

**МИНОБРНАУКИ РОССИИ**  
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

**Рабочая программа дисциплины**  
**Защита систем квантовой связи**

Направление подготовки (специальности)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2023 г.

## 1. Цели освоения дисциплины

Целью освоения дисциплины «Защита систем квантовой связи» является приобретение обучающимися теоретических и практических навыков обеспечения информационной безопасности в системах квантовой связи. Дисциплина обеспечивает приобретение знаний и умений в области использования систем квантовой связи и квантовых вычислений, разработки криптографических протоколов, обеспечивающих безопасность в системах квантовой связи, способствует освоению принципов корректного применения современных и перспективных технологий защиты информации.

Задачи дисциплины:

- формирование общих представлений о квантово-механических методах, лежащих в основе обеспечения информационной безопасности, а также основных квантово-криптографических протоколах;
- ознакомление с принципами квантовых вычислений, с квантовыми алгоритмами, направленными на анализ существующих систем криптографии с открытым ключом;
- ознакомление с перспективными физическими платформами для создания квантовых вычислительных систем;
- ознакомление с системами квантового распределения ключей.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита систем квантовой связи» относится к вариативной части образовательной программы и является дисциплиной по выбору.

Для освоения данной дисциплиной обучающиеся должны владеть математическим аппаратом алгебры, линейной алгебры, теории чисел, теории вероятностей и математической статистики, теории информации, знать основы построения вычислительных сетей, основы классической криптографии.

Для успешного освоения дисциплины «Защита систем квантовой связи» ей должны предшествовать следующие дисциплины:

- «Алгебра»;
- «Линейная алгебра»;
- «Теория чисел»;
- «Теория вероятностей и математическая статистика»;
- «Теория информации»;
- «Методы и средства криптографической защиты информации»;
- «Компьютерные сети».

Дисциплина «Защита систем квантовой связи» является предшествующей для прохождения производственной и преддипломной практики и итоговой государственной аттестации.

## 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
---	---

<b>Общепрофессиональные компетенции</b>	
<b>ОПК-4</b> Обладает способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<b>Знает:</b> - перспективные физические платформы для создания квантовых вычислительных систем; - основные квантово-механические методы, лежащие в основе обеспечения информационной безопасности, а также основные квантово-криптографические протоколы.
<b>Профессиональные компетенции</b>	
<b>ПК-4</b> Обладает способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	<b>Знает:</b> - принципы квантовых вычислений и квантовые алгоритмы, направленные на анализ существующих криптосистем с открытым ключом; <b>Умеет:</b> - проводить сравнительный анализ систем квантового распределения ключей.

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единиц, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости  Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция	A	1	1					
2	Квантовые вычисления	A	3	3					
3	Квантовые алгоритмы	A	3	3		1		7	Задания для самостоятельной работы
4	Квантовая информация	A	3	3				7	Задания для самостоятельной работы
5	Постулаты квантовой механики	A	3	3		1		7	Задания для самостоятельной работы
6	Квантовые схемы	A	3	3				7	Задания для самостоятельной работы
7	Квантовое преобразование Фурье	A	3	3		1		7	Задания для самостоятельной

									работы
8	Меры различия квантовой информации	A	3	3				7	Задания для самостоятельной работы
9	Квантовая криптография	A	4	4		1		7	Задания для самостоятельной работы
						2	0,3	0,7	зачет
	<b>ИТОГО</b>		<b>26</b>	<b>26</b>		<b>6</b>	<b>0,3</b>	<b>49,7</b>	

### Содержание разделов дисциплины

#### Тема 1: Вводная лекция.

История квантовых вычислений и квантовой информации. Квантовые биты.

#### Тема 2: Квантовые вычисления.

Однокубитовые элементы. Многокубитовые элементы. Измерения в базисах, отличных от вычислительного. Квантовые схемы. Схема копирования кубита?

#### Тема 3: Квантовые алгоритмы.

Классические вычисления на квантовом компьютере. Квантовый параллелизм. Алгоритм Дойча. Алгоритм Дойча-Йожа. Классификация квантовых алгоритмов.

#### Тема 4: Квантовая информация.

Квантовая теория информации.

#### Тема 5: Постулаты квантовой механики.

Пространство состояний. Эволюция. Квантовые измерения. Различение квантовых состояний. Проективные измерения. POVM-измерения. Фаза. Состояние системы.

#### Тема 6: Квантовые схемы.

Квантовые алгоритмы. Условные операции. Измерение. Универсальные квантовые элементы.

#### Тема 7: Квантовое преобразование Фурье.

Квантовое преобразование Фурье. Определение собственного числа. Приложения: нахождение порядка и факторизация.

#### Тема 8: Меры различия квантовой информации.

Меры различия классической информации. Насколько близки два квантовых состояния? Следовая метрика. Степень совпадения. Связь между мерами различия. Насколько квантовый канал сохраняет информацию?

#### Тема 9: Квантовая криптография.

Криптография с секретным ключом. Усиление конфиденциальности и согласование информации. Квантовое распределение ключей. Секретность и когерентная информация. Безопасность квантового распределения ключей.

### 5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках

данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция с элементами лекции - беседы** – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

## **6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса используются:  
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение:

- Microsoft Visual Studio.

## **7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

## **8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

### **а) основная литература**

1. Душкин, Р. В. Квантовые вычисления и функциональное программирование / Душкин Р. В. - Москва : ДМК Пресс, 2015. - 232 с. - ISBN 978-5-97060-275-1. - Текст :

- электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970602751.html>
2. Хренников, А. Ю. Введение в квантовую теорию информации / Хренников А. Ю. - Москва : ФИЗМАТЛИТ, 2008. - 284 с. - ISBN 978-5-9221-0951-2. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785922109512.html>
3. Викторова Н. Б. Основы математического моделирования квантовых вычислительных процессов — Санкт-Петербург: Лань, 2023  
<https://e.lanbook.com/book/327326>

**б) дополнительная литература**

1. Румянцев, К. Е. Квантовые технологии в телекоммуникационных системах : учебник / К. Е. Румянцев. - Ростов-на-Дону : ЮФУ, 2021. - 346 с. - ISBN 978-5-9275-3857-7. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785927538577.html>
2. Нильсен М. Квантовые вычисления и квантовая информация. – М: Мир, 2006.

**в) ресурсы сети «Интернет» (при необходимости)**

1. Общероссийский математический портал (<http://www.mathnet.ru/>).

**9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

**Автор(ы):**

Доцент кафедры КБиММОИ, канд. физ.-мат. наук

Д. М. Мурин

**Приложение № 1 к рабочей программе дисциплины  
«Защита систем квантовой связи»**

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

**1. Типовые контрольные задания и иные материалы,  
используемые в процессе текущего контроля успеваемости**

**Задания для самостоятельной работы**

**Задания для самостоятельной работы по теме № 3: Квантовые алгоритмы.**

Упражнение 1. Какова эффективность наилучшего классического алгоритма, гарантированно различающего постоянную функцию от сбалансированной с некоторой вероятностью ошибки  $\epsilon < 1/2$ ?

Упражнение 2. Найдите точки на сфере Блоха, соответствующие нормализованным собственным векторам различных матриц Паули.

Упражнение 3. Пусть  $x$  – действительное число и  $A$  — такая матрица, что  $A^2 = I$ . Покажите, что  $\exp(iAx) = \cos(x) I + i \sin(x) A$ .

Упражнение 4. Покажите, что с точностью до общей фазы элемент  $\pi/8$  удовлетворяет условию  $T = R_z(\pi/4)$ .

Упражнение 5. Представьте оператор Адамара  $H$  в виде произведения поворота операторов  $R_x$  и  $R_z$  и общего фазового множителя  $e^{i\varphi}$  для некоторого действительного  $\varphi$ .

Упражнение 6. Покажите, что  $X Y X = -Y$ , и выведите отсюда уравнение  $X R_y(\theta) X = R_y(-\theta)$ .

Упражнение 7. Произвольный унитарный оператор, действующий на кубитах, можно записать в виде  $U = \exp(i \alpha) R_n(\theta)$  для некоторых вещественных чисел  $\alpha$  и  $\theta$  и вещественного трехмерного единичного вектора  $n$ .

1. Докажите это.

2. Найдите значения  $\alpha$ ,  $\theta$  и  $n$ , при которых получится оператор Адамара  $H$ .

**Задания для самостоятельной работы по теме № 4: Квантовая информация.**

Упражнение 1. Объясните, как использовать устройство, правильно идентифицирующее одно из двух поданных на его вход неортогональных квантовых состояний  $|\psi\rangle$  или  $|\varphi\rangle$ , для построения другого устройства, копирующего состояния  $|\psi\rangle$  и  $|\varphi\rangle$  в нарушение теоремы о невозможности копирования. И наоборот, объясните, как использовать устройство для копирования с целью различения неортогональных квантовых состояний.

**Задания для самостоятельной работы по теме № 5: Постулаты квантовой механики.**

Упражнение 1. Проверьте, что оператор Адамара  $H$  является унитарным.

Упражнение 2. Докажите, что  $H^2 = I$ .

Упражнение 3. Чему равны собственные числа и собственные векторы оператора  $H$ ?

Упражнение 4. Пусть  $A$  и  $B$  — коммутирующие эрмитовы операторы. Докажите, что  $\exp(A)\exp(B) = \exp(A+B)$ .

Упражнение 5. Используя спектральное разложение, покажите, что для любого унитарного оператора  $U$  оператор  $K = -i \log(U)$  является эрмитовым, а следовательно,  $U = \exp(iK)$  для некоторого эрмитова оператора  $K$ .

Упражнение 6. Пусть  $\{L_l\}$  и  $\{M_m\}$  – два набора операторов измерений. Покажите, что последовательное выполнение измерения, задаваемого операторами  $\{L_l\}$ , и операторами

$\{M_m\}$ , физически эквивалентно одному измерению, задаваемому операторами  $\{N_{lm}\}$ , где  $N_{lm} = M_m L_l$ .

Упражнение 7. Предположим, мы приготовили квантовую систему в собственном для некоторой наблюдаемой  $M$  состоянии  $|\varphi\rangle$  (соответствующее собственное значение равно  $m$ ). Чему будут равны среднее измеренное значение наблюдаемой  $M$  и среднеквадратичное отклонение?

Упражнение 8. Пусть кубит находится в состоянии  $|0\rangle$  и выполняется измерение наблюдаемой  $X$ . Чему равно среднее значение и среднеквадратичное отклонение  $X$ ?

Упражнение 9. Покажите, что собственные значения оператора  $\mathbf{v} \cdot \boldsymbol{\sigma}$  равны  $\pm 1$ , а проекторы на соответствующие собственные пространства определяются выражениями  $P_{\pm} = (I \pm \mathbf{v} \cdot \boldsymbol{\sigma})/2$ .

Упражнение 10. Вычислите вероятность получения результата  $+1$  при измерении  $\mathbf{v} \cdot \boldsymbol{\sigma}$ , полагая, что перед измерением система находилась в состоянии  $|0\rangle$ . В каком состоянии будет находиться система после измерения, если известно, что было получено значение  $+1$ ?

Упражнение 11. Покажите, что любое измерение, в котором операторы измерения и POVM-элементы совпадают, является проективным.

Упражнение 12. Пусть Боб получает квантовое состояние, выбираемое из набора  $|\psi_1\rangle, \dots, |\psi_m\rangle$  линейно-независимых состояний. Постройте такой POVM-набор  $\{E_1, E_2, \dots, E_{m+1}\}$  при котором в случае, если результат измерения равен  $E_m$  ( $0 < i < m+1$ ), Бобу достоверно известно, что ему было выдано состояние  $|\psi_i\rangle$ , (POVM-набор должен удовлетворять условию  $\langle \psi_i | E_i | \psi_i \rangle > 0$  при любом  $i$ .)

### Задания для самостоятельной работы по теме № 6: Квантовые схемы.

Упражнение 1. Пусть  $m$  и  $n$  – непараллельные единичные вещественные трехмерные векторы. Покажите, что любая унитарная операция  $U$  на одном кубите может быть записана в виде

$$U = e^{i\alpha} R_n(\beta_1) R_m(\gamma_1) R_n(\beta_2) R_m(\gamma_2) \dots$$

при соответствующих значениях  $\alpha$ ,  $\beta_k$  и  $\gamma_k$ .

Упражнение 2. Укажите  $A$ ,  $B$ ,  $C$  и  $\alpha$  для элемента Адамара.

Упражнение 3 (тождества для схем). Полезно уметь упрощать схемы «с первого взгляда» с использованием тождеств для операторов. Докажите три следующих тождества:

$$H X H = Z; H Y H = -Y; H Z H = X.$$

Упражнение 4. С помощью предыдущего упражнения покажите, что, с точностью до общего фазового множителя  $H T H = R_x(\pi/4)$ .

Упражнение 5. Докажите, что  $C^2(U)$  для любого однокубитового оператора  $U$  может быть представлено схемой, состоящей из не более 8 однокубитовых элементов и 6 элементов CNOT.

Упражнение 6. Постройте схемы, реализующие  $C^1(U)$  для  $U = R_x(\theta)$  и  $U = R_y(\theta)$ , с помощью элемента CNOT и операций на одном кубите. Можно ли сократить число последних с трех до двух?

Упражнение 7. Пусть  $\rho$  – матрица плотности, описывающая двухкубитовую систему. Предположим, что мы производим проективное измерение второго кубита (в вычислительном базисе). Пусть  $P_0 = |0\rangle\langle 0|$  и  $P_1 = |1\rangle\langle 1|$  – проекторы на состояния  $|0\rangle$  и  $|1\rangle$  соответственно, а  $\rho'$  – матрица плотности системы после измерения наблюдателем, не узнавшим результат измерения. Покажите, что имеет место формула  $\rho' = P_0 \rho P_0 + P_1 \rho P_1$ . Покажите также, что редуцированная матрица плотности для первого кубита не меняется после измерения, т. е.  $\text{tr}_2(\rho') = \text{tr}_2(\rho)$ .

Упражнение 8 (иррациональность  $\theta$ ). Пусть  $\cos \theta = 3/5$ . Докажите от противного, что  $\theta$  несоизмеримо с  $2\pi$ .

1. Пользуясь тем, что  $e^{i\alpha} = (3 + 4i)/5$ , покажите, что если  $\theta$  рационально, то существует такое целое положительное число  $m$ , что  $(3 + 4i)^m = 5^m$ .

2. Покажите, что  $(3 + 4i)^m = 3 + 4i \pmod{5}$  для всех  $m > 0$ , и выведите отсюда, что равенство  $(3 + 4i)^m = 5^m$  невозможно.



Упражнение 8. Пусть  $U$  – унитарное преобразование, реализованное с помощью  $n$ -кубитовой квантовой схемы, состоящей из элементов  $H$ ,  $S$ , CNOT и Тоффоли. Покажите, что  $U$  имеет вид  $2^{-k/2}M$ , где  $k$  – целое число, а  $M$  – матрица размера  $2^n \times 2^n$ , элементы которой – комплексные числа с целыми действительной и мнимой частями. Выполните то же упражнение с элементом  $\pi/8$  вместо элемента Тоффоли.

### **Задания для самостоятельной работы по теме № 7: Квантовое преобразование Фурье.**

Упражнение 1. Приведите прямое доказательство того, что квантовое преобразование Фурье в ортонормальном базисе, унитарно.

Упражнение 2. Вычислите в явном виде преобразование Фурье  $n$ -кубитового состояния  $|00\dots 0\rangle$ .

Упражнение 3 (классическое быстрое преобразование Фурье). Предположим, требуется получить на классическом компьютере преобразование Фурье вектора с  $2^n$  комплексными компонентами. Проверьте, что при непосредственном вычислении для этого потребуется  $\Theta(2^{2n})$  элементарных арифметических операций. Найдите способ сократить число таких операций до  $\Theta(n2^n)$ .

Упражнение 4. Разложите элемент «управляемое  $R_k$ » в композицию однокубитовых и CNOT-элементов.

Упражнение 5. Постройте квантовую схему, реализующую обратное квантовое преобразование Фурье.

Упражнение 6 (приближенное квантовое преобразование Фурье). Очевидно, что в схеме, реализующей квантовое преобразование Фурье, применяются элементы экспоненциальной (в зависимости от числа кубитов) точности. На самом деле, однако, ни в какой квантовой схеме полиномиального размера такая точность не требуется. Пусть, например,  $U$  – идеальное квантовое преобразование Фурье на  $n$  кубит и  $V$  – преобразование, которое получится, если элементы «управляемое  $R_k$ » реализованы с точностью  $\Delta = 1/p(n)$ , где  $p(n)$  – многочлен. Покажите, что ошибка  $E(U, V) = \max_{|\psi\rangle} \|(U - V)(|\psi\rangle)\|$  имеет порядок  $\Theta(n^2/p(n))$  и тем самым полиномиальной точности в каждом элементе достаточно, чтобы гарантировать полиномиальную точность схемы в целом.

### **Задания для самостоятельной работы по теме № 8: Меры различия квантовой информации.**

Упражнение 1. Найдите расстояние между распределениями вероятностей  $(1, 0)$  и  $(1/2, 1/2)$  в следовой метрике; между распределениями  $(1/2, 1/3, 1/6)$  и  $(3/4, 1/8, 1/8)$ .

Упражнение 2. Покажите, что расстояние между распределениями вероятностей  $(p, 1-p)$  и  $(q, 1-q)$  в следовой метрике равно  $|p - q|$ .

Упражнение 3. Найдите степень совпадения для распределениями вероятностей  $(1, 0)$  и  $(1/2, 1/2)$ ; для распределений  $(1/2, 1/3, 1/6)$  и  $(3/4, 1/8, 1/8)$ .

Упражнение 4. Покажите, что для любых состояний  $\rho$  и  $\sigma$  можно представить их разность в виде  $\rho - \sigma = Q - S$ , где  $Q$  и  $S$  – положительно определенные операторы с ортогональными носителями.

Упражнение 5 (существование неподвижной точки). Теорема Шаудера о неподвижной точке – классический математический результат, заключающийся в том, что любое непрерывное отображение в себя выпуклого компактного множества в гильбертовом пространстве имеет неподвижную точку.

Используя эту теорему, докажите, что любое сохраняющее след квантовое преобразование  $E$  имеет неподвижную точку, т. е., что существует  $\rho$ , такое, что  $E(\rho) = \rho$ .

Упражнение 6. Пусть сохраняющее след квантовое преобразование  $E$  является строго сжимающим, т. е. для любых  $\rho_0$  и  $\sigma$  выполняется неравенство  $D(E(\rho), E(\sigma)) < D(\rho, \sigma)$ . Докажите, что  $E$  имеет единственную неподвижную точку.

Упражнение 7. Рассмотрим деполаризующий канал  $E(\rho) = \rho I / 2 + (1 - \rho) \rho$ . Для произвольных  $\rho$  и  $\sigma$  найдите  $D(E(\rho), E(\sigma))$ , используя блеховское представление, и явно докажете, что отображение  $E$  является строго сжимающим, т. е. что  $D(E(\rho), E(\sigma)) < D(\rho, \sigma)$ .

Упражнение 8. Покажите, что канал с классической ошибкой является сжимающим, но не является строго сжимающим. Найдите множество неподвижных точек для этого канала.

### Задания для самостоятельной работы по теме № 9: Квантовая криптография.

Упражнение 1. Рассмотрите систему с  $n$  пользователями, любая пара которых хотела бы общаться лично. Сколько требуется ключей при использовании криптографии с открытым ключом? Сколько требуется ключей при использовании криптографии с секретным ключом?

Упражнение 2. Может быть неясно, почему. Покажите, что из наихудшего допущения, состоящего в том, что Ева имеет полный контроль над каналом следует, что  $S(\rho)$  ограничивает взаимную информацию Евы с результатами измерений Алисы и Боба.

Упражнение 3. Отметим, что локальные измерения, которые производят Алиса и Боб, как, например,  $I \otimes X$  и  $X \otimes I$ , не коммутируют с базисом Белла. Покажите, что, несмотря на это, статистика, которую Алиса и Боб получают из своих измерений, такая же, какую они могли бы получить, измеряя  $P_{bf}$  и  $P_{pf}$ .

Упражнение 4. Пусть  $\{M_1, M_2, \dots, M_n\}$  – множество наблюдаемых, которые принимают значения  $X_i$  при измерении над состоянием  $\rho$ . Докажите, что случайные величины  $X_i$  можно описывать в терминах классической теории вероятностей, если  $[M_i, M_j] = 0$ , т. е. если они попарно коммутируют.

Упражнение 5. Покажите, что, если мы начинаем с  $n$  ЭПР пар в состоянии  $|\beta_{00}\rangle^{\otimes n}$  и выполняем измерения одинаковых образующих на двух  $n$ -кубитовых половинах этих пар, а затем применяем операторы Паули для исправления разницы в результатах этих измерений, то получаем закодированное состояние  $|\beta_{00}\rangle^{\otimes m}$ . Покажите также, что если стабилизирующий код исправляет до  $\delta n$  ошибок, то даже когда в  $n$ -кубитовой половине допускается  $\delta n$  ошибок, мы получим  $|\beta_{00}\rangle^{\otimes m}$ .

## 2. Список вопросов к зачету

1. История квантовых вычислений и квантовой информации.
2. Квантовые биты.
3. Однокубитовые элементы. Многокубитовые элементы.
4. Измерения в базисах, отличных от вычислительного.
5. Квантовые схемы.
6. Схема копирования кубита.
7. Классические вычисления на квантовом компьютере.
8. Квантовый параллелизм.
9. Алгоритм Дойча.
10. Алгоритм Дойча-Йожа.
11. Классификация квантовых алгоритмов.
12. Квантовая теория информации.
13. Пространство состояний. Эволюция.
14. Квантовые измерения.
15. Различение квантовых состояний.
16. Проективные измерения.
17. POVM-измерения.
18. Фаза.
19. Состояние системы.
20. Квантовые алгоритмы.
21. Условные операции.

22. Измерение.
23. Универсальные квантовые элементы.
24. Квантовое преобразование Фурье.
25. Определение собственного числа.
26. Приложения: нахождение порядка и факторизация.
27. Меры различия классической информации.
28. Насколько близки два квантовых состояния?
29. Следовая метрика.
30. Степень совпадения.
31. Связь между мерами различия.
32. Насколько квантовый канал сохраняет информацию?
33. Криптография с секретным ключом.
34. Усиление конфиденциальности и согласование информации.
35. Квантовое распределение ключей.
36. Секретность и когерентная информация.
37. Безопасность квантового распределения ключей.

### **3. Правила выставления оценки на зачете.**

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

**Оценка «Зачтено»** выставляется студенту, который демонстрирует владение содержанием материала и понятийным аппаратом квантовой информатики и квантовой теории связи; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ.

**Оценка «Не зачтено»** выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

## **Приложение № 2 к рабочей программе дисциплины «Защита систем квантовой связи»**

### **Методические указания для студентов по освоению дисциплины**

Учебным планом на изучение дисциплины «Защита систем квантовой связи» отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен зачет. В процессе изучения дисциплины выполняются семь самостоятельных работ.

При изучении учебного материала по дисциплине «Защита систем квантовой связи» соблюдается баланс между лекционными и практическими занятиями. Это связано с тем, что с одной стороны в рамках дисциплины излагается большое количество нетривиального учебного материала, в том числе результаты научных исследований последнего десятилетия, а, с другой стороны, для полноценного освоения данного материала обучающемуся необходимо получить самостоятельный опыт по применению изучаемого в рамках дисциплины математического аппарата.

Основную роль для анализа и контроля качества усвоения материала играют самостоятельные работы. В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические задачи, которые должны позволить студенту переосмыслить изученные на лекциях понятия и методы, применить их для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены в письменном виде и представлены в установленные сроки.

Для повышения качества усвоения теоретического материала, приобретенных практических навыков работы с изучаемым в рамках дисциплины математическим аппаратом проводятся консультации по разбору заданий для самостоятельной работы. Также на консультациях, возможно повторно, разъясняются вопросы, вызвавшие затруднения у обучающихся.

По окончании семестра изучения дисциплины обучающиеся сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя один теоретический вопрос. На самостоятельную подготовку к зачету выделяется 2 дня.

Опыт преподавания дисциплины «Защита систем квантовой связи» говорит о высокой сложности ее самостоятельного изучения для обучающегося в первую очередь ввиду достаточно узкого выбора учебной литературы на русском языке, а также ввиду необходимости обладания достаточно глубокими знаниями линейной алгебры и теории вероятностей и математической статистики. Излагаемый на лекциях материал часто является нетривиальным и отражает результаты научных исследований последнего десятилетия. Поэтому посещение всех аудиторных занятий является обязательным.