

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы физики
и исследований им. Ландау
А.В. Рогачев**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Квантовая связь
по направлению:	Прикладные математика и физика
профиль подготовки:	Общая и прикладная физика Физтех-школа физики и исследований им. Ландау кафедра Российского квантового центра
курс:	1
квалификация:	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Программу составили:

Ю.В. Курочкин, канд. физ.-мат. наук

Д.В. Сыч, канд. физ.-мат. наук

В.В. Макаров, phd (к.ф.-м.н.)

Программа обсуждена на заседании кафедры Российского квантового центра 29.01.2025

Аннотация

Курс вводит в теорию и практику квантовой связи. Он охватывает кодирование кубитов, суперпозицию, перепутанность, квантовые измерения, практические аспекты волоконно-оптических и атмосферных каналов связи. Он представляет протоколы для генерации случайных чисел, измерения без воздействия на объект, призрачного получения изображений, квантовой телепортации.

Особое внимание уделено квантовому распределению ключей, для которого разобраны несколько протоколов и реализаций, структуры сетей, а также вводятся доказательства безопасности и практические аспекты защищенности реализаций.

1. Цели и задачи

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.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области своей профессиональной деятельности, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.2 Способен оценивать актуальность исследований в области своей профессиональной деятельности и их практическую значимость
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-3 Способен выбирать и (или) разрабатывать подходы к решению типовых и новых задач в области профессиональной деятельности, учитывая особенности и ограничения различных методов решения	ОПК-3.1 Способен анализировать задачу, планировать пути решения, предлагать и комбинировать способы решения
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области физико-математических наук и информационно-коммуникационных технологий	ОПК-4.2 Способен применять знания в области физико-математических наук для решения поставленной задачи, формулирования выводов и оценки полученных результатов

ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты

3. Перечень планируемых результатов обучения по дисциплине (модулю)

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.

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

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Вводная лекция	2			2
2	Элементная база квантовых оптических систем	2			2
3	Основы квантовой оптики	2			2
4	Измерение в квантовой механике	2			2
5	Квантовое распределение ключей (КРК)	2			2
6	Применение КРК	2			2
7	Квантовая перепутанность	2			2
8	Квантовые измерения	2			2
9	Перепутанные состояния	2			2
10	Безопасность протокола BB84	2			2
11	Белловское измерение средствами линейной оптики	2			2
12	Модель безопасности КРК	2			2
13	Разбор научной статьи по квантовой телепортации; Атака с ослеплением детекторов	2			2
14	Разбор научной статьи по КРК на полях-близнецах; Методы защиты от практических атак и сертификация	2			2
15	Дискуссия и консультации	2			2

Итого часов	30			30
Подготовка к экзамену	30 час.			
Общая трудоёмкость	90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 1 (Осенний)

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. Измерение в квантовой механике

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 BB84 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. Протокол с дифференциальным фазовым кодированием. (Юрий)

6. Применение КРК

Скорость генерации ключа в реализациях. Ограничения на максимальное расстояние передачи. Квантовые сети. Защищённые 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 состояний 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 BB84

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

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; Атака с ослеплением детекторов

Разбор статьи J.-G. Ren et al., “Ground-to-satellite quantum teleportation,” Nature 549, 70 (2017). (Вадим)

14. Разбор научной статьи по КРК на полях-близнецах; Методы защиты от практических атак и сертификация

Разбор статьи M. Lucamarini et al., “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” Nature 557, 400 (2018). (Вадим)

15. Дискуссия и консультации

Дискуссия и консультации (все лекторы)

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная мультимедиапроектором и экраном.

6. Перечень рекомендуемой литературы

Основная литература

1. The Physics of Quantum Information, ed. by Bouwmeester, Ekert, Zeilinger; Springer, Berlin, Heidelberg (2000).
2. Nielsen and Chuang, Quantum Computation and Quantum Information, Cambridge University press (2010).

Дополнительная литература

1. N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)
2. V. Scarani et al., Rev. Mod. Phys. 81, 1301 (2009)
3. F. Xu et al., arXiv:1903.09051

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<https://arxiv.org/>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Во время лекций могут быть использованы мультимедийные технологии, включая демонстрацию презентаций.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен, с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике. В результате изучения дисциплины студент должен знать основные определения и понятия, уметь применять полученные знания для решения различных задач.

Успешное освоение курса требует:

- посещения всех занятий, предусмотренных учебным планом по дисциплине;
- ведения конспекта занятий;
- напряжённой самостоятельной работы студента.

Самостоятельная работа включает в себя:

- чтение рекомендованной литературы;
- проработку учебного материала, подготовку ответов на вопросы, предназначенных для самостоятельного изучения;
- решение задач, предлагаемых студентам на занятиях;
- подготовку к выполнению заданий промежуточной аттестации.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладные математика и физика
профиль подготовки: Общая и прикладная физика
Физтех-школа физики и исследований им. Ландау
кафедра Российского квантового центра
курс: 1
квалификация: магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Экзамен

Разработчики:

Ю.В. Курочкин, канд. физ.-мат. наук
Д.В. Сыч, канд. физ.-мат. наук
В.В. Макаров, phd (к.ф.-м.н.)

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области своей профессиональной деятельности, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.2 Способен оценивать актуальность исследований в области своей профессиональной деятельности и их практическую значимость
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-3 Способен выбирать и (или) разрабатывать подходы к решению типовых и новых задач в области профессиональной деятельности, учитывая особенности и ограничения различных методов решения	ОПК-3.1 Способен анализировать задачу, планировать пути решения, предлагать и комбинировать способы решения
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области физико-математических наук и информационно-коммуникационных технологий	ОПК-4.2 Способен применять знания в области физико-математических наук для решения поставленной задачи, формулирования выводов и оценки полученных результатов
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты

2. Показатели оценивания компетенций

В результате изучения дисциплины «Квантовая связь» обучающийся должен:

знать:

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

уметь:

ориентироваться в современных исследованиях по квантовой связи и криптографии.

владеть:

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Не предусмотрено.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Примеры контрольных 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. Как лучше всего бороться с уязвимостями в реализациях?

Примеры экзаменационных билетов:

Билет 1.

1. Неравенство Белла. Примеры нарушения неравенства Белла.
2. Сравните квантовую и классическую криптографию. Какие достоинства и недостатки у каждой?

Билет 2.

1. Обобщенные измерения и положительная операторнозначная мера. Примеры оптических схем для обобщенных квантовых измерений. Доступная информация. Граница Холево.
2. Перечислите все схемы и протоколы КРК, которые вы знаете из этого курса. Оцените и обоснуйте, уязвим ли каждый из них для атаки троянским конем, и если он уязвим, то как сложно его будет защитить.

Билет 3.

1. Квантовое распространение ключей: основные протоколы квантовой криптографии (опишите, как три разобранных в лекциях протокола работают).
2. Какими свойствами обладают хэш-функции?

Билет 4.

1. Измерение: что такое измерение в квантовой механике. Как измерить кубит. Измерение неортогональных состояний.
2. Доказать теорему о запрете клонирования.

Билет 5.

1. Кубиты. Одно- и двухлинейные способы кодирования кубитов. Как приготовить состояния света для кодирования кубитов.
2. Нарисовать схему атаки с ослеплением детекторов и объяснить, как она работает.

Критерии оценивания

Оценка отлично 10 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 9 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 8 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо 7 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо 6 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо 5 баллов - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно 4 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно 3 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно 2 балла - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно 1 балл - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Экзамен проводится в устной форме по билетам. В каждом билете представлено два теоретических вопроса. При проведении зачёта и экзамена обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося не должен превышать одного астрономического часа.