**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение**

**высшего образования**

**«Новосибирский национальный исследовательский государственный университет»**

**Кафедра квантовой электроники**

УТВЕРЖДАЮ

Декан ФФ НГУ

Чл.-к. РАН\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. Е. Бондарь

«\_\_\_\_\_» \_\_\_\_\_\_\_\_2018 г.

**Системы квантовой криптографии**

Учебно-методический комплекс

**Физический факультет**

Направление подготовки

**03.04.02 Физика (уровень магистратуры)**

**Курс 1, семестр 2**

Профиль:

**Физика оптических явлений**

Форма обучения

**Очная**

**Новосибирск 2018**

Учебно-методический комплекс «Системы квантовой криптографии» предназначен для студентов магистратуры физического факультета НГУ, разработан в 2018 согласно требованиям Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования от 05.04.2017г. и решению УС ФФ (протокол № 167 от 21.03.2018).В состав комплекса включены рабочая программа дисциплины «Системы квантовой криптографии», банк обучающих материалов, банк контролирующих материалов, фонд оценочных средств.

УМК одобрен на заседании кафедры Квантовой Электроники ФФ НГУ **04 апреля 2018 года, протокол № 1**

Разработчик: к.ф.-м.н. Д.Б. Третьяков

Заведующий кафедрой КвЭл ФФ НГУ

академик РАН С.Н. Багаев

СОГЛАСОВАНО:

Ответственный за образовательную программу

заместитель декана ФФ по учебной работе

профессор, д.ф.-м.н. С.В. Цыбуля

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение**

**высшего образования**

**«Новосибирский национальный исследовательский государственный университет»**

**Кафедра квантовой электроники**

УТВЕРЖДАЮ

Декан ФФ НГУ

Чл.-к. РАН\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. Е. Бондарь

«\_\_\_\_\_» \_\_\_\_\_\_\_\_2018 г.

**Системы квантовой криптографии**

Рабочая программа дисциплины

**Физический факультет**

Направление подготовки

**03.04.02 Физика (уровень магистратуры)**

**Курс 1, семестр 2**

Профиль:

**Физика оптических явлений**

Форма обучения

**Очная**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Семестр** | **Общий**  **объем** | **Виды учебных занятий (в часах)** | | | | | **Промежуточная аттестация**  **(в период сессии) (в часах)** | | | | |
| Контактная работа обучающихся  с преподавателем | | | | Самостоятельная работа, не включая период сессии | Самостоятельная подготовка к промежуточной аттестации | Контактная работа  обучающихся с  преподавателем | | | |
| Лекции | Семинары | Практические занятия | Лабораторные занятия | Консультации | Зачет | Дифференцированный зачет | Экзамен |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2 | 72 | 16 | 16 |  |  | 38 |  |  |  |  | 2 |
| Всего 72 часов / 2 зачетные единицы  из них:  - контактная работа 34 часа  - в интерактивных формах 16 часов | | | | | | | | | | | |
| Компетенции ПК-1,ПК-2 | | | | | | | | | | | |

**Новосибирск 2018**

Рабочая программа дисциплины «Системы квантовой криптографии», предназначенная для магистрантов физического факультета НГУ, разработана в 2018 году согласно требованиям Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования от 05.04.2017г. и решению УС ФФ (протокол № 167 от 21.03.2018).

Место дисциплины в структуре учебного плана

Б.1 «Вариативная часть».

Рабочая программа дисциплины одобрена на заседании кафедры Квантовой Электроники ФФ НГУ **04 апреля 2018 года, протокол № 1**

Разработчик: к.ф.-м.н. Д.Б Третьяков

Заведующий кафедрой КвЭл ФФ НГУ

академик РАН С.Н. Багаев

СОГЛАСОВАНО:

Ответственный за образовательную программу

заместитель декана ФФ по учебной работе

профессор, д.ф.-м.н. С.В. Цыбуля

**Содержание**

Аннотация ..6

1. Цели освоения дисциплины 6

2. Место дисциплины в структуре ООП 6

3. Компетенции обучающегося, формируемые при освоении дисциплины 7

4. Структура и содержание дисциплины 7

5. Образовательные технологии ….9

6. Учебно-методическое обеспечение самостоятельной работы студентов...10

7. Фонд оценочных средств для проведения аттестации по итогам освоения

дисциплины: показатели, критерии оценивания компетенций, типовые

контрольные задания………………………………………………………….10

8. Учебно-методическое и информационное обеспечение дисциплины

Рекомендованная литература к теоретическому курсу 10

9. Материально-техническое обеспечение дисциплины 11

**Аннотация**

Программа курса **«Системы квантовой криптографии»** составлена в соответствии с требованиями к обязательному минимуму содержания и уровню подготовки магистра по направлению подготовки 03.04.02 Физика (уровень магистратуры), а также задачами, стоящими перед Новосибирским государственным университетом по реализации Программы развития НГУ. Дисциплина реализуется на физическом факультете федерального государственного автономного образовательного учреждения высшего образования «Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ) кафедрой квантовой электроники. Дисциплина изучается студентами первого курса магистратуры физического факультета.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, контрольные работы, домашние задания, консультации, самостоятельная работа студента, зачет.

Программой дисциплины предусмотрены следующие виды контроля:

Текущий контроль: выборочный опрос, контрольные.

Промежуточная аттестация: зачет.

Общая трудоемкость рабочей программы дисциплины составляет 72 зачетные единицы:

* занятия лекционного типа – 16 часов;
* занятия лабораторного типа – 16 часов;
* самостоятельная работа обучающегося в течение семестра, не включая период сессии – 38 часа;
* промежуточная аттестация (сдача лабораторных работ и зачет) – 2 часов;

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

## Цели освоения дисциплины

Цели курса – овладение базовыми понятиями современной квантовой криптографии.

## Место дисциплины в структуре образовательной программы:

Курс «Системы квантовой криптографии» является дисциплиной специализации в образовательной магистерской программе «Квантовые информационные технологии», содержит одну часть годового цикла и необходим для овладения основными представлениями об экспериментальной современной квантовой криптографии.

Курс относится к циклу фундаментальных общефизических дисциплин. В результате прохождения курса 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. Необходимые предпосылки для успешного освоения курса перечислены далее. В цикле математических дисциплин: знание теории вероятности и умение применять это знание при решении задач. В цикле физических дисциплин: знание общей физики и квантовой механики. Необходимость владения указанными выше математическими дисциплинами обусловлена тем обстоятельством, что они составляют основу математического аппарата квантовой криптографии. Выбор физических дисциплин, знание которых необходимо для освоения курса, обусловлен тем, что квантовая криптография опирается на квантовые свойства физических систем, а различные экспериментальные реализации генерации квантового ключа имеют специфические свойства, индивидуальные для каждой физической системы.

В последние десятилетия наблюдается бурный прогресс в области экспериментальной квантовой криптографии. 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 направления «Квантовые информационные технологии».

## Компетенции обучающегося, формируемые при освоении дисциплины

Дисциплина нацелена на формирование у выпускника следующих компетенций:

**научно-исследовательская деятельность:**

ПК-1: способность самостоятельно ставить конкретные задачи научных исследований в области квантовой криптографии и решать их с помощью современной аппаратуры и информационных технологий с использованием новейшего российского и зарубежного опыта, в том числе:

ПК 1.1: 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 1.2: уметь самостоятельно ставить и решать конкретные физические задачи научных исследований в области квантовой криптографии с использованием современной аппаратуры и компьютерных технологий.

ПК 1.3: владеть навыками постановки и решения задач научных исследований в области квантовой криптографии с помощью современных методов и средств теоретических и экспериментальных исследований.

**научно-инновационная деятельность:**

ПК-2: способность свободно владеть разделами физики, необходимыми для решения научно-инновационных задач в области квантовой криптографии

В результате освоения дисциплины обучающийся должен:

ПК-2.1 Знать: основные принципы квантовой криптографии, основные протоколы передачи данных, основные физические платформы для реализации генерации квантового ключа;

ПК-2.2Уметь рассчитывать и измерять в эксперименте основные параметры систем квантовой криптографии с использованием лавинных фотоприемников и интерферометров;

ПК-2.3Владеть базовыми принципами квантовой коммуникации.

1. **Структура и содержание дисциплины «Системы квантовой криптографии»**

Общая трудоемкость дисциплины составляет 2зачетных единицы, 72 часа.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Раздел**  **дисциплины** | **Неделя семестра** | **Всего** | **Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)** | | | **Промежуточная аттестация (в период сессии)**  **(в часах)** |
| Аудиторные часы | | Сам.работа в течение семестра (не включая период сессии) |
| Лекции  (кол-во часов) | Лабораторные работы  (кол-во  часов) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Основы классической криптографии  *Промежуточный контроль – домашнее задание* | 1-2 | 8 | 4 |  | 4 |  |
| 2 | Основы квантовой криптографии  *Промежуточный контроль – выборочный опрос* | 3-4 | 8 | 4 |  | 4 |  |
| 3 | Технологические проблемы квантовой криптографии  *Промежуточный контроль – выборочный опрос* | 5-6 | 8 | 4 |  | 4 |  |
| 4 | Методы кодирования в квантовой криптографии  *Промежуточный контроль – выборочный опрос, сдача и разбор домашнего задания* | 7-8 | 8 | 4 |  | 4 |  |
| 5 | Виды атак на защищенные квантовые каналы коммуникации  *Промежуточный контроль – выборочный опрос, сдача домашнего задания* | 9-10 | 8 | 4 |  | 4 |  |
| 6 | Измерение эффективности регистрации детектора одиночных фотонов | 11-12 | 10 |  | 4 | 6 |  |
| 7 | Исследование распределения числа фотонов в ослабленном лазерном импульсе | 13-14 | 10 |  | 4 | 6 |  |
| 8 | Исследование работы интерферометра Маха-Цандера  Контрольная работа | 15-16 | 10 |  | 4 | 6 |  |
| 9 | Зачет | 17 | 2 |  | 2 |  |  |
| **Всего** | | | **72** | **20** | **14** | **38** |  |

**4. Программа курса лекций**

1. Основы классической криптографии

1.1. Ассиметричные криптосистемы.

1.2. Симметричные криптосистемы.

1. Основы квантовой криптографии

2.1.Протокол BB84.

2.2. Коррекция ошибок.

2.3. Усиление секретности.

2.4. Другие протоколы (B92, ЭПР-протокол).

1. Технологические проблемы квантовой криптографии

3.1. Источники одиночных фотонов.

3.2. Квантовые каналы.

3.3. Детекторы одиночных фотонов.

3.4. Генераторы случайных чисел.

1. Методы кодирования в квантовой криптографии

4.1. Поляризационное кодирование.

4.2. Фазовое кодирование.

4.3. Частотное кодирование.

4.4. Релятивистская квантовая криптография.

1. Виды атак на защищенные квантовые каналы коммуникации

5.1. Атака «перехват-пересылка».

5.2. Атака с делением числа фотонов.

5.3. Атака «Троянский конь».

# 5. Образовательные технологии

1. Лекции с использованием презентации PowerPoint
2. Лабораторные работы на имеющихся экспериментальных установках по квантовой криптографии.

# 6. Учебно-методическое обеспечение самостоятельной работы студентов.

Обработка и презентация полученных на лабораторных работах экспериментальных данных.

# 7. Фонд оценочных средств для проведения аттестации по итогам освоения дисциплины: показатели, критерии оценивания компетенций, типовые контрольные задания

Оценочным средством для текущего контроля успеваемости в части самостоятельной работы является регулярная сдача-приемка домашних заданий и написание контрольной работы. Оценочным средством окончательного контроля является экзамен. Освоение компетенций оценивается по способности проводить самостоятельные исследования в области квантовых информационных технологий и владению современным состоянием дел в этой области.

Освоение компетенций оценивается по пятибалльной шкале. Положительная оценка по дисциплине выставляется в том случае, если заявленные компетенции сформированы не ниже порогового уровня в полном объеме в той части, которая соответствует содержанию дисциплины.

## Учебно-методическое и информационное обеспечение дисциплины

Рекомендованная литература

1. **N. Gisin, G.Ribordy, W.Tittel, and Hugo Zbinden**«Quantum cryptography», Reviewsof Modern Physics, v. 74, p. 145, 2002.
2. **С.Я.Килин, Д.Б.Хорошко, А.П.Низовцев**Квантовая криптография: идеи и практика. – Минск,«Беларускаянавука», 2007.–391 с.

**8.1. Программное обеспечение для лиц с ограниченными возможностями здоровья**

Таблица 8.2

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование ПО** | **Назначение** | **Место размещения** |
| 1 | Jaws for Windows | Программа экранного доступа к системным и офисным приложениям, включая интернет-обозреватели. Информация с экрана считывается вслух, обеспечивая возможность речевого доступа к самому разнообразному контенту. Jaws также позволяет выводить информацию на обновляемый дисплей Брайля. JAWS включает большой набор клавиатурных команд, позволяющих воспроизвести действия, которые обычно выполняются только при помощи мыши. | Ресурсный центр, читальные залы библиотеки НГУ, компьютерные классы (сетевые лицензии) |
| 2 | Duxbury Braille Translator v11.3 для Брайлевского принтера | Программа перевода текста в текст Брайля, и печати на Брайлевском принтере | Ресурсный центр |
| 3 | "MAGic Pro 13" (увеличение+речь) | Программа для людей со слабым зрением и для незрячих людей. Программа позволяет увеличить изображение на экране до 36 крат, есть функция речевого сопровождения | Ресурсный центр, читальные залы библиотеки НГУ |

# Материально-техническое обеспечение дисциплины:

Требуется аудитория с использованием мультимедийного проектора

Оборудование, обеспечивающее адаптацию электронных и печатных образовательных ресурсов для обучающиеся из числа лиц с ограниченными возможностями здоровья

Таблица 9.1

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование оборудования** | **Назначение** | **Место размещения** |
|  | Принтер Брайля | Печать рельефно-точечным шрифтом Брайля | Ресурсный центр |
|  | Увеличитель Prodigi Duo Tablet 24 | Устройство для чтения и увеличения плоскопечатного текста | Ресурсный центр, читальные залы библиотеки НГУ |
|  | Специализированное мобильное рабочее место «ЭлНот 311» | Мобильный компьютер с дисплеем брайля | Ресурсный центр |
|  | Портативный тактильный дисплей Брайля “Focus 40 Blue” | Навигация в операционных системах, программах и интернете с помощью отображения рельефно-точечным шрифтом Брайля получаемой информации | Ресурсный центр, читальные залы библиотеки НГУ |
|  | Устройство для печати тактильной графики «PIAF» | Печать тактильных графических изображений | Ресурсный центр |
|  | Портативный видео-увеличитель RUBY XL HD | Увеличение текста и подбор контрастных схем изображения | Ресурсный центр |
|  | Складной настольный электронный видео-увеличитель «TOPAZ PHD 15» | Увеличение текста и подбор контрастных схем изображения | Ресурсный центр |
|  | Электронный ручной видео-увеличитель ONYX Deskset HD 22” | Увеличение текста и подбор контрастных схем изображения | Ресурсный центр |
|  | Смартфон EISmart G3 | Смартфон клавишным управлением и озвученным интерфейсом, обучение спутниковой навигации. | Ресурсный центр |
|  | FM-система «Сонет-РСМ» РМ-3-1 | Звуковая FM-система для людей с нарушением слуха, улучшающая восприятие голосовой информации | Большая физическая аудитория главного корпуса НГУ |

**II. Банк обучающих материалов, рекомендации по организации самостоятельной работы студентов, выполнению курсовых проектов и лабораторных работ**

Задачи:

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.

Задания для лабораторного практикума.

1. Измерить эффективность регистрации детектора одиночных фотонов на основе лавинного фотодиода
2. Измерить распределение числа фотонов в ослабленном лазерном импульсе
3. Измерить контраст волоконного интерферометра Маха-Цандера

Мультимедийные презентации с лекционным материалом

# III. Банк контролирующих материалов

Зачет проходит в виде выборочного опроса по программе курса. Общая оценка выставляется на основе промежуточных оценок по лабораторным работам и ответов на выборочные вопросы.

Контрольные вопросы по курсу:

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».