

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 30.04.2025 11:55:50
Уникальный программный ключ:
03474917c4d012283e5ad996e48a5e701f81b0257

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и
автоматизации производственных процессов
Кафедра интеллектуальных систем и информационной безопасности



УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Квантовые вычисления и квантовая криптография
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Квантовые вычисления и квантовая криптография» является предоставить студентам знание элементов квантовой механики, реализация квантовых вычислений..

Задачи изучения дисциплины:

- изучение принципов работы квантовые компьютеры и их физической реализации, квантовых схем и алгоритмов;
- изучение алгоритмов факторизации и дискретного логарифмирования; выработка умений применять полученные теоретические сведения для решения практических задач.

Дисциплина направлена на формирование общепрофессиональных (ОПК-3, ОПК-4) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Алгебра», «Математический анализ», «Дискретная математика», «Теория вероятностей, математическая статистика и случайные процессы», «Математическая логика и теория алгоритмов», «Теория информации», «Физика», «Основы информационной безопасности», «Криптографические методы защиты информации», «Математика криптографии».

Является основой для изучения следующих дисциплин: «Преддипломная практика», «Выполнение и защита выпускной квалификационной работы».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с научно-исследовательской работой.

Курс является фундаментом для ориентации студентов в сфере научных исследований.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ч.), лабораторные (18 ч.) занятия и самостоятельная работа студента (90 ч.).

Дисциплина изучается на 5 курсе в 10 семестре. Форма промежуточной аттестации – дифференцированный зачет.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Квантовые вычисления и квантовая криптография» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен использовать математические методы необходимые для решения задач профессиональной деятельности	ОПК-3	ОПК-3.2 Использует математические методы, необходимые для решения задач профессиональной деятельности
Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4	ОПК-4.2 Применяет основные физические законы и модели для решения задач профессиональной деятельности

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к дифференцированному зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		4
Аудиторная работа, в том числе:	54	54
Лекции (Л)	36	36
Практические занятия (ПЗ)	–	–
Лабораторные работы (ЛР)	18	18
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	90	90
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	–	–
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	12	12
Домашнее задание	6	6
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к дифзачету	9	9
Промежуточная аттестация – дифференцированный зачет (Д/З)	Д/З	Д/З
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 3 темы:

- тема 1 (Элементы квантовой механики. Квантовые вычисления, квантовые компьютеры и их физическая реализация);
- тема 2 (Квантовые схемы и алгоритмы);
- тема 3 (Квантовая криптография).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Элементы квантовой механики. Квантовые вычисления, квантовые компьютеры и их физическая реализация	Элементы квантовой механики: постулаты, бра- и кет-формализм, основные теоремы Квантовые вычисления, квантовые компьютеры и их физическая реализация	6 6	Бра- и кет-формализм, операторные функции, разложения операторов. Одно- и много-кубитовые элементы. Квантовые схемы. Состояния Белла. Квантовая телепортация.	4 4	—	—

Завершение таблицы 3.

1	2	3	4	5	6	7	8
2	Квантовые схемы и алгоритмы	Квантовые схемы и алгоритмы Алгоритмы факторизации и дискретного логарифмирования.	6 4	Квантовый параллелизм. Алгоритмы Дойча и Дойча-Йожа. Операции на одном кубите. Условные операции. Универсальные квантовые элементы.	4 4 4	—	—
3	Квантовая криптография	Квантовая информация и исправление квантовых ошибок. Квантовая криптография.	6 8	Квантовое преобразование Фурье Алгоритмы факторизации и дискретного логарифмирования Симплектические коды Квантовое распределение ключей	4 4 6 6	—	—
Всего аудиторных часов		36		36		—	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-3	Дифференцированный зачет	Комплект контролирующих материалов для дифзачета

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– практические занятия – всего 100 баллов.

Оценка по дифзачету проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Дифзачет по дисциплине «Квантовые вычисления и квантовая криптография» проводится по результатам работы в семестре. В случае если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание № 1.

С помощью алгоритма Шора факторизовать число 15. Для этого необходимо построить схему для $a^x \bmod N$, добавить QFT^{-1} для получения r – количества столбцов и выделить простые множители, входящие в число 15.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

1. Квантовые гейты и кубиты
2. Квантовая декогерентность
3. Квантовый алгоритм Гровера
4. Квантовый алгоритм Шора
5. Универсальность квантовых вычислений
6. Квантовые алгоритмы
7. Квантовая телепортация
8. Квантовая информатика
9. Квантово-полевая картина мира
10. Возникновение и развитие квантовой физики.
11. Единая квантовая теория.
12. Основные квантово-механические принципы.
13. Принцип неопределенности Гейзенберга.
14. Квантовая физика как новый этап изучения природы
15. Хаос, необратимость времени и брюссельская интерпретация квантовой механики
16. Квантовые свойства макроскопических объектов.
17. Принцип неопределенности Гейзенберга.
18. Парадокс Эйнштейна-Подольского-Розена.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1. Элементы квантовой механики. Квантовые вычисления, квантовые компьютеры и их физическая реализация.

1. В чем заключается проблема выбора базиса в квантовых схемах:

- а) бесконечное множество унитарных операторов
 - б) конечное множество унитарных операторов
 - в) нет верного ответа
2. Решение проблемы выбора базиса в квантовых схемах связано с:
- а) необходимостью содержания бесконечного множества элементов в полном базисе
 - б) возможностью ослабления условия точной реализуемости оператора схемой
 - в) необходимостью введения эрмитово сопряженного оператора
3. Условие приближенной реализуемости:
- а) предназначено для решения проблемы выбора базиса в квантовых схемах
 - б) является заменой условия точной реализуемости
 - в) нет верного ответа
4. Возможность точной реализации оператора квантовой схемой связана с использованием:
- а) эрмитово сопряженного оператора
 - б) оператора с квантовым управлением
 - в) оператора проектирования
5. Автором "задачи о скрытой группе" является
- а) Саймон
 - б) Гровер
 - в) Черч

Тема 2. Квантовые схемы и алгоритмы

1. Решение универсальной переборной задачи алгоритмом Гровера -
- а) является единственным нетривиальным использованием квантовых свойств для вычислений
 - б) дает следствия для теории сложности вычислений
 - в) дает полиномиальное ускорение
2. Выберите верное утверждение:
- а) косвенным свидетельством превосходства по скорости квантовых вычислений над классическими является задача с оракулом
 - б) доказано, что квантовые вычисления значительно превосходят по скорости классические вероятностные вычисления
 - в) любой классический вероятностный алгоритм является экспоненциальным
3. Для любого классического вероятностного алгоритма, делающего не более $2^{k/2}$ обращений к оракулу ($n \geq k$), существует подгруппа $D \subseteq (2)^k$ и соответствующая функция $f: (2)^k \rightarrow \{0,1\}$, для которой вероятность ошибки

алгоритма:

а) $< 1/3$

б) $> 1/3$

в) $< 1/2$

4. Автором каких квантовых алгоритмов является П. Шор:

а) алгоритм нахождения скрытой группы

б) алгоритм разложения числа на простые множители

в) алгоритм вычисления дискретного логарифма

5. Какую сложность имеет алгоритм нахождения скрытой группы $(2)^k$:

а) $O(k^2)$

б) $O(k^3)$

в) $O(k)$

Тема 3. Квантовая криптография.

1. Посредством чего удастся обеспечить достоверный результат квантовых вычислений?

а) повторения квантовых вычислений несколько раз

б) постепенного увеличения точности измерения результата и оценки возникающих ошибок.

в) аппроксимации методом наименьших квадратов (МНК)

г) дополнительной обработки полученного результата дублирующей системой квантовых вычислений

2. Каким образом определяют прослушивание канала связи в протоколе BB84?

а) по отсутствию сигнала

б) по повышенному количеству ошибок протокола

в) по наличию паразитного сигнала

г) По снижению скорости передачи данных

3. К какому типу криптографии относится алгоритм AES?

а) криптография с закрытым ключом

б) криптография с открытым ключом

в) постквантовая криптография

г) квантовая криптография

4. Принцип суперпозиции, приводит к:

а) детерминированному характеру квантовых вычислений

б) вероятностному характеру квантовых вычислений

в) снижению точности квантовых вычислений

г) ограничению сфер применения квантовых технологий

5. Сколько, согласно тексту, можно выделить шагов в протоколе BB84?

- а) 3
- б) 4
- в) 5
- г) 6

6.5 Вопросы для подготовки к дифзачету

- 1) Как развивались квантовые вычисления и квантовая информация?
- 2) Каково современное состояние и перспективы квантовых вычислений?
- 3) Что такое линейные пространства и операторы?
- 4) Что такое матрицы Паули?
- 5) Что такое собственные значения и векторы?
- 6) Что такое эрмитовы операторы?
- 7) Какие Вы знаете операторные функции? Что такое коммутации?
- 8) Как производится полярное разложение и разложение по сингулярным числам?
- 9) Что такое пространство состояний и эволюция? Что такое квантовые измерения?
- 10) Что такое проективные и POVM-измерения? Что такое фаза?
- 11) Какие Вы знаете составные системы?
- 12) Что такое кубит?
- 13) Что такое сверхплотное кодирование? Что такое оператор плотности?
- 14) Что такое разложение Шмидта?
- 15) Что такое Парадокс Эйнштейна-Подольского-Розена? Что такое неравенства Белла?
- 16) Что такое квантовые алгоритмы? Какие Вы знаете операции на одном кубите?
- 17) Какие Вы знаете универсальные квантовые элементы?
- 18) Как производится моделирование квантовых систем?
- 19) Что такое измерения в базисах, отличных от вычислительного? Что такое квантовые схемы?
- 20) Что такое состояния Белла? Что такое квантовая телепортация?
- 21) Как производится классические вычисления на квантовом компьютере?
- 22) Что такое квантовый параллелизм?
- 23) Что такое алгоритм Дойча?
- 24) Что такое алгоритм Дойча-Йожа? Каковы перспективы практической обработки квантовой информации?
- 25) Что такое квантовое преобразование Фурье?

- 26) Что такое собственное число?
- 27) Как производится нахождение порядка и факторизация?
- 28) Как производится нахождение периода? Что такое дискретный логарифм?
- 29) Как формулируется задача о скрытой подгруппе? Каковы возможные эффективные квантовые алгоритмы?
- 30) Что такое квантовый алгоритм поиска и квантовое моделирование?
- 31) Как производится ускорение решения NP-полных задач? Что такое оптимальность алгоритма поиска?
- 32) Как формулируется теорема Готтесмана-Нилла?
- 33) Что такое запутанность как физический ресурс?
- 34) Что такое алгоритм Шора и каковы возможности его применения?
- 35) Как производится представление квантовой информации?
- 36) Как производится реализация унитарных операторов?
- 37) Как производится приготовление начального состояния? Как производится измерение конечного результата?
- 38) Что такое гармонический осциллятор, оптические фотоны, оптические резонаторы, ионные ловушки, ЯМР?

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Душкин, Роман Викторович. Квантовые вычисления и функциональное программирование / Р. В. Душкин. — 2-е изд., эл. — 1 файл pdf: 233 с. — Москва : ДМ К Пресс, 2023. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5; экран 10". — Текст: электронный. — [Электронный ресурс] — Режим доступа: <https://znanium.ru/read?id=435462> (Дата обращения 26.08.2024).

Дополнительная литература

1. Прескилл Дж. Квантовая информация и квантовые вычисления. /Дж. Прескилл. — Ижевск: НИЦ Регулярная и хаотическая динамика, 2011. — 464 с. — [Электронный ресурс] — Режим доступа: <https://djvu.online/file/lp2DRLaBI0n9p> . (Дата обращения 26.08.2024).

2. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. - М.: Мир, 2006. - 824 с. — [Электронный ресурс] — Режим доступа: <https://djvu.online/file/cO8qDRGAwOIe2> . (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education.— Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/>.— Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x>.— Текст : электронный.

4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red.— Текст : электронный.

5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: <http://www.iprbookshop.ru/>. —Текст : электронный.

6. Сайт кафедры ИСИБ <http://scs.dstu.education>

Материально-техническое обеспечение представлено в таблице 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: <i>Мультимедийная аудитория. (60 посадочных мест), оборудованная специализированной (учебной) мебелью (скамья учебная – 20 шт., стол – 1 шт., доска аудиторная – 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран.</i> Аудитории для проведения лекций: <i>Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:</i>	ауд. <u>207</u> корп. <u>4</u> ауд. <u>217</u> корп. <u>3</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования РПД

Разработал:

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(должность)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедрыот 27.08.2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)


(подпись)

В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по направлению 10.05.03
Информационная безопасность
автоматизированных систем


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра


(подпись)

О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	