Рабочая программа дисциплины (модуля)

Разделы

1. Общий

Кафедра: Российского квантового центра

Дисциплина (eng.): Quantum communications
Дисциплина (рус.): Квантовая связь

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

Комментарий:_____

Подготовка к экзаменам:

№	Семестр	Форма контроля	Часы
	(№ семестра, осенний или весенний, курс)	*Дифференцированный зачет* *Зачет* *Экзамен*	
1	9	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.

Компетенции, формируемые в процессе изучения дисциплины

Освоение дисциплины направлено на формирование у обучающегося следующих общекультурных (ОК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

Общекультурные (ОК):

Общепрофессиональных (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 идеям 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
	Тема занятий	*(№ семестра, осенний или весенний, курс)*	*(часы)*	*(часы)*	*(часы)*	*(часы)*	*(часы)*
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	Measurement in quantum mechanics Квантовые измерения	9	2				
5	Quantum key distribution (QKD) Квантовое распределение ключей (КРК)	9	2				
6	Applications of QKD Применения КРК	9	2				
7	Quantum superposition Квантовая перепутанность	9	2				
8	Quantum measurements Квантовые измерения	9	2				
9	Entangled states Перепутанные состояния	9	2				
10	Security of BB84 protocol Безопасность протокола ББ84	9	2				
11	Bell measurement with linear optics Белловское измерение средствами линейной оптики	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. Interferometers in single-photon regime. Photodetectors and power meters. Single-photon detectors. Integrated optics. *(Vadim)*
3. Basics of quantum optics. Qubits. Dual- and single-rail qubits. How to encode states of light to make qubits. Discrete variables vs. continuous variables. Bloch sphere. Phase coding of single photon. *(Yury)*
4. Measurement in quantum mechanics. How to measure qubit. Measurement of non-orthogonal states. How to make annihilation operator with measurement. Application examples: quantum random number generator, interaction-free detection. *(Yury)*
5. 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. Differential-phase-coding protocol. *(Yury)*
6. 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. *(Yury)*
7. Quantum superposition. Pure and mixed states. Transition from pure states to mixed states and vice versa. Double-slit interference and quantum erasure. Quantum ensembles and density matrix. *(Denis)*
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. “Ghost” imaging and “ghost” interference. Superluminal communication and the “no-cloning” theorem. *(Denis)*
10. Security of BB84 protocol. Equivalence of prepare-and-measure and entanglement-based QKD. Decoy state QKD. Detection of eavesdropping attempts. Intercept-resend attack. Optimal attack. Bell inequality. Examples of Bell’s inequality violation. *(Denis)*
11. Bell measurement with linear optics. Quantum teleportation. *(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. Интерферометры в однофотонном режиме. Фотоприемники и измерители мощности. Детекторы одиночных фотонов. Интегральная оптика. *(Вадим)*
3. Основы квантовой оптики. Кубиты. Одно- и двухлинейные способы кодирования кубитов. Как приготовить состояния света для кодирования кубитов. Дискретные и непрерывные переменные. Сфера Блоха. Фазовое кодирование одиночного фотона. *(Юрий)*
4. Квантовые измерения. Как измерить кубит. Измерение неортогональных состояний. Как реализовать оператор уничтожения с помощью измерения. Примеры применений: квантовый генератор случайных чисел, измерение без воздействия на объект. *(Юрий)*
5. Квантовое распределение ключей (КРК). Протокол ББ84 и постобработка. Атака перехват-пересылка. Как реализуются протоколы КРК на физическом уровне. Как приготовляются и измеряются кубиты в эксперименте. Реализации связи по открытому пространству и оптическому волокну. Использование квантовой перепутанности в реализациях КРК. Протокол с состояниями-ловушками. Протокол с дифференциальным фазовым кодированием. *(Юрий)*
6. Применения КРК. Скорость генерации ключа в реализациях. Ограничения на максимальное расстояние передачи. Квантовые сети. Защищенный узел сети. Спутниковые системы КРК и их особенности. *(Юрий)*
7. Квантовая перепутанность. Чистые и смешанные состояния, переходы между ними. Интерференция в двухщелевом интерферометре и квантовое стирание информации. Ансамбли квантовых состояния и матрица плотности. *(Денис)*
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. Призрачное получение изображений и призрачная интерференция. Невозможность передачи информации быстрее скорости света и теорема о запрете клонирования. *(Денис)*
10. Безопасность протокола ББ84. Эквивалентность КРК с приготовлением и измерением состояний КРК на перепутанных состояниях. КРК с состояниями-ловушками. Обнаружение попыток подслушивания. Атака перехват-пересылка. Оптимальная атака. Неравенство Белла. Примеры нарушения неравенства Белла. *(Денис)*
11. Белловское измерение средствами линейной оптики. Квантовая телепортация. *(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)*

6. Материально-техническая база

Описание материально-технической базы _____

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., arXiv:1903.09051.

7.3. Учебно-методическая литература:

_____

7.4. Перечень ресурсов сети интернет:

_____

8. Перечень информационных ресурсов

Описание информационных ресурсов _____

9. Методические указания

Описание методических указаний для обучающихся по усвоению дисциплины (модуля)

10. Фонд оценочных средств

The final grade in the course is composed of grades for several written tests and assignments administered during the term (60%) and an oral exam at the end of the term (40%).

The oral exam starts with a random task assigned to each student and time given for completion of the task. The student then proceeds to a chat with the examiner, at which he/she presents his/her solution to the assigned task. 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 level of understanding.

Аттестация по дисциплине «Квантовая связь» осуществляется по сумме письменных контрольных работ и заданий в течение 9 семестра (60% итоговой оценки) и устного экзамена в конце 9 семестра (40% 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: 29 апреля 2020 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.	