

Рабочая программа дисциплины (модуля) — осень 2022 г.

1. Общая информация

Кафедра: Российского квантового центра

Дисциплина (eng.): **Quantum communications**

Дисциплина (рус.): **Квантовая связь**

Физтех-школа, направление: ЛФИ, 03.04.01 Прикладные математика и физика

Подготовка к экзаменам:

№	Семестр	Форма контроля	Часы
	<i>№ семестра, осенний или весенний, курс</i>	<i>Дифференцированный зачет зачет экзамен</i>	
1	9, осенний, пятый	Экзамен	30

2. Цели и задачи, компетенции

Цель дисциплины: дать студенту представление о современных приложениях квантовой механики к связи на расстоянии.

Задачи дисциплины: снабдить слушателей базовыми знаниями для работы и исследований в области фотонных квантовых технологий, в особенности связи на длинные расстояния.

Освоение дисциплины направлено на формирование у обучающегося следующих компетенций:

Общекультурные (ОК):

Общепрофессиональные (ОПК): ОПК-2, ОПК-4, ОПК-5, ОПК-6

Профессиональные (ПК): ПК-1

3. Место дисциплины

3.1. Место дисциплины (модуля) в структуре образовательной программы бакалавриата (магистратуры):

Дисциплина относится к вариативной части образовательной программы.

3.2. Дисциплина базируется на:

1. Курс общей физики
2. Курс теоретической физики
3. Английский язык

3.3. Дисциплина предшествует изучению дисциплин:

1. Лабораторный практикум по квантовой фотонике и криптографии
2. Научно-исследовательская работа

4. Результаты обучения

В результате освоения дисциплины обучающиеся должны

Знать: теоретические основы квантовой связи и основные известные на сегодняшний день ее приложения.

Уметь: ориентироваться в современных исследованиях по квантовой связи и криптографии.

Владеть: базовыми идеями и методами анализа систем квантовой связи.

5. Темы и разделы

Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий:

№	Тема (раздел) дисциплины	Семестр	Лекции	Лаборат. работы	Практич. (семинар.) задания	Задания, курсовые работы	Самост. работа
	<i>Тема занятий</i>	<i>(№ семестра)</i>	<i>(часы)</i>	<i>(часы)</i>	<i>(часы)</i>	<i>(часы)</i>	<i>(часы)</i>
1	Introduction Вводная лекция	9	2				
2	Components of quantum-optical systems Элементная база квантовых оптических систем	9	2				
3	Basics of quantum optics Основы квантовой оптики	9	2				
4	Quantum superposition Квантовая перепутанность	9	2				
5	Measurement in quantum mechanics Квантовые измерения	9	2				
6	Quantum key distribution (QKD) Квантовое распределение ключей (КРК)	9	2				
7	Applications of QKD Применения КРК	9	2				
8	Quantum measurements Квантовые измерения	9	2				
9	Entangled states Перепутанные состояния	9	2				
11	Bell measurement with linear optics Белловское измерение средствами линейной оптики	9	2				
10	Security of BB84 protocol Безопасность протокола BB84	9	2				
12	Security and threat model of QKD Модель безопасности КРК	9	2				
13	Paper seminar on quantum teleportation; Detector control attack Разбор научной статьи по квантовой телепортации; Атака с ослеплением детекторов	9	2				
14	Paper seminar on twin-field QKD; Countermeasures against imperfections and certification Разбор научной статьи по КРК на полях-близнецах; Методы защиты от практических атак и сертификация	9	2				
15	Discussion and question-and-answer session Дискуссия и консультация	9	2				

Course content (*who gives the lecture*):

1. Introduction. History of cryptography. Quantum cryptography. Demonstration that measurement changes a quantum state. Key distribution networks. Course overview. Sources of photons and coherent states. (*Vadim*)
2. Components of quantum-optical systems. Transmission of light in free space and optical fiber. Beamsplitters, polarizers, attenuators, wavelength filters, isolators and circulators. Modulators of polarization, phase, and intensity. Photodetectors and power meters. Single-photon detectors. Integrated optics. (*Vadim*)
3. Basics of quantum optics. Quantum states of light. Statistical properties of light. Single photons. Coherent states. Qubits. Dual- and single-rail qubits. How to encode states of light to make qubits. Bloch sphere. Phase coding of a single photon. Interferometers in single-photon regime. (*Denis*)
4. Quantum superposition. Pure and mixed states. Transition from pure states to mixed states and vice versa. Interaction-free detection. Double-slit interference and quantum erasure. Quantum ensembles and density matrix. (*Denis*)
5. Measurement in quantum mechanics. How to measure qubit. Measurement of non-orthogonal states. How to make annihilation operator with measurement. Application example: quantum random number generator. (*Roman*)
6. Quantum key distribution (QKD). BB84 protocol and post-processing. Intercept-resend attack. How to realise QKD protocols on physical level. How qubits are prepared and measured in experiment. Free-space and fiber realisations. Using entanglement in experimental QKD. Decoy-state protocol. (*Roman*)
7. Main applications of QKD and how they work. Quantum key generation rate in experiments. Limits on QKD distance. Quantum networks. Trusted repeaters. Satellite QKD and its challenges. (*Roman*)
8. Quantum measurements. Measurement-induced transformations. Quantum Zeno paradox. Projective measurements. Generalized measurements and POVM. Examples of optical schemes for generalized quantum measurements. Accessible information. Holevo bound. (*Denis*)
9. Entangled states. Bell basis. Correlations of entangled states. Remote state preparation. Entangled photons. Heralded sources of single photons. Superluminal communication and the “no-cloning” theorem. (*Denis*)
10. Bell measurement with linear optics. Bell inequality. Examples of Bell’s inequality violation. Quantum teleportation. (*Denis*)
11. Security of BB84 protocol. Equivalence of prepare-and-measure and entanglement-based QKD. Detection of eavesdropping attempts. Optimal attack. (*Denis*)
12. Security and threat model of QKD. The use of quantum random number generator in QKD. The need to trust the manufacturer. Processing double-clicks. Optical Trojan-horse attack and countermeasures to it. (*Vadim*)
13. Paper seminar: J.-G. Ren et al., “Ground-to-satellite quantum teleportation,” *Nature* 549, 70 (2017). Detector control attack and countermeasures to it. (*Vadim*)
14. Paper seminar on twin-field QKD: M. Lucamarini et al., “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature* 557, 400 (2018). Types of countermeasures against imperfections. Distinguishability of source states. Certification of cryptographic tools. (*Vadim*)
15. Discussion and question-and-answer session. (*all lecturers*)

Содержание темы (*кто читает лекцию*):

1. Вводная лекция. История криптографии. Квантовая криптография. Демонстрация разрушения квантового состояния при измерении. Сети передачи ключей. Обзор содержания курса. Источники одиночных фотонов и когерентных состояний. (*Вадим*)
2. Элементная база квантовых оптических систем. Передача света по открытому пространству и оптическому волокну. Светоделители, поляризаторы, аттенюаторы, спектральные фильтры, изоляторы и циркуляторы. Модуляторы поляризации, фазы, интенсивности. Фотоприемники и измерители мощности. Детекторы одиночных фотонов. Интегральная оптика. (*Вадим*)
3. Основы квантовой оптики. Квантовые состояния света. Статистические свойства света. Одиночные фотоны. Когерентные состояния. Кубиты. Одно- и двухлинейные способы кодирования кубитов. Как приготовить состояния света для кодирования кубитов. Сфера Блоха. Фазовое кодирование одиночного фотона. Интерферометры в однофотонном режиме. (*Денис*)
4. Квантовая перепутанность. Чистые и смешанные состояния, переходы между ними. Измерение без воздействия на объект. Интерференция в двухщелевом интерферометре и квантовое стирание информации. Ансамбли квантовых состояния и матрица плотности. (*Денис*)
5. Квантовые измерения. Как измерить кубит. Измерение неортогональных состояний. Как реализовать оператор уничтожения с помощью измерения. Пример применения: квантовый генератор случайных чисел. (*Роман*)

6. Квантовое распределение ключей (КРК). Протокол ББ84 и постобработка. Атака перехват-пересылка. Как реализуются протоколы КРК на физическом уровне. Как готовятся и измеряются кубиты в эксперименте. Реализации связи по открытому пространству и оптическому волокну. Использование квантовой перепутанности в реализациях КРК. Протокол с состояниями-ловушками. *(Роман)*
7. Применения КРК. Скорость генерации ключа в реализациях. Ограничения на максимальное расстояние передачи. Квантовые сети. Защищенный узел сети. Спутниковые системы КРК и их особенности. *(Роман)*
8. Квантовые измерения. Изменение состояния, вызванное его измерением. Квантовый парадокс Зенона. Проекционные измерения. Обобщенные измерения и положительная операторнозначная мера. Примеры оптических схем для обобщенных квантовых измерений. Доступная информация. Граница Холево. *(Денис)*
9. Перепутанные состояния. Белловский базис. Корреляции между перепутанными состояниями. Удаленное приготовление состояния. Перепутанные фотоны. Объявленный источник одиночных фотонов. Невозможность передачи информации быстрее скорости света и теорема о запрете клонирования. *(Денис)*
10. Белловское измерение средствами линейной оптики. Неравенство Белла. Примеры нарушения неравенства Белла. Квантовая телепортация. *(Денис)*
11. Безопасность протокола ББ84. Эквивалентность КРК с приготовлением и измерением состояний КРК на перепутанных состояниях. Обнаружение попыток подслушивания. Оптимальная атака. *(Денис)*
12. Модель безопасности КРК. Использование квантового генератора случайных чисел в КРК. Необходимость доверять производителю систем. Обработка одновременных срабатываний детекторов. Оптическая атака троянским конем и методы защиты от нее. *(Вадим)*
13. Разбор научной статьи по квантовой телепортации с земли на спутник J.-G. Ren et al., “Ground-to-satellite quantum teleportation,” *Nature* 549, 70 (2017). Атака с ослеплением детекторов и методы защиты от нее. *(Вадим)*
14. Разбор научной статьи по КРК на полях-близнецах M. Lucamarini et al., “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature* 557, 400 (2018). Классификация методов защит от практических атак. Различимость состояний источника. Сертификация средств криптографии. *(Вадим)*
15. Дискуссия и консультация. *(все лекторы)*

7. Учебно-методическое и информационное обеспечение

- 7.1. Основная литература: The Physics of Quantum Information, под редакцией Bouwmeester, Ekert, Zeilinger; Nielsen and Chuang, Quantum Computation and Quantum Information.
- 7.2. Дополнительная литература: глава учебника arXiv:1108.1718; обзоры в Reviews of Modern Physics по квантовой криптографии: N. Gisin et al., *Rev. Mod. Phys.* 74, 145 (2002); V. Scarani et al., *Rev. Mod. Phys.* 81, 1301 (2009); F. Xu et al., *Rev. Mod. Phys.* 92, 025002 (2020).

10. Фонд оценочных средств

The final grade in the course is composed of grades for a take-home written assignment during the term (50%) and an oral exam at the end of the term (50%).

The take-home assignment consists of a random task assigned to each student. A well-researched treatment of the task is expected, using the course material and, possibly, additional sources.

No aids are allowed at the oral exam. It starts with a random topic from the course assigned to each student and time given for preparing his/her presentation of the topic. The student then proceeds to a chat with the examiner, at which he/she presents and explains the assigned topic. The examiner may then ask the student additional questions from any part of the course. The grade is assigned based on the quality of answers and demonstrated overall level of understanding.

Аттестация по дисциплине «Квантовая связь» осуществляется по сумме письменной аналитической домашней работы по индивидуальному заданию с доступом студента к произвольным материалам в течение 9 семестра (50% итоговой оценки) и устного экзамена без доступа студента к каким-либо материалам в конце 9 семестра (50% итоговой оценки).

Примеры экзаменационных заданий:

1. Доказать теорему о запрете клонирования.
2. Нарисовать схему атаки с ослеплением детекторов и объяснить, как она работает.

Примеры контрольных вопросов:

1. Чем квантовая криптография лучше и чем хуже классической?
2. Как можно кодировать оптические квантовые состояния и для каких применений каждый способ лучше подходит?
3. Какие типы источников фотонов бывают и чем они отличаются?
4. За счет каких эффектов возникают потери в атмосферном оптическом канале?
5. Какими свойствами обладают хэш-функции?
6. Как лучше всего бороться с уязвимостями в реализациях?

11. Составители

Зав. кафедрой: Шляпников Георгий Всеволодович.

Дата обсуждения на заседании кафедры: 29 марта 2019 г.

Составителями внесены обновления и изменения: 29 апреля 2020 г.; 1 сентября 2022 г.

№	ФИО составителя дисциплины	ФИО на английском	Ученая степень	Ученое звание
1	Юрий Курочкин	Yury Kurochkin	к.ф.-м.н.	
2	Вадим Макаров	Vadim Makarov	dr. ing.	
3	Денис Сыч	Denis Sych	к.ф.-м.н.	