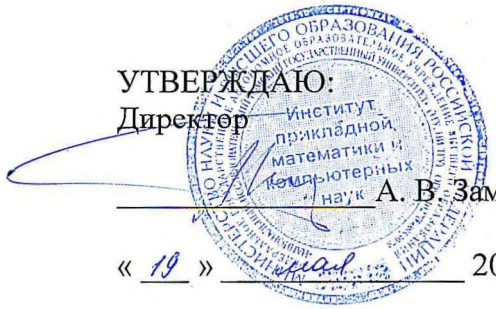
Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук



УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 19 » января 2022 г.

Рабочая программа дисциплины

Квантовые вычисления

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2022

Код дисциплины в учебном плане: Б1.В.01

СОГЛАСОВАНО:
Руководитель ОП
_____ В.Н. Тренькаев

Председатель УМК
_____ С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-1 – Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

– ОПК-7 – Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

– ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ПК-2 – Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности.

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.

ИОПК-7.3 Демонстрирует навыки создания программ с применением методов и инструментальных средств программирования для решения различных профессиональных, исследовательских и прикладных задач.

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации.

2. Задачи освоения дисциплины

– Сформировать у студентов способность учитывать современные тенденции развития информационных технологий в своей профессиональной деятельности, в частности: ознакомить с основами квантовых вычислений и квантовой криптографии; сформировать навыки использования инструментальных средств моделирования квантовых схем.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, является обязательной для изучения.

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

Десятый семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Физика, Информатика, Общая алгебра, Дискретная математика, Теория чисел, Методы и средства криптографической защиты информации.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-лабораторные: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение в квантовые вычисления

- Квантовая гонка.
- Квантовый компьютер.
- Квантовые вычисления.

Тема 2. Математические основы квантовых вычислений

- Линейное пространство.
- Линейные операторы.
- Обратимые вычисления.
- Обратимые вентили.
- Обратимые схемы.

Тема 3. Квантовые схемы

- Кубит. Одно/двух/трехкубитовые вентили.
- Простые квантовые схемы. Вычисление булевой функции.
- Сложные квантовые схемы.

Тема 4. Квантовые протоколы

- Квантовые протоколы передачи данных.
- Квантовые протоколы распределения ключей.

Тема 5. Раздел 5. Квантовые алгоритмы

- Алгоритм Дойча – Джозса.
- Алгоритм Бернштейна – Вазирани
- Алгоритм Саймона.
- Алгоритм Гровера.
- Алгоритм Шора.

Тема 6. Квантовая коррекция ошибок

- Общая схема квантовых кодов.
- Трехкубитовый квантовый код.
- Девятикубитный код Шора.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения лабораторных работ/контрольных заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Типовые варианты заданий для лабораторных работ:

1. Реализация квантовой схемы Базис Белла. Выполнить моделирование квантовой схемы для создания состояния Белла с использованием системы IBM Quantum Experience и объяснить полученные результаты.
2. Реализация квантовой схемы Reverse CNOT. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль Reverse CNOT на базе двухкубитового вентиля CNOT, объяснить полученные результаты моделирования.
3. Реализация квантовой схемы SWAP. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль SWAP на базе двухкубитовых вентилей CNOT и Reverse CNOT, объяснить полученные результаты моделирования.
4. Алгоритм Дойча. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Дойча для выбранной сбалансированной булевой функции, объяснить полученные результаты моделирования.
5. Алгоритм Бернштейна – Вазирани. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Бернштейна – Вазирани для нахождения скрытой строки длины 2, объяснить полученные результаты моделирования. Прокомментировать построение квантового оракула для булевой функции, которая скрывает задуманную строку.
6. Алгоритм Гровера. С использованием системы IBM Quantum Experience выполнить моделирование квантовой схемы, реализующей алгоритм Гровера для выбранной булевой функции от двух переменных, объяснить полученные результаты моделирования.

Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ/контрольных заданий, с оценкой за каждую не менее 50 баллов.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в десятом семестре проводится в устной/письменной форме с использованием перечня контрольных вопросов по курсу. Схема вопросов экзамена должна соответствовать компетентностной структуре дисциплине. При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов – результатов обучения. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Примерный перечень вопросов к экзамену:

1. Основные постулаты квантовой теории.
2. Линейное пространство.
3. Унитарные операторы.
4. Обратимые вычисления.
5. Обратимые вентили.
6. Принципы функционирования квантового компьютера.
7. Декогеренция и ошибки квантовых вычислений.
8. Кубит. Квантовый регистр.
9. Квантовые вентили X, Y, Z.
10. Квантовые вентили H, S, T.
11. Квантовый вентиль NOT.
12. Квантовый вентиль CNOT.
13. Квантовый вентиль CCNOT.
14. Невозможность клонирования кубита.
15. Состояние Белла.
16. Квантовый параллелизм.
17. Основные постулаты квантовой теории.
18. Принципы функционирования квантового компьютера.
19. Декогеренция и ошибки квантовых вычислений.
20. Кубит. Квантовый регистр.
21. Унитарные операторы и квантовые вычисления.
22. Однокубитовые вентили.
23. Двухкубитовые вентили.
24. Трехкубитовые вентили.
25. Простые квантовые схемы.
26. Невозможность клонирования кубита.
27. Алгоритм Дойча-Джозса.
28. Алгоритм Саймона.
29. Алгоритм Гровера.
30. Алгоритм Бернштейна – Вазирани.
31. Квантовое преобразование Фурье.
32. Алгоритм Шора.
33. Квантовое плотное кодирование.
34. Квантовая телепортация.

35. Квантовый протокол распределения ключей (BB84).
36. Квантовый протокол распределения ключей (B92).
37. Квантовый протокол распределения ключей (E91).
38. Общая схема квантовых кодов.
39. Трехкубитовый квантовый код.

Критерии выставления оценок:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

11. Учебно-методическое обеспечение

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

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

в) Семинарских / практических занятий по дисциплине нет.

г) Методические указания по проведению лабораторных работ.

Для выполнения лабораторной работы студенту необходимо:
1. Изучить методические указания по выполнению лабораторной работы.
2. Реализовать требуемую квантовую схему.
3. Прокомментировать преподавателю процесс вычислений квантовой схемы.

г) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа со слайдами лекции; изучение вопросов, выносимых за рамки лекционных занятий; выполнение контрольных заданий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации). Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы. Контрольные задания и лабораторные работы, приведенные в планах занятий, выполняются студентами в обязательном порядке. Методические указания обучающимся по освоению дисциплины: целенаправленно, систематически и планомерно работать со слайдами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; тратить не менее часа в день на самостоятельную работу; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе Moodle ТГУ; работать с тематическими форумами в сети Интернет.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Сысоев С. С. Введение в квантовые вычисления. Квантовые алгоритмы : учебное пособие. - СПб : Изд-во С.-Петерб. ун-та, 2019, 144 с.

– Торгаев С.Н., Шульга И.Д., Юрченко Е.А., Громов М.Л. Основы квантовых вычислений: учебное пособие. - Томск: STT, 2020, 100 с.

– Райли Т. Перри Элементарное введение в квантовые вычисления. Учебное пособие. - М.: ИНТЕЛЛЕКТ, 2015, 203 с.

– Альбов А.С. Квантовая криптография. -Санкт-Петербург: СТРАТА, 2015, 245 с.

б) дополнительная литература:

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

– Имре Ш., Баланж Ф. Квантовые вычисления и связь. Инженерный подход. - М.: ФИЗМАТЛИТ, 2008, 320 с.

– Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления.- Ижевск: Регулярная и хаотическая динамика, 2009, 360 с.

в) ресурсы сети Интернет:

– Михаил Вялый, Александр Шень Курс “ Классические и квантовые вычисления” [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/1057/136/info

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– операционная система Windows/Linux, браузер Firefox/Яндекс

– публично доступные облачные сервисы квантовых симуляторов (IBM Quantum, Azure Quantum 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 лабораторных занятий и занятий лекционного типа, а также для проведения 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

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности