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

Институт экономики и менеджмента

УТВЕРЖДЕНО:
Директор
_____Е. В. Нехода

Рабочая программа дисциплины

Квантовые технологии и коммуникации

по направлению подготовки

38.04.08 Финансы и кредит

Направленность (профиль) подготовки:
Финансовые технологии: разработка и внедрение

Форма обучения
Очная

Квалификация
Руководитель проекта в области финансовых технологий

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
_____Л.И. Ткаченко

Председатель УМК
_____М.В. Герман

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ОПК-2 Способен применять продвинутые инструментальные методы экономического и финансового анализа в прикладных и (или) фундаментальных исследованиях в области финансовых отношений и технологий, в том числе с использованием интеллектуальных информационно-аналитических систем;

ПК-1 Способен создавать продукты и сервисы с применением финансовых технологий;

2. Задачи освоения дисциплины

– Освоить теоретический и методический аппарат квантовых вычислений и технических платформ для их реализации.

– Научиться применять теоретический и методический аппарат квантовых вычислений в финансовой сфере, для оптимизации портфеля и решения других практических задач в финансовой сфере.

3. Место дисциплины 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

Второй семестр, 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 курса студенты должны иметь базовые знания в области математического анализа, линейной алгебры, теории вероятности и случайных процессов, математической статистики, методов оптимизации, экономической теории и эконометрики, иметь представление о рынке ценных бумаг. Желательно владение английским языком на уровне, достаточном для свободного чтения профессиональной литературы

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 8 ч.
-практические занятия: 20 ч.
в том числе практическая подготовка: 20 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в квантовые вычисления.

Мотивация: какие задачи и проблемы решаем. Основные понятия: кубит, квантовая суперпозиция, запутанность, белловские состояния, сфера Блоха, чистые состояния Вентили: XZY - матрицы Паули, Адамар, Phase gate, CNOT, Тоффоли, универсальный набор операторов. Запрет о клонировании, квантовая телепортация. Коррекция классических и квантовых ошибок, пятикубитный алгоритм коррекции одной бит-флип ошибки.

Тема 2. Технические платформы для реализации квантовых вычислений

Типы кубитов, времена релаксации, дефазировки и когерентности, квантовые ошибки. Платформы: фотоны, спины, ионы, атомы, сверхпроводники, их применение в квантовых вычислениях, сенсорике и коммуникациях. Технические аспекты квантовых вычислений Квантовые компьютеры и их архитектура. Программирование на Qiskit, D-Wave. Написание простых квантовых программ.

Тема 3. Применение квантовых вычислений в финансовой сфере

Введение в финансовые задачи. Обзор квантовых алгоритмов: оптимизация портфеля, ценообразование деривативов, управление рисками. Технические аспекты квантовых вычислений. Квантовые компьютеры и их архитектура. Программирование на Qiskit, D-Wave. Написание простых квантовых программ

Тема 4. Квантовые вычисления для оптимизации портфеля

Постановка задачи оптимизации. Классические методы vs. квантовые методы. Примеры и кейсы. Решение реальных финансовых задач с использованием квантовых вычислений (оптимизация портфеля). Анализ результатов и выводы

Тема 5. Постквантовые алгоритмы шифрования

Введение. Ключевые термины и понятия: в части криптографии – виды алгоритмов, понятие стойкости алгоритма, понятие (математической) сложности задачи; в части квантовой физики – квантовая информация, квантовые вычисления, квантовый компьютер, эмуляторы квантовых компьютеров, квантовая угроза, квантовый ключ. Современные криптографические алгоритмы: симметричные; асимметричные; влияние длины ключа на скорость работы и стойкость; общая оценка надежности алгоритмов. Квантовая угроза — новый риск информационной безопасности для государства и бизнеса: Алгоритмы Шора и Гровера. Обзор неустойчивых к квантовой угрозе алгоритмов шифрования данных. Актуализация квантовой угрозы. Международный опыт: позиция крупнейших государств, включая обзор стратегий кибербезопаности. Методы квантовой атаки на криптографию: суть (цель) атак; срок/вероятность проведения успешных атак, модель злоумышленника. Постквантовая криптография - оптимальный метод защиты данных от квантовой угрозы с помощью программных и программно-аппаратных решений: отличия квантовой и постквантовой криптографии; введение в технологию постквантовой криптографии: научно-технологический задел РФ и Исполнителя по постквантовой криптографии. Основные направления интеграций программных продуктов на основе постквантовых алгоритмов в существующие информационные решения и сервисы государства и бизнеса. обзор продуктов Исполнителя. Опыт пилотирования постквантовых алгоритмов и программных решений на их основе в РФ (обзор кейсов). Позиция регуляторов по постквантовой криптографии в РФ и мире. Обзор процесса разработки новых госстандартов.

Тема 6. Конфиденциальные вычисления

Основные технологические подходы к решению задач конфиденциальных вычислений. Примеры протоколов и сферы применения технологий конфиденциальных вычислений. Гомоморфное шифрование: технология и сферы применения. Различия

между классическими подходами технологий конфиденциальных вычислений и гомоморфным шифрованием. Примеры задач, решаемых с применением технологий конфиденциальный вычислений. Примеры существующих решений в РФ и мире. Политика регулятора РФ в отношении конфиденциальных вычислений.

Тема 7. Введение в квантовые коммуникации

Симметричное шифрование: принцип, задача распределения секретных ключей, способы решения (фельдъегерская служба (недостатки), ассиметричная криптография) Ассиметричные схемы: протокол распределения ключей Диффи-Хеллмана, шифр RSA Алгоритм Шора, стратегия "перехвати сейчас, взломай потом" Абсолютная криптостойкость: определение, одноразовый блокнот, условия абсолютной криптостойкости, доказательство. Необходимость КРК и КГСЧ. Задача об интерференции Маха-Цандера (интерференция электрических полей) волновой пакет, понятие фотона. Принципы квантовой физики: вектор состояния в гильбертовом пространстве, чистые состояния, наблюдаемые и операторы, эволюция квантовой системы, ур. Шредингера, необходимость комплексных чисел, принцип суперпозиции, правило Борна, проективные измерения. Понятие о кубите: двухуровневая квантовая система, вектор Джонса. Пример: суперпозиция путей, пространственный кубит, простейший генератор случайных чисел: ИОФ, светоделитель, два детектора. Задача об интерференции Маха-Цандера (оператор светоделителя, оператор зеркала, оператор наблюдаемой, интерференция амплитуд вероятностей). Протокол КРК BB84: теорема о запрете клонирования: схема (источник, канал, приемник), протокол, постобработка (что происходит с ключом после приема 4n посылок). Теория информации: Бинарная энтропия Шеннона, совместная энтропия, условная энтропия, взаимная информация, бинарный симметричный канал. Оптимальная стратегия Евы: максимальный процент допустимых ошибок в канале, формула секретного ключа. Стратегии Евы: Симметричное измерение, Перехват/перепосыл, Симметричная индивидуальная атака, Оптимальная атака. Все стратегии на одном графике Взаимной информации от QBER Задача о расчете скорости генерации секретного ключа в типичных условиях.

Тема 8. Основные элементы и схемы систем квантового распределения ключей. Применимость технологии в финансовой отрасли

Детекторы одиночных фотонов Детекторы одиночных фотонов (эффективность, темновой счет, мертвое время). Лазер: когерентные состояния, распределение Пуассона, число фотонов в импульсе PNS-атака. Обманные состояния. Атаки на несовершенною работу элементов КРК (детекторы, фазовые модуляторы). Волоконные схемы КРК. Схема на поляризационном кодировании. Схема на фазовом кодировании. Схема на фазово-временном кодировании. Преимущества/недостатки. Формула вычисления QBER. Оптическая схема КРК plug & play. Применимость технологии в финансовой индустрии. Проекты России и в мире.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости лекций и семинарских занятий, а также активности при устных опросах, обсуждениях, дискуссиях на семинарах и лекциях, проведения контрольных работ, письменных опросов по лекционному материалу, решения задач и кейсов по темам, выполнения домашних заданий 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 во втором семестре проводится в письменной форме по билетам. Билет состоит из двух частей. Продолжительность зачета 90 мин.

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 электронной среде обучения iDO https://lms.tsu.ru/course/view.php?id=37296

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

- Львовский А. Отличная квантовая механика. В 2 ч. Ч. I : учебное пособие / Львовский А. – Издательство: Альпина Паблишер, 2019 – 422 с. – ISBN 978-5-91671-952-9// Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140480

б) дополнительная литература:

- Чивилихин, С. А. Квантовая информатика: учебное пособие/С. А. Чивилихин. — Санкт- Петербург: НИУ ИТМО, 2009. — 80 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/40805
- Душкин, Р. В. Квантовые вычисления и функциональное программирование / Р. В. Душкин. — Москва: ДМК Пресс, 2015. — 232 с. — ISBN 978-5-97060-275-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/97340

Aleksey Fedorov, [17.07.2024 0:35]
Материалы для самостоятельного ознакомления
Постквантовые алгоритмы
От 15.07.2024
Открытая база знаний о квантовой угрозе и постквантовых алгоритмах
https://qapp.tech/help

Подскасты:

Подкаст AM Live о научно-технологической синергии решений квантовых коммуникаций и постквантовых алгоритмов
https://www.youtube.com/watch?v=vw1wP_7gX_Q
Подкаст Музея Криптографии «Секретная станция»
https://cryptomuseum.mave.digital/

Аналитические отчеты:

Аналитический отчет «Квантовые технологии для государства и бизнеса: настоящее и будущее»
https://qapp.tech/research/analytics/fbt2023
Аналитический отчет ««Квантовые технологии для медицины. Новые подходы в вычислениях, защите данных и сенсорике»»
https://qapp.tech/research/analytics/fbt2024
Аналитический отчет «Безопасность квантовых технологий в сфере IT»

https://qapp.tech/research/analytics/phd2024

Подборка из более чем 25 бизнес-публикаций о постквантовых алгоритмах https://www.cnews.ru/book/PQC_-_Post_Quantum_Cryptography_-_%D0%9F%D0%BE%D1%81%D1%82%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_-_%D0%9F%D0%BE%D1%81%D1%82%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5

Жан-Филипп Омассон: «О криптографии всерьез. Практическое введение в современное шифрование», https://www.labirint.ru/books/840962/

М. Нильсен, И. Чанг, Квантовые вычисления и квантовая информация, Мир, Москва (2006).

Львовский А. Отличная квантовая механика.

40 years of quantum computing. Nat Rev Phys 4, 1 (2022). https://doi.org/10.1038/s42254-021-00410-6

Y. Aharonov, D. Rohrlich Quantum Paradoxes: Quantum Theory for the Perplexed, WILEY (2005)

Ryan LaRose, Overview and Comparison of Gate Level Quantum Software Platforms Quantum 3, 130 (2019)

Jordan, S. Quantum algorithm zoo. https://quantumalgorithmzoo.org/.

M. H. Devoret, R. J. Schoelkopf ,Superconducting Circuits for Quantum Information: An Outlook Science 339,1169-1174(2013). DOI:10.1126/science.1231930

в) ресурсы сети Интернет:

- Официальные сайты – источники отечественных и зарубежных нормативных документов: https://digital.gov.ru/ru/, http://www.grfc.ru/; http://www.etsi.org/; http://www.itu.int/; http://www.fcc.gov/.

- Научная электронная библиотека http://www.elibrary.ru/.

- Электронно-библиотечная система http://www.iprbookshop.ru/

- Специализированные сайты для поиска документации по электронным компонентам: Москабель-Фуджикура https://mkf.mkm.ru/. http://ru.wikipedia.org/wiki/Ethernet, http://www.ot.ru/, http://opten.spb.ru/ru/.

6. Портал Международного союза электросвязи: https://www.itu.int/

7. Портал Международной электротехнической комиссии: https://www.iec.ch/

8. Международная группа по надежности (Gnedenko e-Forum): https://gnedenko.net/index.htm

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

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

б) информационные справочные системы:

- Портал Федеральных государственных образовательных стандартов высшего образования: https://fgosvo.ru

- Справочно-правовая система Консультант – Режим доступа: https://www.consultant.ru/

- Справочно-правовая система Гарант – Режим доступа: https://www.garant.ru/

- Портал Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации: https://digital.gov.ru/ru/documents/

- Портал Федерального агентства по техническому регулированию и метрологии Российской Федерации: https://www.gost.ru/portal/gost/

– 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/

в) профессиональные базы данных:

- Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)

- Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)

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.

15. Информация о разработчиках

Алексей Константинович Федоров, PhD, директор Института физики и квантовой инженерии НИТУ МИСИС, руководитель научной группы «Квантовые информационные технологии» РКЦ, заведующий лабораторией квантовых информационных технологий НИТУ МИСИС, профессор кафедры РКЦ МФТИ