

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультета Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Квантовая информация

Кафедра Информатики и Информационных Технологий

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

очная


Статус дисциплины:

Вариативная по выбору

Махачкала, 2018

Рабочая программа дисциплины " Квантовая информация " составлена в 2018 году в соответствии с требованиями ФГОС ВО по направлению 10.03.01 - Информационная безопасность (уровень бакалавриата) от 1 декабря 2016 г. №1515

Разработчик(и): кафедра ИиИТ

ст.пр. Муртузалиева А.А. 

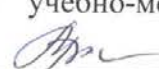
Рабочая программа дисциплины одобрена:

на заседании кафедры КИиИТ от "2" 07 2018г., протокол № 12

Зав.кафедрой  Ахмедов С.А.

на заседании Методической комиссии ФИиИТ от "3" 07 2018г., протокол № 10

Председатель  Камилов К.Б.

Рабочая программа дисциплины согласована с учебно-методическим управлением " " _____ 2018г. 

Аннотация рабочей программы дисциплины

Дисциплина "Квантовая информация" является дисциплиной *по выбору* образовательной программы *бакалавриата* по направлению 10.03.01 - Информационная безопасность.

Дисциплина реализуется на факультете ИиИТ кафедрой ИиИТ.

Содержание дисциплины охватывает круг вопросов, связанных с квантовыми вычислениями, квантовых компьютеров, квантовой телепортации и квантовой криптографии, проблемы декогеренции и спектроскопии одиночных молекул и примесных центров. Изучаются некоторые новые результаты в этой быстро развивающейся области исследований.

Дисциплина нацелена на формирование следующих компетенций выпускника:

Общепрофессиональных - ОПК-1, ОПК-2, ОПК-3,

профессионально-специализированных – ПСК-1.2, ПСК-1.3.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме *контрольная работа, коллоквиум и пр.* и промежуточный контроль в форме *зачета.*

Объем дисциплины 3 зачетных единиц, в том числе в академических часах по видам учебных занятий

Семес тр	Учебные занятия						СРС, в том числе экза мен	Форма промежуточной аттестации (зачет, дифференцирован ный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем							
	Всег о	из них						
Лекц ии		Лабораторн ые занятия	Практичес кие занятия	КСР	консуль тации			
6	108	36		18			54	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины «Квантовая информация» являются: освоение студентами общих закономерностей передачи, хранения и преобразования информации в микро- и нано-системах, подчиняющихся законам квантовой информации; квантовых алгоритмов решения вычислительных задач и физических принципов функционирования квантовых компьютеров; изучению различных аспектов квантовой информации, таких как меры информации и перепутанности, квантовые каналы и квантовые методы исправления ошибок; дать систематический обзор современных разработок безопасных протоколов передачи информации (квантовая криптография).

В результате изучения курса студент должен

Знать:

- основные понятия физики квантовой информации и квантовых вычислений;
- свойства, отличающие квантовую информацию от классической;
- физические и математические основы квантовых вычислений и принципов работы квантового компьютера;
- требования для физической реализации квантового компьютера и проблемы, которые необходимо решить для его создания.

Уметь выполнять операции с векторами в гильбертовом пространстве.

Владеть основными методами квантовых вычислений.

2. Место дисциплины в структуре ОПОП бакалавриата

Данная дисциплина входит в блок дисциплин по выбору образовательной программы. Для успешного освоения дисциплины необходимы знания и умения, полученные в результате изучения следующих дисциплин: «Информатика», «Физика», «Электротехника», «Языки программирования», «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Математическая логика и теория алгоритмов», «Теория вероятности и математическая статистика», «Криптографические методы защиты информации», «Криптографические протоколы», «Аппаратные средства вычислительной техники»

Освоение дисциплины «Квантовая информация» необходимо для последующего изучения дисциплин «Информационные технологии», «Техническая защита информации», «Программно-аппаратные средства защиты информации».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ОПК-1	способностью анализировать физические явления и процессы для решения профессиональных задач	знать: основные теоретические объекты квантовой физики, квантовой информации и квантовых вычислений; способы отображения квантовых состояний в абстрактном пространстве состояний чистых, смешанных и перепутанных состояний; проекционные представления квантовых состояний, особенности квантовых единиц информации; уметь: раскрывать основные постулаты квантовой механики и информатики; Владеть: основополагающими принципами и понятиями теории квантовой информации и квантовых вычислений; навыками описания состояний кубита; правилами составления квантовых логических цепей и навыками их изображения;
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать Основные понятия классической и квантовой теории информации, понимать их фундаментальные свойства и отличия. Уметь: Выполнять математические преобразования в системе квантовых вычислений. Владеть: математическим аппаратом в системе квантовых

		вычислений.
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знает Основные методы и подходы экспериментальных попыток реализации квантового компьютера, как физического устройства. Умеет: анализировать схемы реализации квантовых логических операций и квантовых алгоритмов. Владеет: обозначениями элементов квантовых логических цепей и правилами их составления; схемами управления кубитами.
ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	Знать Основные понятия классической и квантовой теории информации, понимать их фундаментальные свойства и отличия. Уметь: Выполнять математические преобразования в системе квантовых вычислений. Владеть: математическим аппаратом в системе квантовых вычислений.
ПСК-1.3	способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	Знать: алгоритмические основы классической и квантовой теории информатики. Уметь: Моделировать на классическом компьютере цепочки квантовых логических элементов для осуществления информационного процесса. Владеть: навыками построения и компьютерной реализации алгоритмов криптографии и криптоанализа;.

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетные единицы, 108 академических часа.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
Модуль 1.									
1	Логический аппарат квантовых вычислений	7		8	4			6	Устный опрос Доклад Контрольная работа
2	Квантовые протоколы передачи информации			6	4			8	Устный опрос Доклад Контрольная работа
Итого по модулю 1:				14	8			14	
Модуль 2.									
	Квантовые вычисления			12	6			18	Устный опрос Доклад Контрольная работа
Итого по модулю 2				12	6			18	
Модуль 3									
2	Квантовые компьютеры			10	4			22	Устный опрос Доклад Контрольная работа
Итого по модулю 3:				10	4			22	
ИТОГО:				36	18			54	

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль1.

1.Введение Краткая история развития квантовых вычислений.

2 Логический аппарат квантовых вычислений

Квантовые биты (кубиты) и их свойства.

Однокубитные преобразования.

Многокубитные системы, их описание векторами гильбертова пространства.

Многокубитные преобразования.

Элементарные наборы операторов.

Особенности квантовых вычислений.

3 Квантовые протоколы передачи информации

Плотное кодирование.

Квантовая телепортация.

Квантовые протоколы передачи секретного ключа.

Модуль2.

4 Квантовые вычисления

Квантовое преобразование Фурье.

Алгоритм Шора.

Алгоритм Гровера.

Коррекция ошибок в квантовых вычислениях.

Модуль3.

5 Квантовые компьютеры

Требования к квантовым компьютерам.

Устройство квантового компьютера на ионах в ловушках.

Другие возможные реализации квантовых компьютеров: жидкостные и твердотельные квантовые компьютеры на ЯМР, компьютеры на квантовых точках.

4.3.2. Содержание лабораторно-практических занятий по дисциплине.

7 СЕМЕСТР

№ п/п	№ раздела дисциплины	□ Темы практических занятий	Время на выполнение работы, ч
1.	1-2	Квантовая информатика как наука на стыке квантовой механики и теории информации. Из истории вопроса. Физические принципы, лежащие в основе квантовой информатики.	2
□2	3-5.	Кубит как элементарная квантовая информационная ячейка. Логические элементы как базисные состояния кубита и принцип суперпозиции. Примеры физических систем, реализующих кубиты: спин, поляризационные состояния фотона, двухуровневая система	4
□3	6-8.	□Квантовый n-кубитовый регистр и его информационная емкость. Проекционный постулат и измерение квантовых состояний. Измерение состояния квантового регистра	2
4	9-11.	□Парадокс Эйнштейна-Подольского-Розена и физическая нелокальность. Концепция перепутывания квантовых состояний подсистем. ЭПР-пары. Неравенства Белла и эксперименты по их верификации. Примеры перепутанных состояний для двухкубитовых систем. Состояния Белла как максимально перепутанные состояния. Преобразование состояний Белла при изменении базиса. Меры перепутывания	2
5	12-14.	Основные квантовые логические операции- Унитарные матрицы и однокубитовые гейты: NOT, преобразование Адамара и другие.- Физическая реализация однокубитовых гейтов: спин в магнитном поле, фазовая пластинка, светоделитель, двухуровневая система в резонансном поле. - Необходимость двухкубитовых гейтов. Двухкубитовый гейт CNOT.	4

□6	6.	□Квантовые вычисления - Унитарные преобразования гильбертова пространства состояний n-кубитового регистра. - Локальные логические операции и квантовое параллельное вычисление – квантовый параллелизм.	4
	итого		18

5. Образовательные технологии

В аудитории проводятся лекции и практические (семинарские) занятия. Лекционные занятия освещают концептуальные и теоретические вопросы. На них обучаемым предлагается базовый материал курса. Лекционные занятия проводятся с применением мульти-медийных средств. Семинарские занятия проводятся с целью закрепления лекционного материала с помощью показа и разбора конкретных примеров, обсуждения проблемных вопросов, а также освоения конкретных языков и систем, а также получения навыков решения задач с использованием изученных систем. На семинарских занятиях студенты выступают с презентациями докладов, подготовленных ими по заданной теме.

Самостоятельная работа выполняется студентами по предлагаемым темам, в том числе выбранным для самостоятельного изучения. Некоторые из них докладываются на семинарах с последующим обсуждением студентами. Коллоквиумы проводятся с целью закрепления лекционного материала и контроля знаний обучающихся. Консультации по курсу учебным планом не регламентируются. Они проводятся в форме ответов на вопросы студентов и обсуждений.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Список тем для изучения

1. Использование формализма Дирака для представления векторов и операторов. Соотношение полноты в гильбертовом пространстве.
2. Спектральное разложение эрмитова оператора. Свойства собственных чисел и собственных векторов.
3. Классическое и квантовое описание статистического эксперимента, их сходство и отличия.
4. Матрица плотности. Классическое и квантовое чистое состояние. Вектор состояния.
5. Определение и свойства проекционного оператора. Разложение единицы (спектральная мера).
6. Спектральное разложение эрмитова оператора в терминах проекторов на собственные под-пространства.
7. Статистический постулат Борна-фон Неймана. Математическое ожидание и распределение вероятностей квантовой наблюдаемой.
8. Пространство состояний q-бита. Шар Блоха. Векторы чистых состояний.
9. Свойства матриц Паули. Наблюдаемая «проекция спина».
10. Функции от эрмитова оператора. Совместимые наблюдаемые.
11. Соотношение неопределенностей.
12. Проекционный постулат фон Неймана-Людерса. Изменение квантового состояния в результате измерения. Апостериорное состояние.
13. Определение и свойства унитарного оператора. Динамический постулат квантовой механики. Уравнение Шредингера.
14. Состояния составной квантовой системы. Тензорное произведение векторов, матриц и операторов.
15. Пространство состояний системы из n q-битов. Одно- и двух- q-битные операции. 16. Сцепленное (запутанное) состояние. Разложение Шмидта.
17. Протокол сверхплотного кодирования.
18. Протокол телепортации квантового состояния.
19. Протокол BB84 квантового распределения секретного ключа.
20. Алгоритм Дойча.

21. Алгоритм Саймона.

22. Алгоритм Гровера.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Процедура освоения
ОПК-1	способностью анализировать физические явления и процессы для решения профессиональных задач	знать: основные теоретические объекты квантовой физики, квантовой информации и квантовых вычислений; способы отображения квантовых состояний в абстрактном пространстве состояний чистых, смешанных и перепутанных состояний; проекционные представления квантовых состояний, особенности квантовых единиц информации; уметь: раскрывать основные постулаты квантовой механики и информатики; Владеть: основополагающими принципами и понятиями теории квантовой информации и квантовых вычислений; навыками описания состояний кубита; правилами составления квантовых логических цепей и навыками их изображения;	Устный опрос, письменный опрос, доклад, реферат
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать Основные понятия классической и квантовой теории информации, понимать их фундаментальные свойства и отличия. Уметь: Выполнять математические преобразования в системе квантовых вычислений. Владеть: математическим аппаратом в системе квантовых вычислений.	Устный опрос, письменный опрос, доклад, реферат
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знает Основные методы и подходы экспериментальных попыток реализации квантового компьютера, как физического устройства. Умеет: анализировать схемы реализации квантовых логических операций и квантовых алгоритмов. Владеет: обозначениями элементов квантовых логических цепей и правилами их составления; схемами управления кубитами.	Устный опрос, письменный опрос, доклад, реферат
ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	Знать Основные понятия классической и квантовой теории информации, понимать их фундаментальные свойства и отличия. Уметь: Выполнять математические преобразования в системе квантовых вычислений. Владеть: математическим аппаратом в системе квантовых вычислений.	Устный опрос, письменный опрос, доклад, реферат

ПСК-1.3	способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	Знать: алгоритмические основы классической и квантовой теории информатики. Уметь: Моделировать на классическом компьютере цепочки квантовых логических элементов для осуществления информационного процесса. Владеть: навыками построения и компьютерной реализации алгоритмов криптографии и криптоанализа;	Устный опрос, письменный опрос, доклад, реферат
----------------	---	--	---

7.2. Типовые контрольные задания

Приблизительные вопросы для контрольной работы или зачета.

1. Бра- и кет-вектора. Операторы, унитарные операторы.
2. Кубиты и квантовые гейты.
3. Операторы Адамара, Уолша-Адамара, NOT, CNOT, управляемого обмена.
4. Квантовый параллелизм.
5. Квантовые схемы.
6. Плотное кодирование.
7. Квантовая телепортация.
8. Протокол передачи ключа.
9. Квантовое преобразование Фурье.
10. Алгоритм Шора.
11. Алгоритм Гровера.
12. Декогеренция квантовых состояний.
13. Источники ошибок в квантовых вычислениях. Алгоритмы коррекции ошибок.
14. Требования к квантовым компьютерам.
15. Устройство квантового компьютера на ионах в ловушках.

7.3. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 50 % и промежуточного контроля - 50 %.

Текущий контроль по дисциплине включает:

- посещение занятий - 10 баллов,
- участие на практических занятиях - 30 баллов,
- выполнение лабораторных заданий - баллов,
- выполнение домашних (аудиторных) контрольных работ - 10 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 20 баллов,
- письменная контрольная работа - 20 баллов,
- тестирование - 10 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Квантовая информация и квантовые вычисления : [в 2-х т.]. Т.1 / пер. с англ. Т.С.Нечаевой под науч. ред. С.С.Епифанова и С.Г.Новокшонова. - М.; Ижевск : НИЦ "Регуляр. и хаотич. динамика"; Изд-во Ин-та компьют. исслед., 2008. - 462 с. - ISBN 978-5-93972-651-1 : 200-00.

2. Прескилл, Джон. Квантовая информация и квантовые вычисления : [в 2-х т.]. Т.2 / пер. с англ. Т. С. Нечаевой; под науч. ред. С. Г. Новокшенова. - М.; Ижевск : НИЦ "Регуляр. и хаотич. динамика"; Изд-во Ижев. ин-та компьют. исслед., 2011. - 311 с. - Библиогр.: с. 202-203. - Библиогр. в конце прил. - ISBN 978-5-4344-0030-5 : 210-00.
3. Имре, Шандор. Квантовые вычисления и связь. Инженерный подход / пер. с англ. А.А.Калачёва, Т.Г.Митрофановой, С.В.Петрушкина, В.В.Самарцева; под ред. В.В.Самарцева. - М. : ФИЗМАТЛИТ, 2008. - 319 с. - Библиогр.: с. 306-315. - ISBN 978-5-9221-0993-2 : 431-97.
4. Чивилихин С.А. Квантовая информатика [Электронный ресурс] : учебное пособие / С.А. Чивилихин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2009. — 80 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/66501.html>
5. Ильичев Е.В. Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур [Электронный ресурс] : учебник / Е.В. Ильичев, Я.С. Гринберг. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2013. — 170 с. — 978-5-7782-2287-8. — Режим доступа: <http://www.iprbookshop.ru/45122.html>

б) дополнительная литература:

1. Брайан Клегг Квантовая теория [Электронный ресурс] / Клегг Брайан. — Электрон. текстовые данные. — М. : РИПОЛ классик, 2014. — 160 с. — 978-5-386-07920-8. — Режим доступа: <http://www.iprbookshop.ru/71429.html>
2. Квантовая информатика. Лабораторный практикум [Электронный ресурс] : учебное пособие / Ю.Т. Мазуренко [и др.]. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2009. — 59 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/66500.html>
3. Стин, Эндрю. Квантовые вычисления : пер. с англ. - Ижевск : Регуляр. и хаотич. динамика, 2000. - 111 с. - ISBN 5-93972-023-4 : 0-0.
4. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики. – М.: МИФИ, 2004. – 80с
5. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация: Пер. с англ. – М.: Мир, 2006г. – 824с.
6. Боумейстер Д., Экерт А., Цайлингер А. Физика квантовой информации. – М.: Постмаркет, 2002. - 376 с.
7. Холево А.С. Введение в квантовую теорию информации. – М.: МЦНМО, 2002. - 228 с.
8. А. С. Холево, Квантовые системы, каналы, информация. МЦНМО 2010.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: <http://elibrary.ru/defaultx.asp> (дата обращения: 01.09.2018). – Яз. рус., англ.
2. Moodle[Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.dgu.ru/>(датаобращения: 22.08.2018).
3. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: <http://elib.dgu.ru>, свободный (дата обращения: 21.09.2018).
4. Сайт кафедры <http://iit.dgu.ru/> (дата обращения 15.09.2018)

5. Национальный Открытый Университет «ИНТУИТ» – <http://www.intuit.ru/>(дата обращения 15.09.2018)
6. Интернет-энциклопедия «Википедия». – <https://ru.wikipedia.org/>(дата обращения 15.09.2018)
7. Учебные курсы — Кафедра теоретической физики – МФТИ
http://theorphys.mipt.ru/courses/stat-eko/part1_a5-arpe0hsla66.pd/ (дата обращения 20.09.2018)

10. Методические указания для обучающихся по освоению дисциплины.

Дисциплина рассматривает математические абстракции, помогающие качественно и количественно описывать сложные системы, но в отрыве от практических навыков пользу математических абстракций невозможно осознать и почувствовать их практическую значимость.

Для более полного понимания целей, задач и практических результатов теории систем следует:

- 1) Ознакомиться с дополнительной литературой, особенно с трудами основоположников.
- 2) Ознакомиться, хотя бы поверхностно, с другими подходами к построению систем (см. доп. литературу).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Предусмотрено использование электронной почты для связи студентов с преподавателями.

Программное обеспечение для лекций: MS PowerPoint (MS PowerPoint Viewer), Adobe Acrobat Reader, средство просмотра изображений, табличный процессор.

Программное обеспечение практической работы компьютерном классе: Linux, MS PowerPoint (MS PowerPoint Viewer), Adobe Acrobat Reader, средство просмотра изображений, Интернет, E-mail.

Программные продукты

- Операционная система: Windows7
- Microsoft office.
- Программные средства сжатия данных. . WinRAR. WinArj. WinZip.

<http://www.dgu.ru>

<http://ru.wikipedia.org/wiki/Википедия>

<http://www.chaynikam.info/foto.html> Компьютер для «чайников»

<http://urist.fatal.ru/Book/Glava8/Glava8.htm> Электронные презентации

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Реализация учебной дисциплины требует наличия типовой учебной аудитории с возможностью подключения технических средств. Учебная аудитория должна иметь следующее оборудование:

- Компьютер, медиа-проектор, экран.
- Программное обеспечение для демонстрации слайд-презентаций.