УТВЕРЖДАЮ
Декан физического факультета
МГУ имени М.В. Ломоносова
профессор

_____Н.Н. Сысоев

«____» _____ 20__ г.

ПРОГРАММА
повышения квалификации

КВАНТОВАЯ ОБРАБОТКА ИНФОРМАЦИИ И КВАНТОВЫЕ ТЕХНОЛОГИИ

Москва - 2017

1. Цель реализации программы

Цель курса - сформировать у слушателей знания о физических основах современных квантовых технологий и методах обработки квантовой информации.
В лекционном курсе рассматриваются основные понятия квантовой механики, статистической физики, теории измерений и классической информатики, необходимые для введения в проблематику квантовой обработки информации. Курс ориентирован на слушателей, имеющих высшее образование и знакомым с общим курсом физики в формате стандарта специалиста или бакалавра, а также работников предприятий, специализирующихся в области квантовых оптических технологий.

Упор делается на физические эффекты и аналогии, лежащие в основе обсуждаемых понятий и помогающие раскрыть их содержание. В их числе:

- основные понятия квантовой информации (кубиты, перепутанные состояния, квантовые логические элементы и проч.)

- эффекты (квантовая телепортация, квантовый обмен и др.),

- неклассические световые поля,

- квантовые алгоритмы (поиск в базе данных, факторизация на простые множители и др.)

- квантовая криптография,

- квантовая коррекция ошибок,

а также некоторые другие разделы, в том числе те, к которым относятся научные интересы и оригинальные работы экспериментальной группы, где работает автор курса.

2. Формализованные результаты обучения

Обучение в МГУ имени М.В. Ломоносова направлено на подготовку работника высокой квалификации, который:

в полной мере обладает профессиональными и личностными качествами, обеспечивающими ему приоритетную востребованность и устойчивую конкурентоспособность на российском и международном рынке труда и широкие возможности самореализации, в том числе в новейших областях знаний, наиболее значимых сферах профессиональной деятельности и общественной жизни;

стремится к продолжению образования и самообразованию в течение всей жизни, способен максимально продуктивно использовать свой творческий потенциал в интересах личности, общества и государства;

сознает ответственность за результаты своей профессиональной и научной деятельности перед страной и человечеством, обладает активной гражданской позицией, основанной на демократических убеждениях и гуманистических ценностях;

умеет порождать новые идеи, расширять сферу собственной компетентности, вырабатывать оптимальные стратегии своей деятельности; готов решать проблемы в

новых и нестандартных профессиональных и жизненных ситуациях с учетом социальной и этической ответственности за принимаемые решения.

Выпускник МГУ имени М.В. Ломоносова, завершивший обучение по программе повышения квалификации «Квантовая обработка информации и квантовые технологии», должен обладать следующими универсальными и профессиональными компетенциями.

Универсальные компетенции

а) инструментальные:

способность использовать базовые знания и навыки управления информацией для решения исследовательских профессиональных задач, соблюдать основные требования информационной безопасности (ИК-1);

способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение (ИК-2);

б) системные:

способность к творчеству, порождению инновационных идей, выдвижению самостоятельных гипотез (СК-1);

способность к поиску, критическому анализу, обобщению и систематизации научной информации, к постановке целей исследования и выбору оптимальных путей и методов их достижения (СК-2);

способность к самостоятельному обучению и разработке новых методов исследования, к изменению научного и научно-производственного профиля деятельности; к инновационной научно-образовательной деятельности (СК-3).

Профессиональные компетенции

способность свободно владеть разделами физики, необходимыми для решения научно-исследовательских и научно-инновационных задач (ПК-1);

способность использовать знания современных проблем и новейших достижений физики в своей профессиональной деятельности (ПК-2);

способность и готовность применять на практике навыки составления и оформления научно-технической документации, научных отчётов, обзоров, докладов и статей (ПК-4);

способность использовать профессиональные знания в области информационных технологий, современных компьютерных сетей, программных продуктов и ресурсов интернета для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки (ПК-5);

способность свободно владеть профессиональными знаниями для анализа и синтеза физической информации (ПК-6);

Результатом освоения дисциплины является формирования у слушателей специализированных компетенций по профессиональным знаниям в области квантовых технологий и квантовой обработки информации.

3. Содержание программы

Учебный план
программы повышения квалификации
«Квантовая обработка информации и квантовые технологии»

Объем – 84 часа.
Форма обучения – очно-заочная.

№ п/п	Наименование разделов	Всего, час.	Обязательная аудиторная нагрузка		Самостоятельная работа, час.
			лекции	практич. и лаборат. занятия	
1	Введение. Кубиты и основные операции над ними	4	2		2
2	Основные способы реализации кубитов.				
3	Вектор состояния, волновая функция	4	2		2
4	Принцип суперпозиции и квантовая интерференция.				
5	Матрица и оператор плотности.	4	2		2
6	Энтропия в квантовой механике				
7	Теорема о запрете клонирования квантовых состояний.	4	2		2
8	Основные понятия классической криптографии. Часть 1.	4	2		2
9	Основные понятия классической криптографии. Часть 2.	4	2		2
10	Основные понятия квантовой криптографии.	4	2		2
11	Протоколы B92 и BB84	4	2		2
12	Практические реализации и атаки на системы квантового распределения ключей (КРК).	4	2		2
13	Неклассические состояния света	4	2		2
14	Составные квантовые системы и перепутанные состояния	4	2		2
15	Основные меры перепутывания	4	2		2
16	Парадокс Эйнштейна-Подольского-Розена и неравенства Белла	4	2		2
17	Протокол Экерта	4	2		2
18	Квантовая телепортация кубитов	4	2		2
19	Основы квантовой теории измерений	4	2		2
20	Основные модели квантовых вычислений	4	2		2

21	Современное состояние и перспективы квантовой обработки информации	4	2		2
Общее количество часов		84	42		42
Итоговая аттестация		зачет (4 час.)			

Учебно-тематический план
программы повышения квалификации
«Квантовая обработка информации и квантовые технологии»

№ п/п	Наименование разделов и тем	Всего, час.	В том числе		Самостоятельная работа, час.
			лекции	практич. и лаборат. занятия	
1	2	3	4	5	6
1	ВВЕДЕНИЕ. КУБИТЫ И ОСНОВНЫЕ ОПЕРАЦИИ НАД НИМИ. Что такое квантовая информация. Квантовые биты, двухуровневая система. Основные операции над единичными кубитами. Преобразование Адамара, интерферометр Маха-Цандера. Интерферометр Юнга. Временная и пространственная когерентность. Принцип суперпозиции, квантовая интерференция. Интерференция одного фотона. Закон Мура, роль квантовых эффектов. Биты и их реализация. Регистры. Понятие машины Тьюринга. Классические вычисления. Логические операции. Сложение по модулю 2. Требования, предъявляемые к квантовому компьютеру. Основные проблемы на пути к его созданию.	2	2		2
2	ОСНОВНЫЕ СПОСОБЫ РЕАЛИЗАЦИИ КУБИТОВ. Временная и пространственная когерентность. Интерферометр Маха-Цандера. Интерферометр Юнга. Поляризационные преобразования в оптике. Поляризационные, пространственные, и фазово-временные кубиты.	2	2		2

3	ВЕКТОР СОСТОЯНИЯ, ВОЛНОВАЯ ФУНКЦИЯ. Уравнение Шредингера, теория представлений. Описание состояний в квантовой механике. Волновая функция. Принцип суперпозиции. Физический смысл ВФ. Чистые и смешанные состояния. Вычисление средних величин. Аналогия с классическими поляризационными состояниями. Линейные операторы. Энтропия фон Неймана. Вычисление энтропии фон Неймана и Шеннона для двухуровневой системы.	2	2		2
4	ПРИНЦИП СУПЕРПОЗИЦИИ И КВАНТОВАЯ ИНТЕРФЕРЕНЦИЯ. КВАНТОВЫЕ СОСТОЯНИЯ ВЫСОКОЙ РАЗМЕРНОСТИ - КУДИТЫ. Интерференция одиночных фотонов и интерпретации интерференционных экспериментов. Биты, наты, диты. Основные модели квантовых состояний высокой размерности (D>2).	2	2		2
5	МАТРИЦА И ОПЕРАТОР ПЛОТНОСТИ. Свойства матрицы плотности, ее размерность. Энтропия фон Неймана для смешанных состояний				
6	ЭНТРОПИЯ В КВАНТОВОЙ МЕХАНИКЕ Энтропия фон Неймана, ее неотрицательность, максимальное значение. Квантовая относительная энтропия. Неравенство Клейна. Композиционные системы. Субаддитивность и вогнутость энтропии. Энтропия смеси состояний. Совместная энтропия. Условная энтропия. Взаимная информация. Примеры. Различие между классической и квантовой информацией. Достижимая информация. Априорная и апостериорная энтропии.	2	2		2

7	ТЕОРЕМА О ЗАПРЕТЕ КЛОНИРОВАНИЯ КВАНТОВЫХ СОСТОЯНИЙ. Ее связь с достижимой информацией. Граница и информация Холево. Примеры. Передача (transposition) квантовой информации. Понятие квантового канала связи. Точность воспроизведения информации (fidelity). Теорема Б.Шумахера о кодировании при отсутствии шума.				
8	ОСНОВНЫЕ ПОНЯТИЯ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ. ЧАСТЬ 1. Криптология, криптография и криптоанализ. Основные задачи криптографии. Понятия открытого текста, криптограммы, ключа и криптосистемы. Принцип Керкхгоффа. Приложения криптографии. Симметричные криптографические системы. Криптосистема с открытым ключом - асимметрия шифровки и дешифровки. Протокол RSA. Понятия криптографического протокола и криптографического алгоритма. Корректность и полнота протокола. Криптоанализ и основные виды атак. Подслушиватели (нарушители). Активный и пассивный, внутренний и внешний подслушиватели. Стеганография и ее задачи. Типы секретности сообщений (по Шеннону). Безусловно и условно стойкие шифры. Пример: код Вернама (одноразовый блокнот).	2	2		2

9	ОСНОВНЫЕ ПОНЯТИЯ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ ЧАСТЬ 2. Распределение ключей. Генерация ключей, их хранение и уничтожение. Одноключевые (симметричные) методы шифрования. Рассеивание и перемешивание. Понятие о криптосистемах DES и ГОСТ 28147-89, их достоинства и недостатки. Основные проблемы симметричных протоколов. Аутентификация секретного ключа. Атаки раздельных миров. Двухключевые (асимметричные) методы шифрования. Механизм распределения ключей по открытому каналу по У.Диффи и М.Хеллману. Понятие о криптосистемах RSA и Эль-Гамаля. Электронная подпись.				
10	ОСНОВНЫЕ ПОНЯТИЯ КВАНТОВОЙ КРИПТОГРАФИИ. Проблема распределения ключа в классической криптографии и пути ее решения. Физические основы квантового распределения ключа: теорема о запрете копирования и неразличимость неортогональных состояний. Общая схема протокола квантового распределения ключей (КРК). Основные свойства поляризованных фотонов. Некоторые сведения из теории квантовых измерений. Сопряженные базисы. Три сопряженных базиса для поляризованныхфотонов.	2	2		2
11	ПРОТОКОЛЫ B92 И BB84 Протокол BB84. Сырой и просеянный ключ. Коррекция ошибок и усиление секретности - на примере протокола BB84. Подслушивание в протоколе BB84. Стратегия перехватчик-ретранслятор. Стратегия “задержанного выбора”. Активный подслушиватель и схема аутентификации Вегмана-Картера. Недостатки протокола BB84. Протокол BB92. Его преимущества и недостатки по сравнению с BB84.	2	2		2

12	ПРАКТИЧЕСКИЕ РЕАЛИЗАЦИИ И АТАКИ НА СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ (КРК). Как приготовить квантовые состояния. Ослабленные лазерные импульсы. Оценка однофотонного состояния при ослаблении импульса когерентного поля. Двухфотонные импульсы. Способы кодирования квантовых состояний. Кодирование поляризации. Оптические волокна, сохраняющие поляризацию. Фазовая кодировка. Фарадеевское зеркало. Ротатор. Циркулятор. Система “Plug&Play”. Кодирование по частоте. Подслушивание в квантовой криптографии. Суть проблемы. Безусловная и практическая стойкость. Индивидуальные (некогерентные) атаки. Стратегия передатчик-ретранслятор. Стратегия «промежуточного базиса». Симметричные индивидуальные атаки. Оценка максимальной взаимной информации Алиса и Боба, Алисы и Евы при односторонних сообщениях. Критерий стойкости для протокола BB84. Когерентные атаки. Коллективные атаки. Атаки класса «Троянский конь». Атаки с помощью светоделителя.	2	2		2
13	НЕКЛАССИЧЕСКИЕ СОСТОЯНИЯ СВЕТА Роль неклассических полей в физике квантовой информации. Определение (I) неклассического света и его недостатки. Наблюдаемые признаки неклассического света. Мера Ли. Операциональное определение (II) неклассического света. g_2 - и D -критерии. Примеры: лазерный свет, тепловое излучение, смесь вакуумного и К-фотонного состояний.	2	2		2

14	СОСТАВНЫЕ КВАНТОВЫЕ СИСТЕМЫ И ПЕРЕПУТАННЫЕ СОСТОЯНИЯ Составные квантовые системы, двухкомпонентные коррелированные системы. Тензорное произведение векторных пространств, описание составных квантовых систем. Тензорное произведение матриц. Роль ПС в квантовых алгоритмах. Примеры: ионы в ловушках, коррелированные ядерные спины в молекулах, атом в оптическом резонаторе. Определение (I) перепутанных состояний. Пример приготовления двухчастичного ПС. Редуцированная матрица плотности компонент ПС. Состояния Белла, как частный случай ПС. Оптическая реализация ПС. Отдельные фотоны и квадратурные компоненты поля. Спонтанное параметрическое рассеяние (СПР) света, волновая функция СПР, амплитуда бифотона, корреляционные свойства. Перепутывание по времени, временная пост-селекция. Пространственно-частотные, поляризационно-частотные, поляризационно-угловые ПС. Амплитудная пост-селекция.	2	2		2

15	ОСНОВНЫЕ МЕРЫ ПЕРЕПУТЫВАНИЯ Понятие пебита (ebit). Кубиты и пебиты как прямые и косвенные ресурсы квантовой информации. Чистые перепутанные состояния. Разложение Шмидта двухкомпонентной системы. Энтропия перепутывания. Степень перепутывания. Локальные операции и классические сообщения. Смешанные перепутанные состояния. Перепутывание создания. Пример: состояния Вернера. Очищение перепутывания. Протоколы двустороннего и одностороннего обмена. Дистилляция и концентрация перепутывания. Критерий Переса-Хородецки. Сепарабельность квантовых состояний. Пример: состояния Вернера. Свободное и граничное перепутывание. Разложение Шмидта и параметр Федорова Состояния Белла. Их преобразования при смене базиса. Инварианты. Приложение: матрица плотности немаксимально перепутанных состояний.	2	2		2
16	ПАРАДОКС ЭЙНШТЕЙНА-ПОДОЛЬСКОГО-РОЗЕНА И НЕРАВЕНСТВА БЕЛЛА Парадокс ЭПР в варианте Бома. Антисимметричные состояния. Их инвариантность относительно поворота базиса. Аналогия между состояниями частиц со спином 1/2 и поляризационными состояниями света. Неравенства Белла. Классическая модель с двумя дихотомными переменными. Измеряемая Белла. Модель скрытых параметров. Квантовая модель. Спонтанное параметрическое рассеяние из двух кристаллов. Роль некоммутирующих операторов. *Парадокс Белла для трех наблюдаемых. Состояния Гринберга - Хорна - Цайлингера. Теорема Белла без неравенств. Парадокс Гринберга-Хорна-Цайлингера.	2	2		2
17	ПРОТОКОЛ ЭКЕРТА Описание протокола и его основные реализации	2	2		2

18	КВАНТОВАЯ ТЕЛЕПОРТАЦИЯ КУБИТОВ Копирование и передача квантовых состояний. Протокол квантовой телепортации. Требования, предъявляемые к нему: не нарушение теоремы о запрете клонирования; наличие неизвестного входного состояния; идентичность выходного состояния входному; отсутствие сверхсветовых сигналов; полное измерение оператора Белла. Обзор некоторых экспериментальных результатов по квантовой телепортации. Эксперименты группы А.Цайлингера; группы Ф.де-Мартини; группы Дж.Кимбла. Полное измерение состояний Белла. Эксперимент группы Я.Ши. “No-Go” - теорема. Ее доказательство по Л.Вайдману. Телепортация при наличии взаимодействия между квантовыми системами. Операция “CNOT” как пример таких взаимодействий. Телепортация состояний, описываемых непрерывными переменными (дополн.)	2	2		2
19	ОСНОВЫ КВАНТОВОЙ ТЕОРИИ ИЗМЕРЕНИЙ Классические вероятностные модели. Приготовление и измерение классического состояния. Аналог смешанного состояния. Маргинальные моменты. Связь моментов и вероятностей. Проблема моментов. Квантовые вероятностные модели. Прямые и косвенные измерения. Опыты Штерна и Герлаха. Двухуровневые системы (примеры). Формула Раби для вероятности перехода. Измерительный (Борна) и проекционный постулаты (фон Неймана). Понятие о квантовой томографии.	2	2		2

20	ОСНОВНЫЕ МОДЕЛИ КВАНТОВЫХ ВЫЧИСЛЕНИЙ. В чем проблема? Компьютерное моделирование физических процессов. Дискретизация. Ограничение, накладываемое на классический компьютер. Полиномиальный класс задач P. Моделирование времени. Алгоритм клеточного автомата. Моделирование вероятности. Экспоненциальный рост объема вычислительного устройства. Класс задач NP. Элементарные логические операции над кубитами. Унитарность. Формализм операторов рождения и уничтожения. Моделирование квантовых эффектов. Квантовый компьютер и построение его гамильтониана. Декогерентизация квантовой системы. Эволюция состояния в квантовом компьютере. Программный счетчик (курсор). Недостатки компьютера и необратимые потери энергии. Квантовый регистр. Случай Nкубитов. Общие требования, необходимые для реализации полномасштабных квантовых компьютеров. Условия ДиВинченсо. Основные физические модели для реализации квантовых вычислений. Квантовый компьютер на фотонах. Сверхпроводниковые квантовые компьютеры. Квантовые компьютеры на квантовых точках. Квантовые компьютеры на нейтральных атомах и ионах в ловушках.	2	2		2
21	СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ КВАНТОВОЙ ОБРАБОТКИ ИНФОРМАЦИИ (КОИ) Структура КОИ. Квантовые вычислители и квантовые симуляторы. Оптоволоконные каналы связи и системы КРК. Атмосферные и космические каналы связи и системы КРК. Квантовая память и квантовые интерфейсы.	2	2		2

4. Материально-технические условия реализации программы

Реализация программы планируется на базе физического факультета МГУ. Для реализации программы есть необходимый аудиторный фонд, позволяющий работать с меловой (маркерной) доской, проектором, персональным компьютером, доступ в кабинет физических демонстраций и лаборатории общего физического практикума.

Аттестация участников осуществляется в форме зачета.

5. Учебно-методическое обеспечение программы

Основная литература

1 Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Монография. Пер. с англ - М.: Мир, 2006. - 824с.

2 Д. Бауместер, А. Экерт, А. Цайлингер Физика квантовой информации. Москва: Постмаркет, 2002. – 376с.

Дополнительная литература

1. Д. Прескилл. Квантовая информация и квантовые вычисления. Регулярная и хаотическая динамика, Институт компьютерных исследований, 2008, 464с.

6. Требования к результатам обучения

Приводится перечень вопросов, выносимых на аттестацию в форме зачета, а также рекомендуемые темы рефератов.

Оценка уровня освоения программы осуществляется аттестационной комиссией по пятибалльной системе.

Оценка качества освоения программы осуществляется на зачете посредством защиты доклада с презентацией по теме, соответствующей программе и согласованной с преподавателем. Результаты защиты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают сдачу зачета.

Критерии оценивания защиты доклада:

1. Авторская самостоятельность.
2. Четкость, обоснованность, конкретность и ясность изложения содержания системы заданий, лабораторных работ, тем исследований, соответствие действующим нормативным требованиям.
3. Умение обосновать и отстаивать как предложенные задачи, лабораторные работы, темы исследований так и систему на их основе.
4. Использование современных методов диагностики образовательных результатов.
5. Возможность индивидуализации разработанной программы.
6. Использование навыков, полученных на практических занятиях курса.

Форма защиты доклада – очная (презентация проекта перед членами аттестационной комиссии, авторами и слушателями программы).

7. Составители программы

Кулик Сергей Павлович, доктор. физ.-мат. наук, профессор кафедры квантовой электроники физического факультета МГУ имени М.В. Ломоносова.