МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Новосибирский национальный исследовательский государственный университет»
(Новосибирский государственный университет, НГУ)

Физический факультет
Кафедра квантовой электроники

УТВЕРЖДАЮ
Декан ФФ
академик РАН _____ А. Е. Бондарь
«07» 10 2020 г.

Рабочая программа дисциплины
Системы квантовой криптографии

Направление подготовки **03.04.02 Физика, Курс 1, семестр 1**
Направленность (профиль): **Общая и фундаментальная физика**

Форма обучения **Очная**

Семестр	Общий объем	Виды учебных занятий (в часах)				Промежуточная аттестация (в часах)				
		Контактная работа обучающихся с преподавателем			Самостоятельная работа, не включая период сессии	Самостоятельная подготовка к промежуточной аттестации	Контактная работа обучающихся с преподавателем			
		Лекции	Практические занятия	Лабораторные занятия			Консультации	Зачет	Дифференцированный зачет	Экзамен
1	2	3	4	5	6	7	8	9	10	11
1	72	16	16		38				2	
Всего 72 часа / 2 зачётные единицы, из них: - контактная работа 34 часа - в интерактивных формах 16 часов										
Компетенции ПК-1, ПК-2										

Разработчик:
к.ф.-м.н., ст. преподаватель каф. КвЭл ФФ НГУ Третьяков Д.Б. Третьяков

Заведующий кафедрой КвЭл ФФ НГУ
академик РАН С.Н. Багаев

Руководитель программы
д.ф.-м.н. И.Б. Логашенко

Новосибирск 2020

Содержание

Аннотация

к рабочей программе дисциплины курса «Системы квантовой криптографии»
Направление: **03.04.02 Физика**
Направленность (профиль): Общая и фундаментальная физика

Программа дисциплины **«Системы квантовой криптографии»** составлена в соответствии с требованиями СУОС к уровню магистратуры по направлению подготовки **03.04.02 Физика, Общая и фундаментальная физика,** а также задачами, стоящими перед Новосибирским государственным университетом по реализации Программы развития НГУ. Дисциплина реализуется на физическом факультете Федерального государственного автономного образовательного учреждения высшего профессионального образования Новосибирский национальный исследовательский государственный университет (НГУ) кафедрой квантовой электроники в качестве дисциплины по выбору. Дисциплина изучается студентами первого курса физического факультета в осеннем семестре.

Цель курса – овладение базовыми понятиями современной квантовой криптографии.

Дисциплина нацелена на формирование у выпускника профессиональных компетенций:

ПК-1 – способность самостоятельно ставить конкретные задачи научных исследований в области физики и решать их с помощью современной аппаратуры и информационных технологий с использованием новейшего российского и зарубежного опыта.

ПК-2 - способность свободно владеть разделами физики, необходимыми для решения научно-инновационных задач, и применять результаты научных исследований в инновационной деятельности.

В результате освоения дисциплины обучающийся должен:

Знать: методы и способы постановки и решения задач физических исследований в области квантовой криптографии, принципы действия, функциональные и метрологические возможности современной аппаратуры для физических исследований в области квантовой криптографии, возможности, методы и системы компьютерных технологий для физических теоретических и экспериментальных исследований в данной области, основные принципы квантовой криптографии, основные протоколы передачи данных, основные физические платформы для реализации генерации квантового ключа;

Уметь: самостоятельно ставить и решать конкретные физические задачи научных исследований в области квантовой криптографии с использованием современной аппаратуры и компьютерных технологий, рассчитывать и измерять в эксперименте основные параметры систем квантовой криптографии с использованием лавинных фотоприемников и интерферометров;

Владеть: навыками постановки и решения задач научных исследований в области квантовой криптографии с помощью современных методов и средств теоретических и экспериментальных исследований, базовыми принципами квантовой коммуникации.

Курс рассчитан на один семестр (2-й). Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента, дифференцированный зачет.

Программой дисциплины предусмотрены следующие виды контроля:

Текущий контроль: выборочный опрос по темам предыдущих лекций, проверка домашних заданий.

Промежуточная аттестация: – дифференцированный зачет.

Общая трудоемкость рабочей программы дисциплины составляет **72** академических часа / **2** зачетные единицы.

1. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы.

В результате прохождения курса «Системы квантовой криптографии» у студентов физического факультета должно сформироваться представление о фундаментальных принципах, на которых базируется квантовая криптография, о различных протоколах передачи данных и физических реализациях генерации квантового ключа.

Цель курса – овладение базовыми понятиями современной квантовой криптографии.

Дисциплина нацелена на формирование у выпускника профессиональных компетенций:

ПК-1 – способность самостоятельно ставить конкретные задачи научных исследований в области физики и решать их с помощью современной аппаратуры и информационных технологий с использованием новейшего российского и зарубежного опыта.

ПК-2 - способность свободно владеть разделами физики, необходимыми для решения научно-инновационных задач, и применять результаты научных исследований в инновационной деятельности.

В результате освоения дисциплины обучающийся должен:

знать

- методы и способы постановки и решения задач физических исследований в области квантовой криптографии, принципы действия, функциональные и метрологические возможности современной аппаратуры для физических исследований в области квантовой криптографии, возможности, методы и системы компьютерных технологий для физических теоретических и экспериментальных исследований в данной области (ПК-1.1)
- основные принципы квантовой криптографии, основные протоколы передачи данных, основные физические платформы для реализации генерации квантового ключа (ПК-2.1)

уметь

- самостоятельно ставить и решать конкретные физические задачи научных исследований в области квантовой криптографии с использованием современной аппаратуры и компьютерных технологий (ПК 1.2)
- рассчитывать и измерять в эксперименте основные параметры систем квантовой криптографии с использованием лавинных фотоприемников и интерферометров (ПК-2.2)

владеть

- навыками постановки и решения задач научных исследований в области квантовой криптографии с помощью современных методов и средств теоретических и экспериментальных исследований (ПК 1.3)
- базовыми принципами квантовой коммуникации (ПК-2.3)

2. Место дисциплины в структуре образовательной программы:

Дисциплина **«Системы квантовой криптографии»** реализуется в 1 семестре 1-го курса для магистрантов, обучающихся по направлению подготовки 03.04.02 Физика. Курс является одной из профессиональных дисциплин по выбору, реализуемых кафедрой квантовой электроники. Для его восприятия требуется предварительная подготовка студентов по общей физике, квантовой механике, а также по теории вероятности. Данный курс является специальным, предназначенным для освоения теоретических принципов и особенностей

экспериментальной реализации современных квантовых коммуникаций, которые являются важнейшим направлением современной квантовой информатики. Этим определяется глубокая взаимосвязь данного курса с другими курсами, изучаемыми магистрантами-физиками. Он предшествует выполнению квалификационной работы студента по данной специализации, так как дает ему необходимые знания, навыки и предоставляет инструменты для выполнения научных исследований в рамках подготовки его квалификационной работы.

3. Трудоёмкость дисциплины в зачётных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем

Семестр	**Общий объем**	**Виды учебных занятий (в часах)**				**Промежуточная аттестация (в часах)**				
		Контактная работа обучающихся с преподавателем			Самостоятельная работа, не включая период сессии	Самостоятельная подготовка к промежуточной аттестации	Контактная работа обучающихся с преподавателем			
		Лекции	Практические занятия	Лабораторные занятия			Консультации	Зачет	Дифференцированный зачет	Экзамен
1	2	3	4	5	6	7	8	9	10	11
1	72	16	16		38				2	
Всего 72 часа / 2 зачётные единицы, из них: - контактная работа 34 часов - в интерактивных формах 16 часов										
Компетенции ПК-1, ПК-2										

Реализация дисциплины предусматривает практическую подготовку при проведении следующих видов занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента, дифференцированный зачет.

Программой дисциплины предусмотрены следующие виды контроля:

Текущий контроль: выборочный опрос по темам предыдущих лекций, проверка домашних заданий.

Промежуточная аттестация: – дифференцированный зачет.

Общая трудоемкость рабочей программы дисциплины составляет **72** академических часа / **2** зачетных единицы:

- занятия лекционного типа – 16 часов;
- практические занятия – 16 часов;
- самостоятельная работа обучающегося в течение семестра, не включая период сессии – 38 часов;
- промежуточная аттестация (дифференцированный зачет) – 2 часа;

Объём контактной работы обучающегося с преподавателем (занятия лекционного типа, практические занятия, дифференцированный зачет) составляет 34 часа. Работа с обучающимися в интерактивных формах (практические занятия) составляет 16 часов.

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

№ п/п	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоёмкость (в часах)					Групповая консультация (часов)	Промежуточная аттестация (зачет)
			Всего	Аудиторные часы		Сам. работа во время занятий (не включая период сессии	Сам. работа во время промежуточной аттестации		
				Лекции	Практические занятия				
1	2	3	4	5	6	7	8	9	10
1	Основы классической криптографии	1-2	8	4		4			
2	Основы квантовой криптографии	3-4	8	4		4			
3	Технологические проблемы квантовой криптографии	5-6	8	4		4			
4	Методы кодирования в квантовой криптографии	7-8	8	2		6			
5	Виды атак на защищенные квантовые каналы коммуникации	9-10	8	2		6			
6	Измерение эффективности регистрации детектора одиночных фотонов	11-12	12		6	6			
7	Исследование распределения числа фотонов в ослабленном лазерном импульсе	13-14	14		6	8			
8	Исследование работы интерферометра Маха-Цандера	15-16	4		4				
	Дифференцированный зачет	17	2						2
Всего			72	16	16	38			2

Программа и основное содержание лекций (16 часов)

1. Основы классической криптографии (2 часа)

1.1. Ассиметричные криптосистемы.

1.2. Симметричные криптосистемы.

2. Основы квантовой криптографии (2 часа)

2.1.Протокол BB84.

2.2. Коррекция ошибок.

2.3. Усиление секретности.
2.4. Другие протоколы (B92, ЭПР-протокол).

3. Технологические проблемы квантовой криптографии (2 часа)
3.1. Источники одиночных фотонов.
3.2. Квантовые каналы.
3.3. Детекторы одиночных фотонов.
3.4. Генераторы случайных чисел.

4. Методы кодирования в квантовой криптографии (2 часа)
4.1. Поляризационное кодирование.
4.2. Фазовое кодирование.
4.3. Частотное кодирование.
4.4. Релятивистская квантовая криптография.

5. Виды атак на защищенные квантовые каналы коммуникации (2 часа)
5.1. Атака «перехват-пересылка».
5.2. Атака с делением числа фотонов.
5.3. Атака «Троянский конь».

Программа практических занятий (16 часов)

1. Измерение эффективности регистрации детектора одиночных фотонов на основе лавинного фотодиода. (6 часов)
2. Измерение распределения числа фотонов в ослабленном лазерном импульсе. (6 часов)
3. Измерение контраста волоконного интерферометра Маха-Цандера. (4 часа)

Самостоятельная работа студентов (38 часов)

Перечень занятий на СРС	Объем, час
Изучение материала лекций	16
Изучение теоретического материала, не освещаемого на лекциях	6
Решение домашних заданий	16

5. Перечень учебной литературы.

5.1.Основная литература:

1. С.Я.Килин, Д.Б.Хорошко, А.П.НизовцевКвантовая криптография: идеи и практика. – Минск,«Беларускаянавука», 2007.–391 с.

5.2.Дополнительная литература:

6. Перечень учебно-методических материалов по самостоятельной работе обучающихся.

1. Gisin, G.Ribordy, W.Tittel, and Hugo Zbinden«Quantum cryptography», Reviewsof Modern Physics, v. 74, p. 145, 2002.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

Для освоения дисциплины используются следующие ресурсы:
- электронная информационно-образовательная среда НГУ (ЭИОС);
- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

7.1 Современные профессиональные базы данных

Не используются

7.2. Информационные справочные системы

Не используются.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MSOffice.

Использование специализированного программного обеспечения для изучения дисциплины не требуется.

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

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации.

2. Помещения для самостоятельной работы обучающихся.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду НГУ.

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

10. Оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине.

10.1 Порядок проведения текущего контроля и промежуточной аттестации по дисциплине

Текущий контроль

Текущий контроль осуществляется в ходе семестра путем выборочного опроса в начале каждой лекции по материалам предыдущей лекции, проверки выполнения домашних заданий.

Промежуточная аттестация

Освоение компетенций оценивается согласно шкале оценки уровня сформированности компетенции. Положительная оценка по дисциплине выставляется в том случае, если заявленные компетенции ПК-1 и ПК-2 сформированы не ниже порогового уровня в части, относящейся к формированию способности использовать специализированные знания в области систем квантовой криптографии в профессиональной деятельности.

Окончательная оценка работы студента в течение семестра происходит на зачете. Дифференцированный зачет проводится в конце семестра в устной форме.

Вывод об уровне сформированности компетенций принимается преподавателем. Каждый вопрос билета оценивается от 0 до 5 баллов. Положительная оценка ставится, когда все компетенции освоены не ниже порогового уровня. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

10.2 Описание критериев и шкал оценивания индикаторов достижения результатов обучения по дисциплине «Системы квантовой криптографии».

Критерии оценивания результатов обучения	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Уровень освоения компетенции			
		Не сформирован (не зачтено)	Пороговый уровень (зачтено)	Базовый уровень (зачтено)	Продвинутый уровень (зачтено)
1	2	3	4	5	6
Полнота знаний	ПК 1.1 ПК 2.1	Уровень знаний ниже минимальных требований. Имеют место грубые ошибки.	Минимально допустимый уровень знаний. Допускается значительное количество негрубых ошибок.	Уровень знаний соответствует программе подготовки по темам/разделам дисциплины. Допускается несколько негрубых/ несущественных ошибок. Не отвечает на дополнительные вопросы.	Уровень знаний соответствует программе подготовки по темам/разделам дисциплины. Свободно и аргументированно отвечает на дополнительные вопросы.
Наличие умений	ПК 1.2 ПК 2.2	Отсутствие минимальных умений. Не умеет решать стандартные задачи. Имеют место грубые ошибки.	Продемонстрированы частично основные умения. Решены типовые задачи. Допущены негрубые ошибки.	Продемонстрированы все основные умения. Решены все основные задания с негрубыми ошибками или с недочетами.	Продемонстрированы все основные умения. Решены все основные задания в полном объеме без недочетов и ошибок.
Наличие навыков (владение опытом)	ПК 1.3 ПК 2.3	Отсутствие владения материалом по темам/разделам дисциплины. Нет навыков в решении стандартных задач. Наличие грубых ошибок.	Имеется минимальный набор навыков при решении стандартных задач с некоторыми недочетами.	Имеется базовый набор навыков при решении стандартных задач с некоторыми недочетами.	Имеется базовый набор навыков при решении стандартных задач без ошибок и недочетов. Продемонстрированы знания по решению нестандартных задач.

Типовые контрольные задания и материалы, необходимые для оценки результатов обучения

Примеры домашнего задания

1. Найти скорость генерации «просеянного» квантового ключа для протокола BB84 при следующих заданных параметрах: тактовая частота импульсов, эффективность регистрации детекторов, коэффициент пропускания квантового канала, среднее число фотонов в импульсе.
2. Найти коэффициент ослабления лазерного излучения для получения среднего числа фотонов в лазерном импульсе 0.1 при следующих заданных параметрах: средняя импульсная мощность излучения на выходе из лазера, тактовая частота лазерных импульсов, длина волны излучения лазера.
3. Найти предельное расстояние, на котором можно сгенерировать секретный квантовый ключ по протоколу BB84 в оптоволоконной однопроходной схеме, при заданных параметрах: тактовая частота импульсов, эффективность регистрации детекторов, коэффициент затухания в квантовом канале, среднее число фотонов в импульсе, уровень ошибок при единичном коэффициенте пропускания квантового канала.

Вопросы к дифференцированному зачету

1. Ассиметричные и симметричные криптосистемы в классической криптографии.
2. Протокол BB84.
3. Процедура коррекции ошибок и усиления секретности.
4. Протокол B92.
5. ЭПР-протокол.
6. Источники одиночных фотонов.
7. Оптоволоконные квантовые каналы.
8. Атмосферные квантовые каналы.
9. Детекторы одиночных фотонов.
10. Лавинные фотодиоды. Пассивное и активное гашение лавины.
11. Генераторы случайных чисел.
12. Поляризационное кодирование. Метод активного восстановления поляризации.
13. Фазовое кодирование. Двухпроходная автокомпенсационная схема.
14. Частотное кодирование.
15. Релятивистская квантовая криптография.
16. Атака «перехват-пересылка». Атака с делением числа фотонов. Атака «Троянский конь».

Пример билета к дифференцированному зачету

1. Ассиметричные и симметричные криптосистемы в классической криптографии.
2. Детекторы одиночных фотонов.

Оценочные материалы по промежуточной аттестации, предназначенные для проверки соответствия уровня подготовки по дисциплине требованиям СУОС, хранятся на кафедре-разработчике РПД в печатном и электронном виде.

Лист актуализации фонда оценочных средств
по дисциплине «Системы квантовой криптографии»
по направлению подготовки 03.04.02 Физика
Профиль «Общая и фундаментальная физика»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Учёного совета ФФ НГУ	Подпись ответственного