ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПРИВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ»

Квантовые технологии

рабочая программа дисциплины (модуля)

Направление подготовки 09.04.02 Информационные системы и технологии
Направленность (профиль) Корпоративные информационные системы

Квалификация **магистр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля в семестрах:

зачеты 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	13 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	10	10	10	10
Лабораторные	20	20	20	20
Конт. ч. на аттест. в период ЭС	0,15	0,15	0,15	0,15
В том числе в форме практ.подготовки	20	20	20	20
Итого ауд.	30	30	30	30
Контактная работа	30,15	30,15	30,15	30,15
Сам. работа	69	69	69	69
Часы на контроль	8,85	8,85	8,85	8,85
Итого	108	108	108	108

Программу составил(и):
к.э.н., доцент, Ефимова Т.В.

Рабочая программа дисциплины
Квантовые технологии

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 917)

составлена на основании учебного плана: 09.04.02-25-2-ИСТмКИС.plm.plx

Направление подготовки 09.04.02 Информационные системы и технологии Направленность (профиль) Корпоративные информационные системы

Рабочая программа одобрена на заседании кафедры
Цифровые технологии

Зав. кафедрой Ефимова Т.Б.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является формирование у студентов способности учитывать современные тенденции развития информационных технологий в своей
1.2	профессиональной деятельности, в частности ознакомить с основами квантовых
1.3	вычислений и квантовой криптографии

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДВ.01.01

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-3 Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований

ПК-3.1 Проводит анализ научных данных, результатов экспериментов и наблюдений

40.011. Профессиональный стандарт "СПЕЦИАЛИСТ ПО НАУЧНО-ИССЛЕДОВАТЕЛЬСКИМ И ОПЫТНО-КОНСТРУКТОРСКИМ РАЗРАБОТКАМ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 4 марта 2014 г. N 121н (зарегистрирован Министерством юстиции Российской Федерации 21 марта 2014 г., регистрационный N 31692)

ПК-3. В. Проведение научно-исследовательских и опытно-конструкторских разработок при исследовании самостоятельных тем

В/02.6 Проведение работ по обработке и анализу научно-технической информации и результатов исследований

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	особенности проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий
3.1.2	
3.1.3	
3.2	**Уметь:**
3.2.1	
3.2.2	Проводить анализ научных данных, результатов экспериментов и наблюдений в области квантовых технологий
3.3	**Владеть:**
3.3.1	проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1. Введение в квантовые вычисления			
1.1	Квантовая гонка, квантовый компьютер, квантовые вычисления /Лек/	2	2	
	Раздел 2. Математические основы квантовых вычислений			
2.1	Линейное пространство. Линейные операторы. /Лек/	2	2	
2.2	Обратимые вычисления. Обратимые вентили /Лаб/	2	1	Практическая подготовка
2.3	Обратимые схемы. /Лаб/	2	1	Практическая подготовка
	Раздел 3. Квантовые схемы			
3.1	Кубит. Одно/двух/трехкубитовые вентили. /Лек/	2	2	
3.2	Простые квантовые схемы. Вычисление булевой функции. /Лек/	2	4	
3.3	Квантовая схема Базис Белла. /Лаб/	2	2	Практическая подготовка
3.4	Квантовая схема Reverse CNOT. /Лаб/	2	2	Практическая подготовка
3.5	Квантовая схема SWAP. /Лаб/	2	2	Практическая подготовка
3.6	Сложные квантовые схемы /Ср/	2	10	

	Раздел 4. Квантовые протоколы			
4.1	Квантовые протоколы передачи данных /Ср/	2	6	
4.2	Квантовые протоколы распределения ключей. /Лаб/	2	2	Практическая подготовка
4.3	Квантовые протоколы. ЭПР-протокол. /Лаб/	2	2	Практическая подготовка
	Раздел 5. Квантовые алгоритмы			
5.1	Алгоритм Дойча – Джозса. Алгоритм Бернштейна – Вазирани /Лаб/	2	2	Практическая подготовка
5.2	Алгоритм Саймона. Алгоритм Гровера. /Лаб/	2	2	Практическая подготовка
5.3	Квантовое преобразование Фурье. Алгоритм Шора /Лаб/	2	2	Практическая подготовка
5.4	Алгоритм Дойча /Ср/	2	4	
5.5	Алгоритм Бернштейна – Вазирани /Ср/	2	4	
5.6	Алгоритм Гровера /Ср/	2	4	
5.7	Языки квантового программирования /Ср/	2	8	
	Раздел 6. Квантовая коррекция ошибок			
6.1	Общая схема квантовых кодов. /Ср/	2	4	
6.2	Трехкубитовый квантовый код. /Ср/	2	4	
6.3	Алгоритмы QEC /Лаб/	2	2	Практическая подготовка
	Раздел 7. Самостоятельная работа			
7.1	Подготовка к лекциям /Ср/	2	5	
7.2	Подготовка к лабораторным занятиям /Ср/	2	20	
	Раздел 8. Контактные часы на аттестацию			
8.1	Зачет /КЭ/	2	0,15	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценочные материалы для проведения промежуточной аттестации обучающихся приведены в приложении к рабочей программе дисциплины.

Формы и виды текущего контроля по дисциплине (модулю), виды заданий, критерии их оценивания, распределение баллов по видам текущего контроля разрабатываются преподавателем дисциплины с учетом ее специфики и доводятся до сведения обучающихся на первом учебном занятии.

Текущий контроль успеваемости осуществляется преподавателем дисциплины (модуля), как правило, с использованием ЭИОС или путем проверки письменных работ, предусмотренных рабочими программами дисциплин в рамках контактной работы и самостоятельной работы обучающихся. Для фиксирования результатов текущего контроля может использоваться ЭИОС.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.2 Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)

6.2.1 Перечень лицензионного и свободно распространяемого программного обеспечения

6.2.1.1	Microsoft Windows10 Pro Договор №034210000481700004
6.2.1.2	Microsoft office 2013 (Лицензия № 61887848) Договор на поставку № 0342100004813000011
6.2.1.3	7-zip (http://www.7-zip.org/ (GNU LGPL license)

6.2.2 Перечень профессиональных баз данных и информационных справочных систем

6.2.2.1	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/
6.2.2.2	База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru

6.2.2.3	Портал для разработчиков электронной техники: http://www.espec.ws/
6.2.2.4	База данных «Библиотека программиста» https://proglib.io/
6.2.2.5	База данных «Отраслевой портал специалистов» http://www.connect-wit.ru/
6.2.2.6	Гарант.ру https://www.garant.ru/
6.2.2.7	КонсультантПлюс http://www.consultant.ru/
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	мультимедийное оборудование для предоставления учебной информации большой аудитории и/или звукоусиливающее оборудование (стационарное или переносное).
7.2	Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование и/или звукоусиливающее оборудование (стационарное или переносное)
7.3	Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.
7.4	Помещения для хранения и профилактического обслуживания учебного оборудования

Приложение к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Квантовые технологии

(наименование дисциплины(модуля)

09.04.02 Информационные системы технологии

(код и наименование)

Корпоративные информационные системы

(наименование)

Содержание

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Формы промежуточной аттестации: *зачет, семестр 2.*

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ПК-3: Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований	ПК-3.1

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы (семестр 4)
ПК-3.1: Проводит анализ научных данных, результатов экспериментов и наблюдений	Обучающийся знает: особенности проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий	Вопросы (№1 - №5)
	Обучающийся умеет: проводить анализ научных данных, результатов экспериментов и наблюдений в области квантовых технологий	Работа (№1 - №7)
	Обучающийся владеет: проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий	

Промежуточная аттестация (зачет) проводится в одной из следующих форм:
1) собеседование;
2) выполнение заданий в ЭИОС Университета.

2. Типовые[1] контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций

2.1 Типовые вопросы (тестовые задания) для оценки знаниевого образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ПК-3.1: Проводит анализ научных данных, результатов экспериментов и наблюдений	Обучающийся знает: особенности проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий

[1] Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники, технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

Примеры вопросов

1.Посредством чего удается обеспечить достоверный результат квантовых вычислений?
-Повторения квантовых вычислений несколько раз (+)
-Постепенного увеличения точности измерения результата и оценки возникающих -ошибок.
-Аппроксимации методом наименьших квадратов (МНК)
-Дополнительной обработки полученного результата дублирующей системой квантовых вычислений.

2.Каким образом определяют прослушивание канала связи в протоколе BB84?
-По отсутствию сигнала
-По повышенному количеству ошибок протокола (+)
-По наличию паразитного сигнала
-По снижению скорости передачи данных

3.К какому типу криптографии относится алгоритм AES?
-Криптография с закрытым ключом (+)
-Криптография с открытым ключом
-Постквантовая криптография
-Квантовая криптография

4.Принцип суперпозиции, приводит к:
-Детерминированному характеру квантовых вычислений
-Вероятностному характеру квантовых вычислений (+)
-Снижению точности квантовых вычислений
-Ограничению сфер применения квантовых технологий

5.Сколько, согласно тексту, можно выделить шагов в протоколе BB84?
-3 (+)
-4
-5
-6

2.2 Типовые задания для оценки навыкового образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ПК-3.1: Проводит анализ научных данных, результатов экспериментов и наблюдений	Обучающийся умеет: Проводить анализ научных данных, результатов экспериментов и наблюдений в области квантовых технологий
	Обучающийся владеет: проведения анализа научных данных, результатов экспериментов и наблюдений в области квантовых технологий

Примеры заданий

Работа 1. Элементарные квантовые алгоритмы

Цель работы: Изучение основных однокубитовых квантовых логических алгоритмов.
Объект исследования: Виртуальная лабораторная работа.
Задачи, решаемые в работе:
1. Изучение работы квантовых логических алгоритмов X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.
ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ
1. Студент подает кубит на вход известного логического элемента и получает выходной кубит. Результаты работы схемы сравниваются со свойствами алгоритма, известными из теории.
2. Используя матричное представление элемента, студент прогнозирует результаты виртуального эксперимента и сравнивает результаты теоретических и экспериментальных расчетов.
3. Студент распознает неизвестный однокубитовый квантовый логический элемент X, Z или H см. рис.3.
4. Распознавание неизвестного однокубитового квантового логического алгоритма.

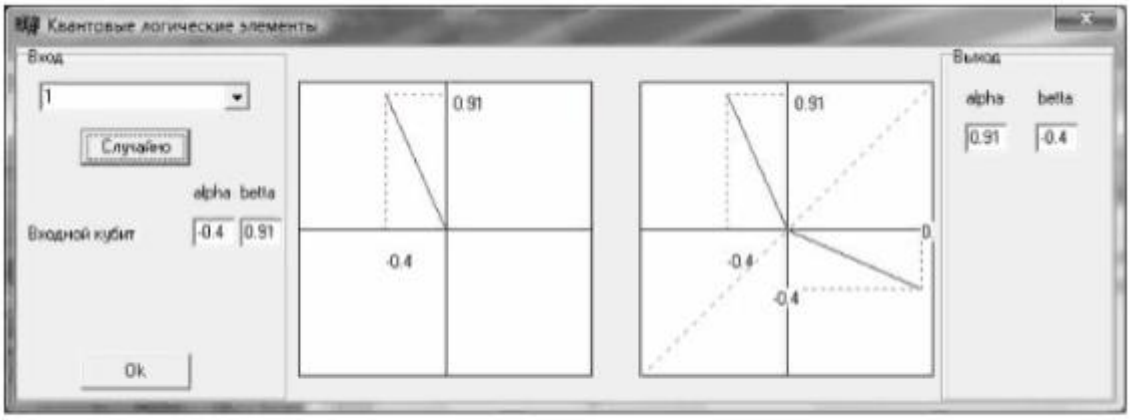

Рис.3. Исследование неизвестного квантового элемента

Работа 2. Однокубитовые квантовые схемы

Цель работы: Изучение простейших однокубитовых квантовых логических схем.

Объект исследования: Виртуальная лабораторная работа.

Задачи, решаемые в работе:

1. Изучение работы квантовых логических схем, составленных из элементов алгоритмов X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Студент выбирает несколько квантовых элементов, подает на вход цепочки элементов кубит, получает выходной кубит и, используя матричное представление схемы, сравнивает результаты теоретических расчетов с полученными экспериментальными данными – см. рис.5.

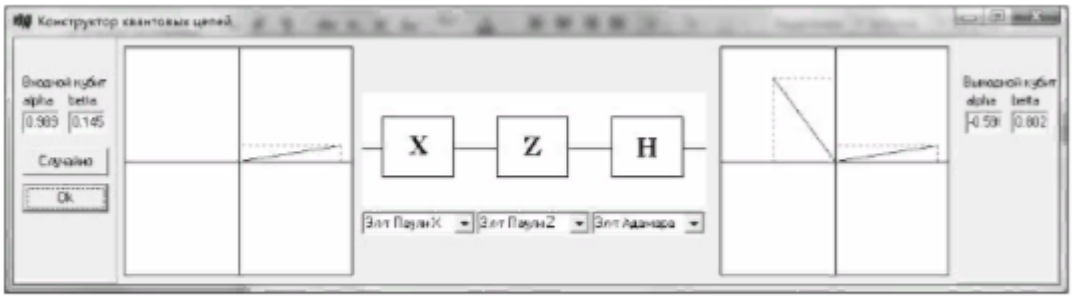

Рис.5. Исследование цепочки однокубитовых элементов

Работа 3. Двухкубитовые квантовые схемы

Цель работы: Изучение простейших двухкубитовых квантовых логических схем.

Объект исследования: Виртуальная лабораторная работа.

Задачи, решаемые в работе:

1. Изучение работы квантовых логических схем, составленных из элементов алгоритмов CNOT, X, Z и H.
2. Прогнозирование результатов виртуального эксперимента и сравнение результатов теоретических и экспериментальных расчетов.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Студент собирает квантовую схему используя квантовые логические элементы CNOT, X, H и Z, подает на вход цепочки элементов двухкубитовое состояние кубит, получает выходное двухкубитовое состоянии и, используя матричное представление схемы, сравнивает результаты теоретических расчетов с полученными экспериментальными данными – см. рис.1.

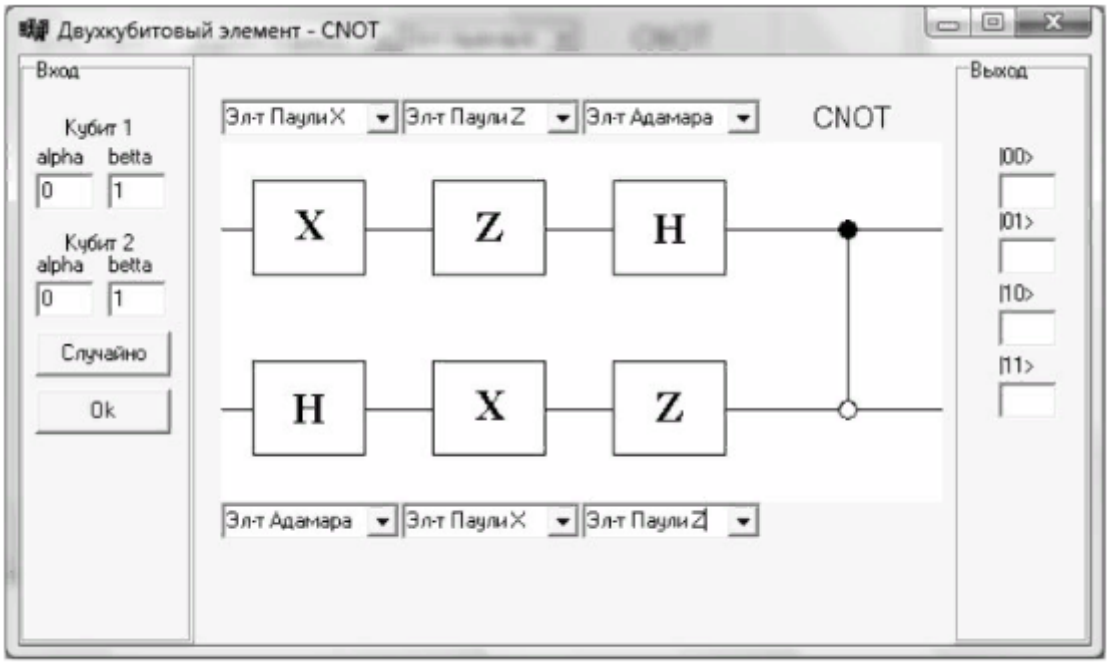

Рис.1. Исследование двухкубитовой квантовой схемы

Работа 4. Квантовый алгоритм Гровера

Цель работы: Изучение принципов работы алгоритма Гровера.

Объект исследования: Виртуальная лабораторная работа.

Задачи, решаемые в работе:

1. Изучение работы квантовой логической схемы, реализующей алгоритм Гровера.
2. Выбор свободных параметров алгоритма для получения требуемых результатов работы схемы.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В приложенном файле QGA.cmd смоделирован квантовый алгоритм Гровера. Задачу можно описать следующим образом: имеется база данных, состоящая из тридцати двух элементов (которые кодируются пятью кубитами), один из которых помечен. Вашей задачей является определить номер помеченного элемента. В вашем распоряжении имеется возможность указать сколько раз необходимо применить операторы контролируемой фазы и диффузии (второй шаг алгоритма Гровера), а также увидеть теоретические результаты измерений (распределение амплитуд вероятностей по элементам) и результаты того, что может получиться на практике (гистограмма результатов измерений ансамбля одинаковых состояний базы). Число кубитов системы (размер базы) менять не рекомендуется – при большем числе элементов (а число их растет как 2 n) наглядность схемы сильно ухудшится. В подразделе “Algorithm realization” описываются основные операторы, используемые в программе. Меняя число итераций второго шага алгоритма, изучите, как меняется распределение амплитуд вероятностей получить в результате поиска тот или иной элемент базы данных (в нашем случае чисел). Также определите количество повторений, при котором один из элементов базы появиться с вероятностью большей 95%. Как зависит это число от количества элементов в базе? Убедитесь, что при дальнейшем увеличении числа итераций эта амплитуда вероятности начнет уменьшаться. На гистограмме (рис.2) приводится результат 16-ти одинаковых измерений состояния базы. Высота столбика показывает, сколько раз в результате данного числа измерений получили заданное число. Это реальная ситуация того, что может получиться в эксперименте, когда теория предсказывает распределение, приведенное на рисунке 1. Меняя количество измерений, посмотрите, как гистограмма результатов будет приближаться к теоретическому распределению.

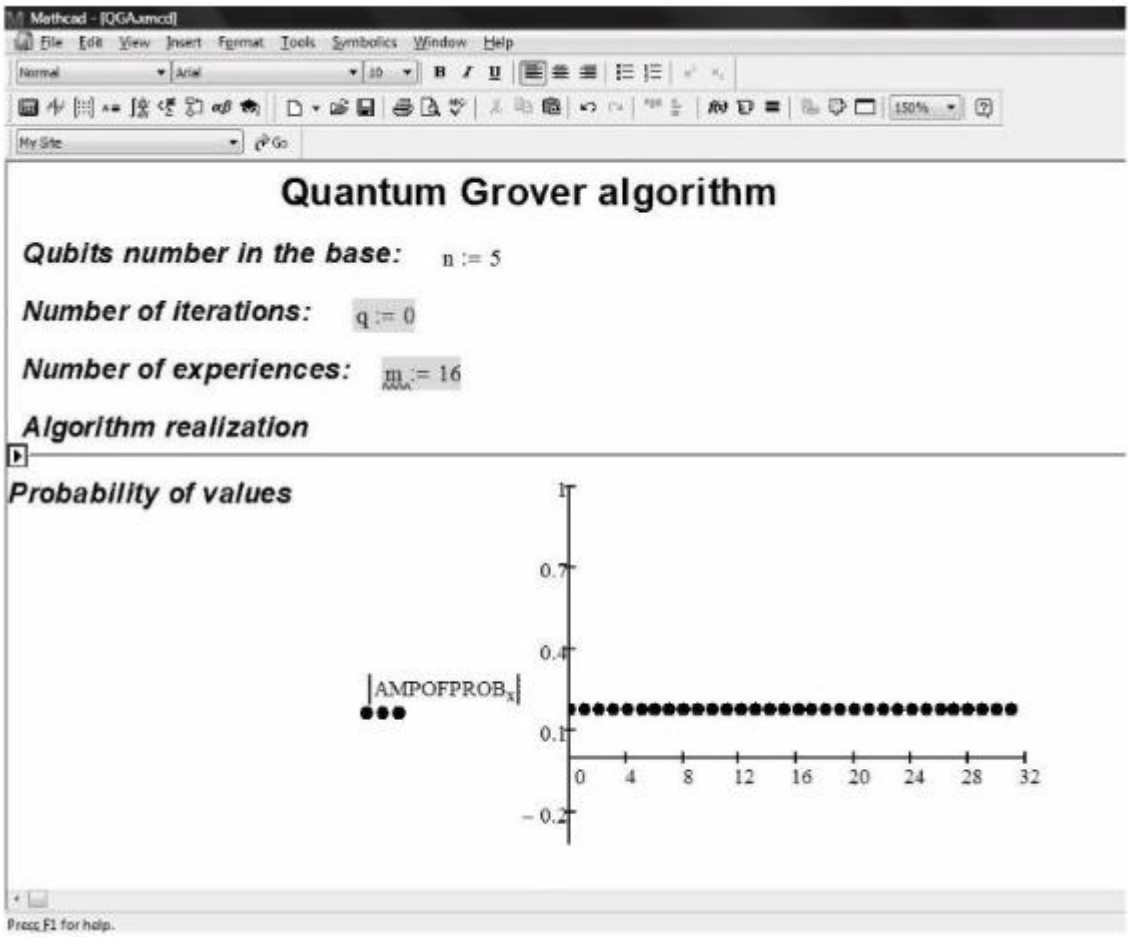

Рис.1. Реализация алгоритма Гровера: распределение амплитуд

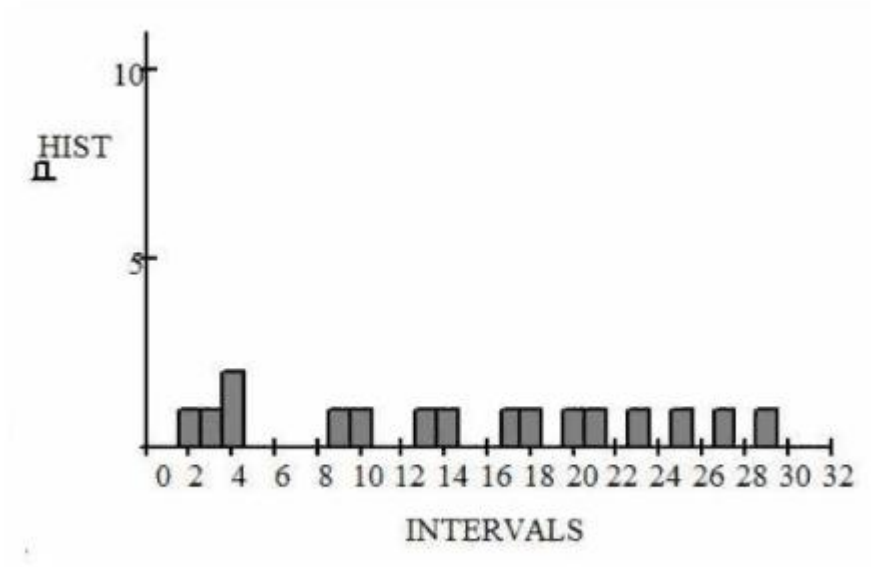

Рис.2. Гистограмма результатов эксперимента

Работа 5. Реализация квантового оптического вентиля CNOT

Цель работы: Изучение принципов работы М-схемы, реализующей квантовый оптический вентиль CNOT.

Объект исследования: Виртуальная лабораторная работа.

Задачи, решаемые в работе:

1. Изучение работы М-схемы, реализующей квантовый оптический вентиль CNOT.
2. Выбор свободных параметров для получения требуемых результатов работы схемы.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В приложенном файле CNOT.mcd смоделирована оптическая схема, на основе которой можно реализовать оптический логический элемент CNOT. В работе предлагается, меняя параметры этой системы добиться того, чтобы она осуществляла эту логическую операцию. В вашем распоряжении имеются однофотонные отстройки и частоты Раби, которые можно изменять (в файле они подсвечены зеленым цветом). Значения однофотонных отстроек Вам потребуется

изменять для того, чтобы получить нелинейные набеги фаз как показано в таблице 1. Для того, чтобы смоделировать ситуацию, когда одно из полей не находится в резонансном взаимодействии с соответствующим ему переходом, необходимо установить частоту Раби этого поля равной нулю. Другие значения частот Раби (кроме нуля и того, что приведено на рисунке) мы использовать не рекомендуем, так как для настройки схемы вполне достаточно однофотонных отстроек. Значения остальных параметров схемы, таких как фазовые сбои на переходах и ширины полос спонтанного распада, менять крайне не рекомендуется в связи с тем, что для их настройки требуется глубокий анализ всей схемы, что выходит за рамки
данной работы.

После того, как Вы установили пробные значения однофотонных отстроек, обратите внимание на оператор Гамильтона системы, который записан в резонансном приближении (объекты, за которыми необходимо наблюдать в работе отмечены светло-желтым цветом). На диагонали этого оператора стоят многофотонные отстройки, значения которых вычисляются по формулам, приведенном в подразделе “Two photon detunings”.

Далее следуют несколько подразделов, которые касаются программной реализации, изучение которых выводит за рамки данной работы. Следующим объектом, достойным внимания, служит матрица плотности атомной системы. Диагональ этой матрицы представляет собой вероятности найти электрон на данных атомных уровнях (номер строки
или столбца равен номеру атомного уровня).

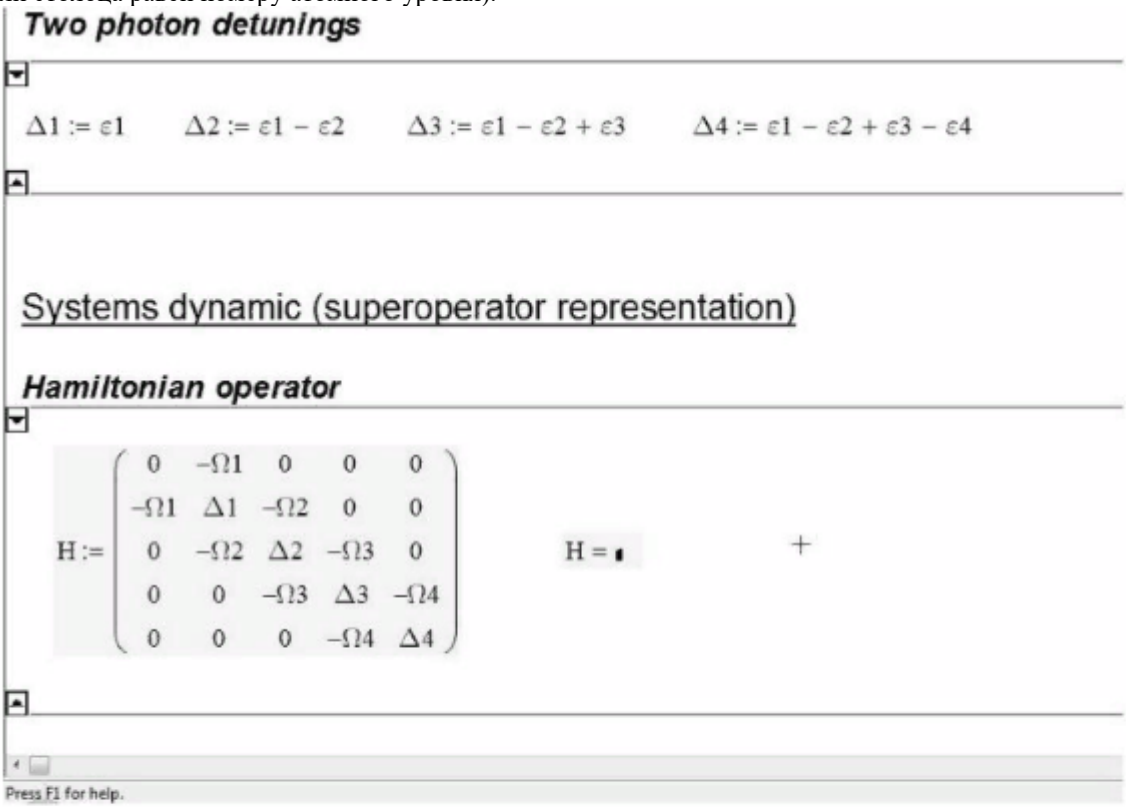

Рис.3. Оператор Гамильтона атомно-полевой системы; на диагонали находятся многофотонные отстройки, частоты Раби находятся на пересечении строки и столбца, номера которых совпадают с номерами атомных уровней на переходах, между которыми включено соответствующее поле

Недиагональные элементы матрицы представляют собой величины, пропорциональные электромагнитной восприимчивости, индуцированной на соответствующем переходе (переход между уровнями с номерами равными номерам строки и столбца). Коэффициент пропорциональности выбран равным единице. Особый интерес, как нетрудно догадаться, здесь представляют элементы 21 DM и 45 DM , так как равны (при выбранном коэффициенте пропорциональности) восприимчивостям на переходах, где нас интересует нелинейный фазовый набег поляризации поля. В файле приведена только вещественная часть элементов матрицы плотности, которая отвечает за дисперсию, тогда как мнимая часть отвечает за поглощение на данном переходе (см. закон Бугера).

На следующем этапе предлагается вычислить суммарный нелинейный набег фазы круговой поляризации полей 1 ω и 4 ω (нумерация строк и столбцов в MathCad начинается с нуля). Формула для его вычисления и получившееся значение (выраженное в радианах) приведены в следующем
подразделе.

Nonlinear phase shifts

Electromagnetic susceptibilities and corresponding conditional phase shifts

$\chi 12 := DM_{1,0}$ $\qquad$ $\chi 45 := DM_{3,4}$

$\phi 12 := 6 \cdot \pi \cdot Re\left(\sqrt{1 + 4 \cdot \pi \cdot \chi 12} - 1\right)$ $\qquad$ $\phi 45 := 6 \cdot \pi \cdot Re\left(\sqrt{1 + 4 \cdot \pi \cdot \chi 45} - 1\right)$

$\phi 12 = \blacksquare \cdot rad$ $\qquad$ $\phi 45 = \blacksquare \cdot rad$

$CPS := \phi 12 + \phi 45$ $\qquad$ $CPS = \blacksquare \cdot rad$

Рис.4. Расчет суммарного нелинейного набега фазы

В последней части работы предлагается сравнить работу реализованного устройства с теорией. Для этого необходимо составить оператор преобразования, которое выполняет система при данном наборе введенных Вами параметров. Он называется “yCPS ” (кратко your CPS) – наш оператор контролируемого набега фазы. Форма этого оператора взята из теоретической части (выражение (5)). Для его составления необходимо знать компоненты вектора “SCPS” (Summary CPS), которые представляют собой суммарные нелинейные набеги фаз круговой поляризации полей 1 ω и 4 ω для четырех различных комбинаций. Так первая компонента отвечает нелинейному набегу фаз, когда отсутствует резонансное взаимодействие этих полей с соответствующими переходами (устанавливаем соответствующие частоты Раби в ноль). Вторая компонента – результат резонансного взаимодействия поля 4 ω со «своим» переходом, когда у поля 1 ω такое взаимодействие отсутствует. Третья компонента – результат обратной ситуации. Четвертая – когда резонансное взаимодействие имеет место для обоих электромагнитных полей.
Далее следует наглядное сравнение операторов CPS и yCPS – идеальный и реальный случай. Также сравниваются операторы CNOT и yCNOT, которые получаются из CPS и yCPS соответственно преобразованием, риведенным в теоретической части (выражение (3)). Значение Posibility возвращает вероятность того, что при выбранных Вами параметрах
устройство сработает как CNOT.

Input summary conditional phase shifts into the vector

$SCPS = (\phi 00 \;\; \phi 01 \;\; \phi 10 \;\; \phi 11)$

$SCPS := \pi(\blacksquare \;\; \blacksquare \;\; \blacksquare \;\; \blacksquare)^T$

$$yCPS := \begin{pmatrix} \exp(-i \cdot SCPS_0) & 0 & 0 & 0 \\ 0 & \exp(-i \cdot SCPS_1) & 0 & 0 \\ 0 & 0 & \exp(-i \cdot SCPS_2) & 0 \\ 0 & 0 & 0 & \exp(-i \cdot SCPS_3) \end{pmatrix}$$

Рис.5. Построение “Вашего” оператора CPS.

При выбранных значениях однофотонных отстроек изучить вид оператора Гамильтона системы и матрицы плотности. Вычислить суммарные нелинейные набеги фаз для четырех возможных комбинаций круговых поляризаций электромагнитных полей 1 ω и 4 ω и составить вектор SCPS как описано выше. Сравнить получившиеся операторы yCPS и yCNOT с операторами, получающимися из теории. Вычислить вероятность корректного срабатывания Вашего устройства. Подбором
параметров добиться того, чтобы эта вероятность была не ниже 90%

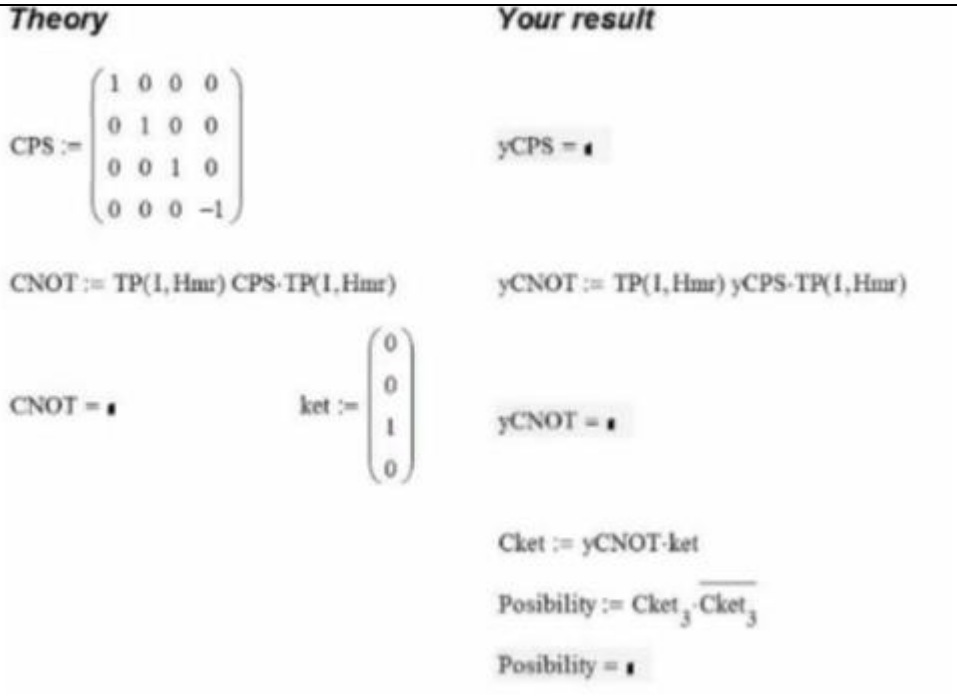

Рис.6. Сравнение результата (справа) с теорией (слева).

Работа 6

Генерация секретного ключа с помощью квантово- криптографической учебно-исследовательской установки на основе несимметричного волоконно- оптического интерферометра Майкельсона

Цель работы: Изучение основ квантовой криптографии.
Объект исследования: Plug&Play система квантовой криптографии,
работающая по протоколу B92 с использованием фазы излучения.
Задачи, решаемые в работе:
1. Генерация и рассылка секретного ключа.
2. Кодирование секретным ключом сообщения и передача сообщении
легитимному пользователю.
3. Декодирование сообщения.

Работа 7

Анализ шумов квантово – криптографической учебно-исследовательской установки на основе несимметричного волоконно-оптического интерферометра Майкельсона

Цель работы: Исследование шумов квантово-криптографической установки.
Объект исследования: Plug&Play система квантовой криптографии, работающая по протоколу B92 с использованием фазы излучения.
Задачи, решаемые в работе:
1. Определение процента ошибок в сыром криптографическом ключе.
2. Анализ ошибок, обусловленных темновыми отсчётами счётчика
фотонов

2.3. Перечень вопросов для подготовки обучающихся к промежуточной аттестации

1. Операторы Паули. Преобразование Адамара, интерферометр Маха-Цандера..

2. Требования, предъявляемые к квантовому компьютеру.
3. Уравнение Шредингера, теория представлений.
4. Чистые и смешанные состояния. Вычисление средних величин.
5. Матрица и оператор плотности.
6. Вычисление энтропии фон Неймана и Шеннона для конкретного состояния двухуровневой системы.
7. Основные модели квантовых состояний высокой размерности (D>2).
8. Интерференция одиночных фотонов и интерпретации интерференционных экспериментов.
9. Композиционные системы. Различие между классической и квантовой информацией. Достижимая информация. Теорема о запрете
клонирования квантовых состояний. Ее связь с достижимой информацией.
10. Теорема Б.Шумахера о кодировании при отсутствии шума.
11. Криптология, криптография и криптоанализ. Основные задачи криптографии. Понятия открытого текста, криптограммы, ключа и

криптосистемы. Принцип Керкхгоффа. Приложения криптографии.
12. Криптоанализ и основные виды атак. Подслушиватели (нарушители). Активный и пассивный, внутренний и внешний
подслушиватели.
13. Криптология, криптография и криптоанализ. Основные задачи криптографии. Понятия открытого текста, криптограммы, ключа и
криптосистемы. Принцип Керкхгоффа. Приложения криптографии.
14. Симметричные криптографические системы. Криптосистема с открытым ключом - асимметрия шифровки и дешифровки. Протокол
RSA.
15. Типы секретности сообщений (по Шеннону). Безусловно и условно стойкие шифры. Распределение ключей. Генерация ключей, их
хранение и уничтожение.
16. Одноключевые (симметричные) методы шифрования. Рассеивание и перемешивание. Понятие о криптосистемах DES и ГОСТ 28147-89,
их достоинства и недостатки. Основные проблемы симметричных протоколов. Аутентификация секретного ключа. Двухключевые
(асимметричные) методы шифрования. Механизм распределения ключей по открытому каналу по У.Диффи и М.Хеллману. Понятие о
криптосистемах RSA и Эль-Гамаля. Электронная подпись. Общая схема протокола квантового распределения ключей.
17. Вектор Джонса. Поляризационные преобразования. Фазовые пластинки. Некоторые сведения из теории квантовых измерений.
Сопряженные базисы.
18. Определение (I) неклассического света и его недостатки.
19. Состояния Белла, как частный случай перепутанных состояний (ПС). Преобразования состояний Белла при смене базиса.
20. Перепутывание по времени, временная пост-селекция. Пространственно-частотные, поляризационно-частотные, поляризационноугловые ПС. Амплитудная пост-селекция.
Чистые перепутанные состояния. Разложение Шмидта двухкомпонентной системы. Энтропия перепутывания. Степень перепутывания.
Локальные операции и классические сообщения. Параметр Федорова.
21. Парадокс ЭПР в варианте Бома.
22. Неравенства Белла. Классическая модель с двумя дихотомными переменными. Измеряемая Белла. Модель скрытых параметров.
Квантовая модель.
23. Парадокс Белла для трех наблюдаемых. Состояния Гринберга - Хорна - Цайлингера.
24. Протокол квантовой телепортации.
25. Протокол сверхплотной кодировки кубитов (dense coding).
26. Протокол обмена перепутыванием (swapping).
27. Измерительный (Борна) и проекционный постулаты (фон Неймана).
28. Понятие о квантовой томографии. Фиксированные и адаптивные протоколы.
29. Общие требования, необходимые для реализации полномасштабных квантовых компьютеров. Условия Ди Винченцо.
30. Основные физические модели для реализации квантовых вычислений

3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90% от общего объёма заданных вопросов;

- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76% от общего объёма заданных вопросов;

- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы –75–60 % от общего объёма заданных вопросов;

- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60% от общего объёма заданных вопросов.

Критерии формирования оценок по результатам выполнения заданий

«Отлично/зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов.

«Хорошо/зачтено» – ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета, не более трех недочетов.

«Удовлетворительно/зачтено» – ставится за работу, если обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой ошибки и двух недочетов.

«Неудовлетворительно/не зачтено» – ставится за работу, если число ошибок и недочетов превысило норму для оценки «удовлетворительно» или правильно выполнено менее 2/3 всей работы.

Виды ошибок:

- *грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.*

- *негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.*

- *недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.*

Критерии формирования оценок по зачету

«Зачтено» - обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности.

«Не зачтено» - выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.