

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Физический факультет

УТВЕРЖДЕНО:
Декан физического факультета
С.Н. Филимонов

Рабочая программа дисциплины

Квантовые вычисления и квантовая криптография

по направлению подготовки

03.04.02 Физика

Направленность (профиль) подготовки:
«Фундаментальная и прикладная физика»

Форма обучения
Очная

Квалификация
Магистр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
О.Н. Чайковская

Председатель УМК
О.М. Сюсина

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины (модуля)

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2. Способен в сфере своей профессиональной деятельности организовывать самостоятельную и коллективную научно-исследовательскую деятельность для поиска, выработки и принятия решений в области физики

ОПК-3. Способен применять знания в области информационных технологий, использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки

ОПК-4. Способен определять сферу внедрения результатов научных исследований в области своей профессиональной деятельности.

ПК-1. Способен самостоятельно ставить конкретные задачи научных исследований в области физики и решать их с помощью современной аппаратуры и информационных технологий с использованием новейшего российского и зарубежного опыта

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.1. Оценивает перспективность планируемых исследований с точки зрения трендов развития выбранной научной области.

ИОПК-3.1. Использует специализированные интернет-ресурсы для поиска научной информации и анализа трендов развития наук.

ИОПК-4.2. Формулирует практическую значимость результатов научных исследований с учетом трендов развития науки и технологии

ИПК-1.1. Знает основные стратегии исследований в выбранной области физики, критерии эффективности, ограничения применимости

ИПК-1.3. Владеет навыками аналитической переработки информации, проведения исследований с помощью современной аппаратуры и информационных технологий, обобщения и представления результатов, полученных в процессе решения задач исследования

2. Задачи освоения дисциплины

– Получить представление об актуальных задачах по обработке информации в виде реальных физических задач, основанных на постулатах квантовой механики.

– Научиться строить эффективные алгоритмы для решения задач классификации, поиска, оптимизации и передачи квантовой информации.

3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Семестр 3, зачет.

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Линейная алгебра и аналитическая геометрия, Математический анализ, Классическая механика, Квантовая механика

6. Язык реализации

Русский

7. Объем дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

– лекции: 18 ч.;

– практические занятия: 14 ч.;

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины (модуля), структурированное по темам

Тема 1. Введение в квантовые вычисления

Принцип суперпозиции, запутанность, квантовые измерения. Квантовые состояния и операторы. Математический аппарат: гильбертово пространство, матрицы плотности. Определение кубита. Однокубитовые и многокубитовые вентили. Унитарные операции и их представление. Решение задач на вычисление состояний кубитов. Моделирование простых квантовых схем.

Тема 2. Квантовые алгоритмы

Алгоритм Дойча-Йожи: Постановка задачи и реализация алгоритма на квантовом компьютере. Алгоритм Шора: Факторизация чисел и её значение для криптографии и квантовое преобразование Фурье. Алгоритм Гровера: поиск в неупорядоченной базе данных и оптимизация алгоритма. Решение задач на квантовые алгоритмы: Моделирование алгоритмов Шора и Гровера.

Тема 3. Квантовая криптография

Основы квантовой криптографии, принципы квантовой защиты информации, квантовое распределение ключей. Протокол BB84: описание протокола и устойчивость протокола против стандартных атак. Другие протоколы квантовой криптографии: протокол E91 (на основе запутанности), протокол B92. Анализ протоколов квантовой криптографии.

Тема 4. Практические аспекты квантовых вычислений и криптографии

Квантовые компьютеры и их реализация: физические реализации кубитов (сверхпроводящие кубиты, ионные ловушки, фотонные системы), проблемы декогеренции и ошибок. Квантовые ошибки и коррекция: Типы квантовых ошибок, коды коррекции ошибок. Практика работы с квантовыми симуляторами: использование IBM Qiskit, Google Cirq и других открытых платформ, реализация простых квантовых алгоритмов и протоколов.

Тема 5. Современные тенденции и приложения

Приложения квантовых вычислений: квантовое машинное обучение, квантовые симуляции в химии и физике. Будущее квантовых технологий: квантовые системы на закрученных фотонах, квантовый интернет и проблемы масштабирования квантовых систем. Анализ современных исследований в области квантовых вычислений и криптографии.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине осуществляется путем контроля посещаемости, контроля выполнения заданий, предлагаемых на практических занятиях, и фиксируется в форме контрольной точки не менее одного раза в семестр. Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» – <https://www.tsu.ru/sveden/education/eduop/>.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в третьем семестре проводится в устной форме по билетам.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» – <https://www.tsu.ru/sveden/education/eduop/>.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle».

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (<https://www.tsu.ru/sveden/education/eduop/>).

в) План лекционных и семинарских / практических занятий по дисциплине.

Тема 1. Основы работы с кубитами. Решение задач на вычисление состояний кубитов после применения вентилей X, Y, Z, оператор Адамара, CNOT, SWAP.

Тема 2. Квантовая запутанность и измерения. Решение задач на измерение состояний запутанных кубитов.

Тема 3. Знакомство с системами моделирования квантовых алгоритмов IBM Qiskit, Google Cirq. Моделирование алгоритма Дойчи-Йожи.

Тема 4. Моделирование алгоритма Гровера для поиска одного элемента.

Тема 5. Моделирование упрощенной версии алгоритма Шора. Анализ работы алгоритма для небольших чисел.

Тема 6. Моделирование криптографического протокола BB84 на симуляторе. Анализ и обсуждение возможных атак.

Тема 7. Моделирование криптографического протокола E91. Решение задач на анализ запутанных состояний. Сравнение с BB84 на устойчивость к стандартным атакам.

Тема 8. Моделирование простого кода коррекции ошибок. Решение задач на анализ устойчивости к ошибкам.

Тема 9. Обсуждение современных тенденций в квантовых вычислениях и криптографии.

и ресурсов сети Интернет

а) основная литература:

- Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг - М.: Мир, 2006. – 824 с.

- Кронберг Д. А. Квантовая криптография: учебное пособие / Д.А. Кронберг, Ю.И. Ожигов, А.Ю Чернявский – М.: МГУ им. М.В. Ломоносова, 2011. – 111 с.

- Williams C. P. Explorations in quantum computing. – Springer-Verlag London Limited, 2011. – 740 p.

б) дополнительная литература:

– Килин С.Я. Квантовая криптография: идея и практика / С.Я. Килин, Д.Б. Хорошко, А. П. Низовцев, В.Н. Шатохин, А.А. Букач, А.А. Игнатенко, А.С. Малоштан – Минск: Булорусская наука, 2007. – 391 с.

– Валиев К. А. Квантовые компьютеры: надежда и реальность / К. А. Валиев, А. А. Кокин - Москва-Ижевск, 2001. – 352 с.

– Холево А.С. Введение в квантовую теорию информации. – М.: МЦНМО, 2002. – 128 с.

– Бауместер Д. Физика квантовой информации / Д. Бауместер, А. Экерт, А. Цайлингер – М.: Постамаркет, 2002. – 376 с.

– Erhard M. et al. Twisted photons: new quantum perspectives in high dimensions //Light: Science & Applications. – 2018. – Т. 7. – №. 3. – С. 17146-17146.

– Kazinski P. O., Korolev P. S. Scattering of plane-wave and twisted photons by helical media //Journal of Physics A: Mathematical and Theoretical. – 2022. – Т. 55. – №. 39. – С. 395301.

в) ресурсы сети Интернет:

– открытые онлайн-курсы;

– <https://learning.quantum.ibm.com/catalog/tutorials>

– <https://github.com/Qiskit/documentation>

– <https://quantumai.google/cirq/start/intro>

– <https://scholar.google.com>

– <https://arxiv.org>

– <https://www.researchgate.net>

технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– офисные пакеты (Microsoft Office/LibreOffice/iWork и т.д.), программы для просмотра pdf файлов (Adobe Acrobat Reader/Okular и т.д.), система компьютерной верстки TeX/LaTeX;

– система для моделирования квантовых алгоритмов IBM Qiskit, система работы с квантовыми схемами Google Cirq;

– публично доступные облачные технологии (Google Collab, Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – <http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system>

– Электронная библиотека (репозиторий) ТГУ – <http://vital.lib.tsu.ru/vital/access/manager/Index>

– ЭБС Лань – <http://e.lanbook.com/>

– ЭБС Консультант студента – <http://www.studentlibrary.ru/>

– Образовательная платформа Юрайт – <https://urait.ru/>

– ЭБС ZNANIUM.com – <https://znanium.com/>

– ЭБС IPRbooks – <http://www.iprbookshop.ru/>

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Аудитории, оборудованные соответствующей техникой (в том числе «Актру»), для реализации учебного процесса в смешанном формате.

15. Информация о разработчиках

Королев Петр Сергеевич, лаборатория теоретической и математической физики, инженер-исследователь; кафедра квантовой теории поля физического факультета ТГУ, ассистент (совм.); лаборатория анализа данных физики высоких энергий, младший научный сотрудник (совм.)