (энергии, координат, импульса, момента), а также вероятностных распределений для заданных квантовых состояний простых ансамблей из нескольких частиц во внешнем потенциале.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.