

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

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

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
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Треньяев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

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. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторные работы.

Текущий контроль по дисциплине проводится путем контроля посещаемости и проведения лабораторных работ.

Типовые варианты заданий для лабораторных работ (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Реализация квантовой схемы Базис Белла. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы для создания состояния Белла и объяснить полученные результаты моделирования.
2. Реализация квантовой схемы Reverse CNOT. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль Reverse CNOT на базе двухкубитового вентиля CNOT и объяснить полученные результаты моделирования.
3. Реализация квантовой схемы SWAP. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы, реализующей двухкубитовый вентиль SWAP на базе двухкубитовых вентилях CNOT и Reverse CNOT и объяснить полученные результаты моделирования.
4. Алгоритм Дойча. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы, реализующей алгоритм Дойча для выбранной сбалансированной булевой функции и объяснить полученные результаты моделирования.
5. Алгоритм Бернштейна – Вазирани. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы, реализующей алгоритм Бернштейна – Вазирани для нахождения скрытой строки длины 2 и объяснить полученные результаты моделирования. Прокомментировать построение квантового оракула для булевой функции, которая скрывает задуманную строку.
6. Алгоритм Гровера. С использованием эмулятора квантового компьютера от ТГУ (<https://qsim.tsu.ru/>) выполнить моделирование квантовой схемы, реализующей алгоритм Гровера для выбранной булевой функции от двух переменных и 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 с оценкой за каждую не менее 50 баллов.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен проводится в устной/письменной форме с использованием перечня контрольных вопросов по курсу. При оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций. 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 оценивания промежуточной аттестации:

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

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

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

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

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

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).

Информация о разработчиках

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