



МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
ИМЕНИ
М.В.Ломоносова

Квантовые технологии: что это и проблемы подготовки кадров

Сергей Кулик



IX летняя школа учителей физики



ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА



МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

ПРИКАЗ

«12» февраля 2018 г. Москва № 125

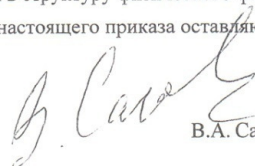
О создании Центра квантовых технологий

В целях выполнения проекта по сквозной технологии «Квантовые технологии» с Фондом поддержки проектов Национальной технологической инициативы по результатам конкурсного отбора на государственную поддержку центров Национальной технологической инициативы

приказываю:

1. Создать структурное подразделение МГУ на физическом факультете – Центр квантовых технологий (далее – Центр) согласно п.15 Правил предоставления субсидии из федерального бюджета на оказание государственной поддержки центров Национальной технологической инициативы (постановление Правительства Российской Федерации от 16 октября 2017 г. № 1251).
2. Назначить руководителем Центра декана физического факультета профессора Н.Н. Сысоева.
3. Создать Наблюдательный совет Центра под моим руководством. Н.Н. Сысоеву внести предложения по составу Наблюдательного совета Центра.
4. Н.Н. Сысоеву организовать работу Центра в соответствии с условиями предоставления финансирования, разработать необходимую для функционирования Центра организационно-распорядительную документацию, в том числе: представить проект положение о Центре, внести предложения по научному руководителю Центра, подготовить предложения о внесении соответствующих изменений в структуру физического факультета.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор
Московского университета
академик



В.А. Садовничий



итета создан
й»
нной поддержки
ологий РФ



приказо
-для осуще
ком

В научно-техническом направлении: преодоление технологических разрывов в области квантовых технологий – между научными разработками в области среднемасштабных квантовых компьютеров и созданием соответствующей элементной базы.

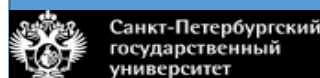
В коммерческом направлении: – вывод на глобальный рынок трех типов продуктов:

- 1) **10G-шифратор на основе квантового распределения ключей** – для использования в магистральных оптоволоконных линиях связи (между ЦОДами);
- 2) **среднемасштабные квантовые компьютеры на основе нейтральных атомов** в микродипольной ловушке и **фотонных чипов** с возможностью удаленного сетевого доступа для решения тестовых задач на основе квантовых алгоритмов;
- 3) высокоскоростные малогабаритные **квантовые генераторы случайных чисел** – для использования в широком спектре криптографической аппаратуры.

В образовательном направлении:

запуск трех образовательных программ, ориентированных на подготовку специалистов широкого профиля в области прикладных квантовых технологий;
запуск системы **дополнительного образования** для повышения квалификации работников технологических предприятий, заинтересованных во внедрении квантовых технологий;
запуск системы **онлайн образования** по квантовым технологиям для максимально широкого круга слушателей, включая **практикум**.

ЧЛЕНЫ КОНСОРЦИУМА:



Санкт-Петербургский
государственный
университет

- Санкт-Петербургский государственный университет



- МГТУ имени Н.Э.Баумана

2

ОБРАЗОВАНИЕ



- Федеральный исследовательский центр «Казанский научный центр РАН»



- Институт физики полупроводников имени А.В.Ржанова СО РАН



- Институт физики твердого тела РАН

4



- Физико-технологический институт РАН

НАУКА



- АО «Концерн «Автоматика»

3

ПРОИЗВОДСТВО
КОММЕРЦИАЛИЗАЦИЯ



- ООО НТПП «Криптософт» (г. Пенза)



ОАО «Информационные технологии и коммуникационные системы»



- «Ассоциация защиты информации»

ПРАВОВАЯ ЗАЩИТА

1



- ВНИИА имени Н.Л.Духова (ГК «Росатом»)

ПОТРЕБИТЕЛЬ

1

Суть технологии

Квантовые технологии: инструменты хранения, обработки, обеспечения безопасности информации и алгоритмы решения задач посредством квантово-механических систем.

Проблема и решение

ЦЕЛЬ: понять, как фундаментальные законы квантовой физики могут способствовать улучшению технологий приема, передачи и обработки информации

Тренды & disruption

Мотивация: Классические информационные технологии не обеспечивают потребности пользователей

Решение: Использование квантовых технологий

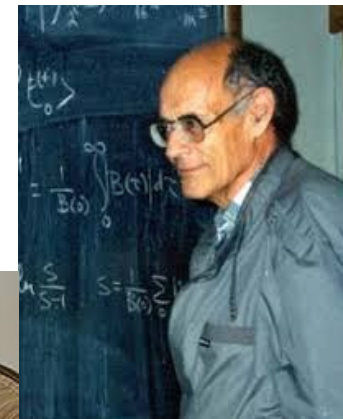
Инструментарий: квантовые биты и суперпозиции;
квантовый параллелизм,
квантовые непрерывные измерения;
перепутывание как новый ресурс и проч.

ЗАДЕЛЫ МГУ В КВАНТОВЫХ ТЕХНОЛОГИЯХ:



ФУНДАМЕНТАЛЬНЫЙ ЗАДЕЛ базируется на коллективах четырех всемирно известных научных школах физического факультета МГУ:

Школа квантовой оптики Д.Н. Клышко



Школа квантовых измерений В.В. Брагинского



Школа взаимодействия излучения с веществом Л.В. Келдыша

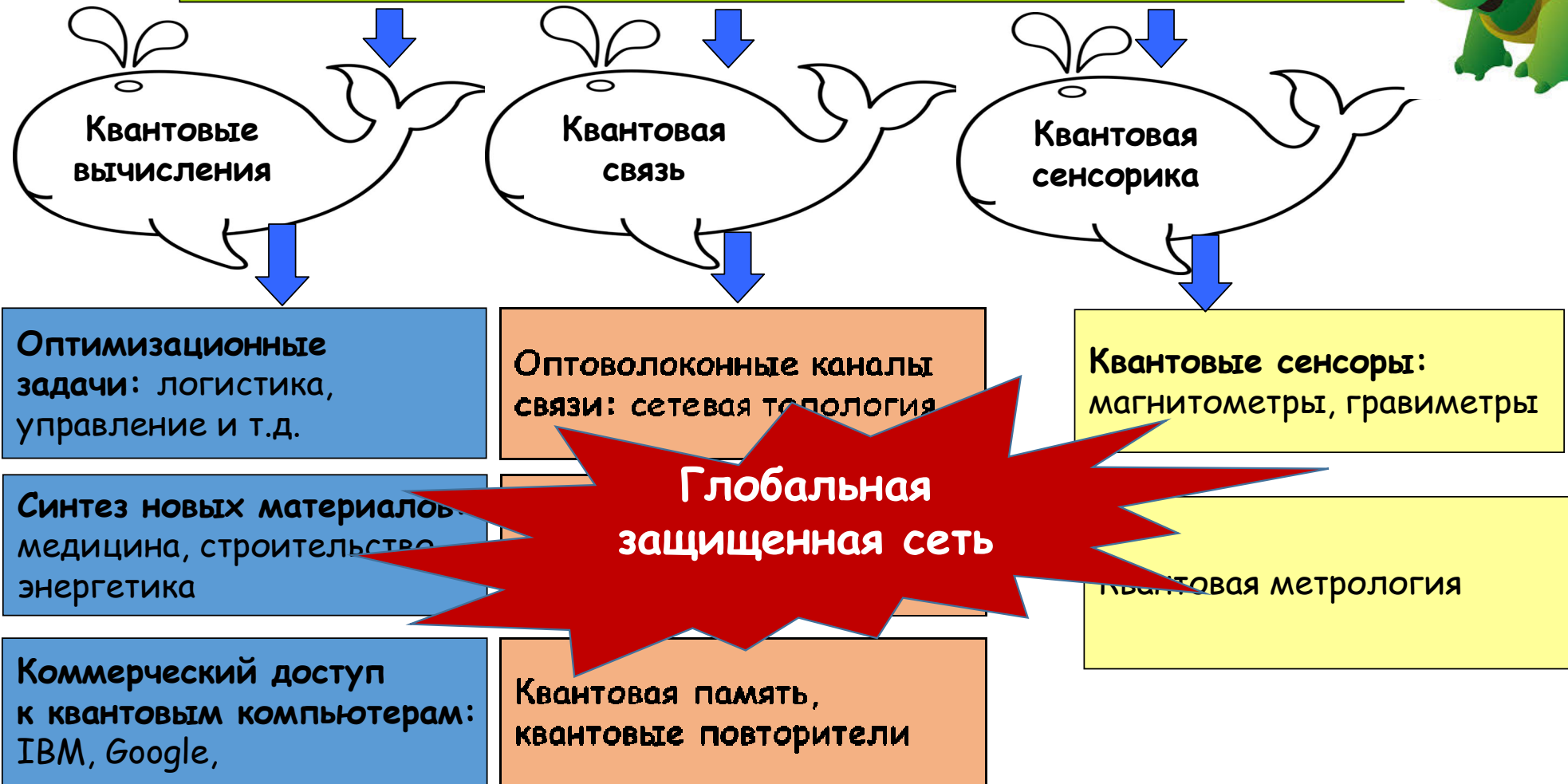


Школа квантовой одноэлектроники К.К. Лихарева



В этих школах было получено большое количество научных результатов, опережающих мировой уровень

Квантовая обработка информации. КВАНТОВЫЕ ТЕХНОЛОГИИ: три кита



АНАЛОГИЧНЫЕ ЦЕНТРЫ В МИРЕ:
Исследования, технологии, коммерциализация, образование



ПЕРСПЕКТИВЫ КОММЕРЦИАЛИЗАЦИИ



КВАНТОВАЯ СВЯЗЬ

ШИФРАТОРЫ:

Планируемая рыночная цена продукции составляет 20 млн. руб. и соответствует наиболее близким по характеристикам зарубежным изделиям, потенциально доступным к покупке компаниями.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

КВАНТОВЫЕ СИМУЛЯТОРЫ СРЕДНЕГО МАСШТАБА

организация доступа потенциальных потребителей (научно-исследовательские организации, R&D отделы производственных компаний) к прототипам симуляторов

коммерциализация побочных результатов и разработок:

- лазерные системы со стабильной частотой;
- аппаратная база интегрально-оптических компонентов и проч.

Учебно-научный практикум:

организация доступа, модульный принцип, автоматический режим (научно-исследовательские и образовательные организации, R&D отделы производственных компаний)

Квантовые вычисления

В настоящий момент в мире имеется несколько реалистичных кандидатов физ. систем для реализации квантовых вычислений.

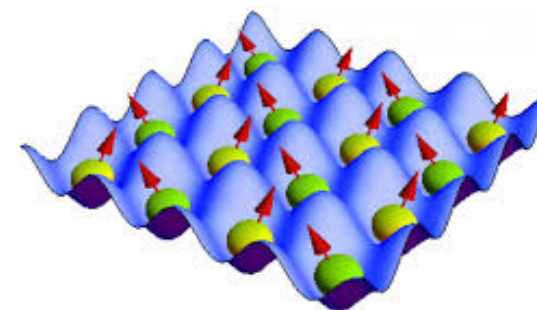
Пока не известно, какая технология станет базовой!

В Российской Федерации интенсивно развиваются четыре платформы:

1. Сверхпроводящие структуры
2. Нейтральные атомы и молекулы
3. Линейно-оптические квантовые вычисления
4. Примесные спины в твердотельных структурах

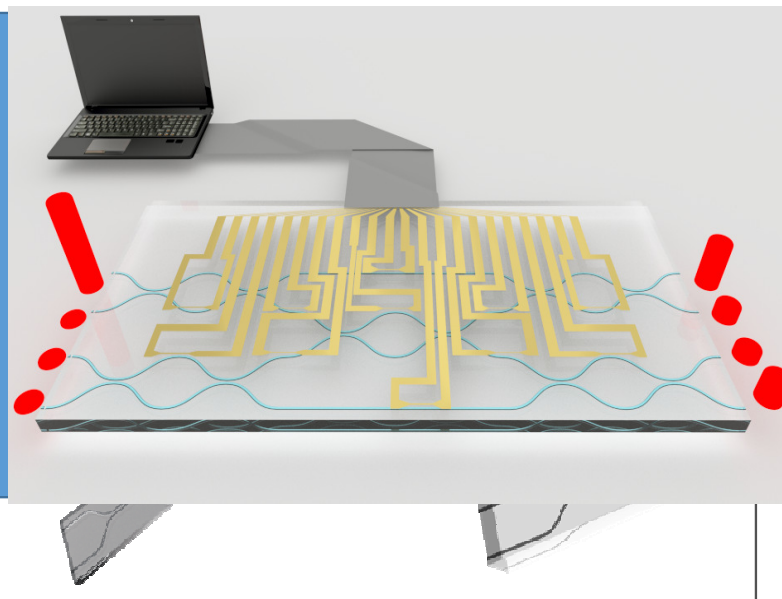
КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Атомная оптика - перспективы:
Создание атомного кристалла - регистра
для выполнения квантовых вычислений;
Квантовый ретранслятор.

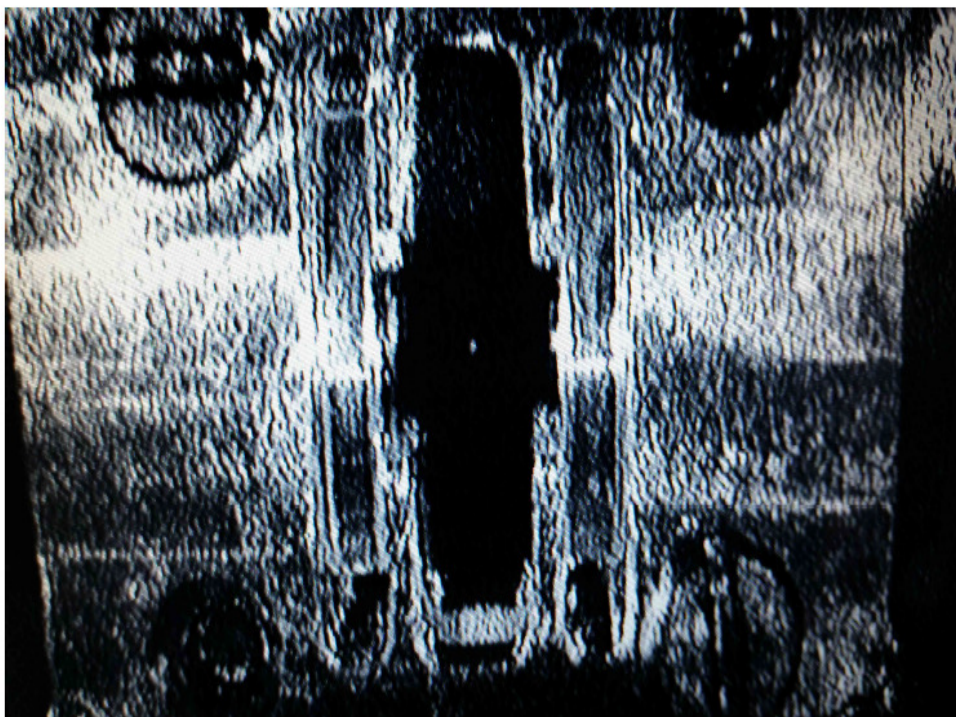


2. Линейно-оптические вычисления

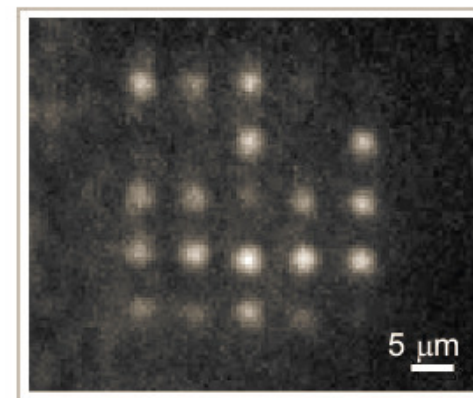
Перспективы:
Создание программируемых чипов
и реализация вычисления спектров
сложных молекул



КВАНТОВЫЕ ВЫЧИСЛЕНИЯ НА ОСНОВЕ НЕЙТРАЛЬНЫХ АТОМОВ

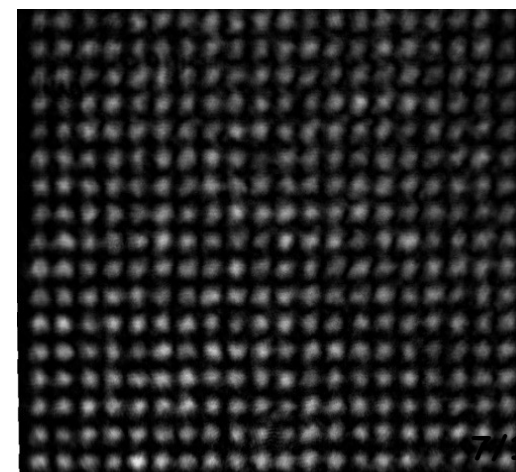


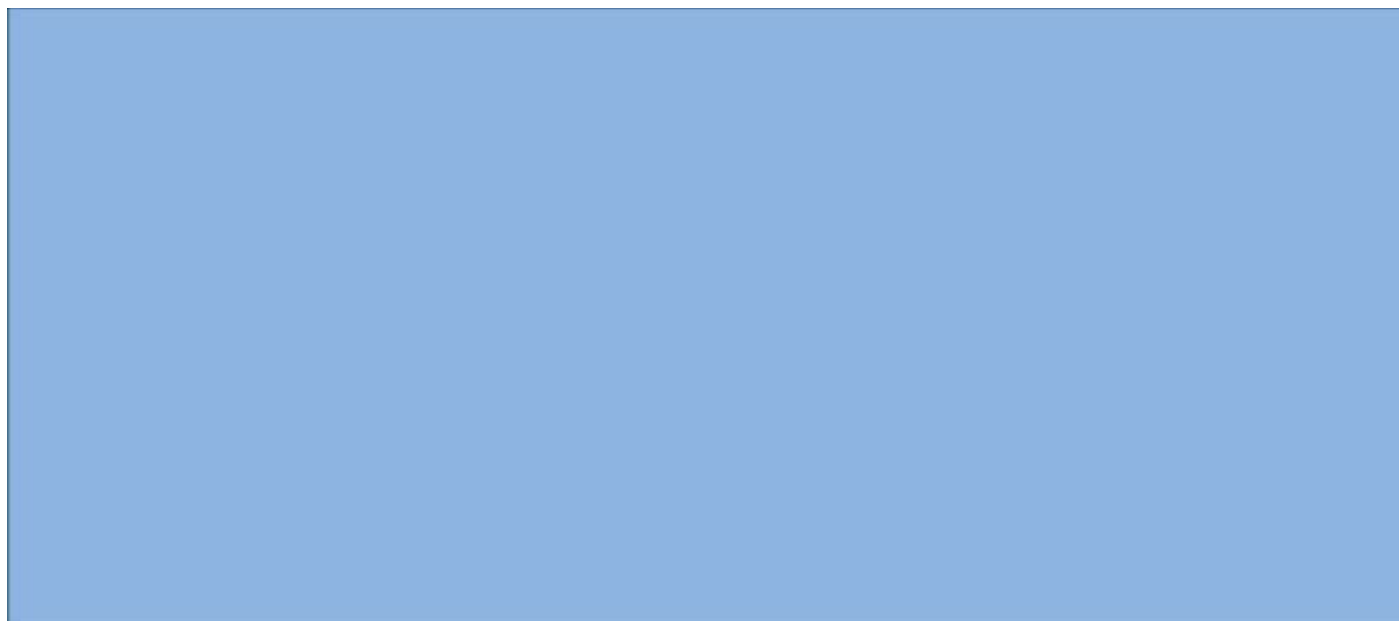
Экспериментальный комплекс по охлаждению,
удержанию и оптическому мониторингу
одиночных атомов в дипольной микроловушке



Время удержания в ловушке
одиночного атома рубидия
около 100 с.

Создание квантовых регистров
для задач квантовой симуляции
и квантовых вычислений



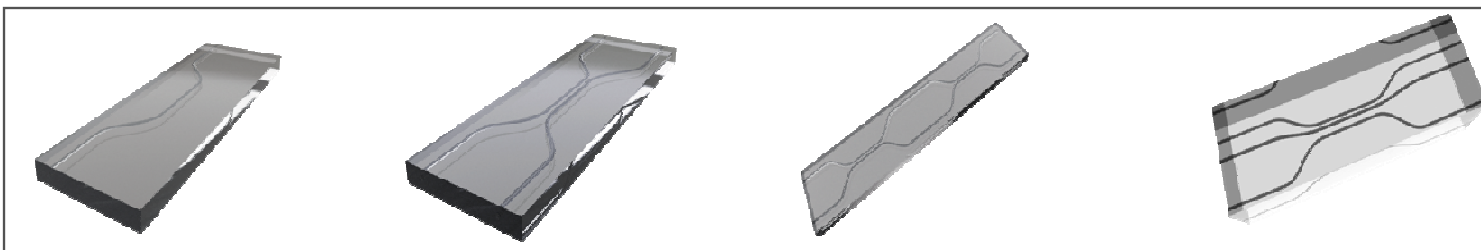


Одномодовый
оптический
волновод

Интегрированный
светоделитель

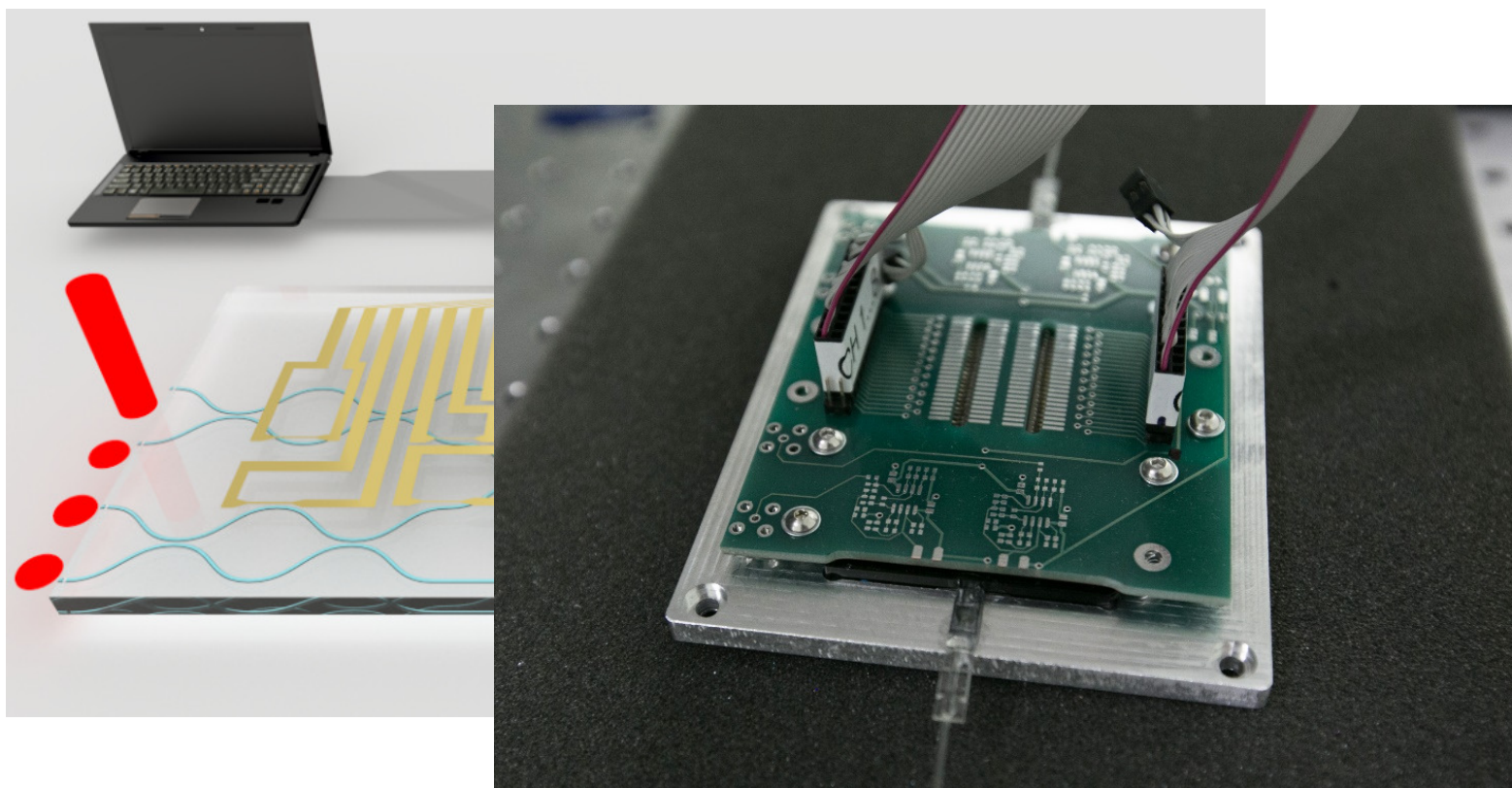
Интегрированный
интерферометр
Маха-Цандера

Трехмерные
интегрально-
оптические
структуры



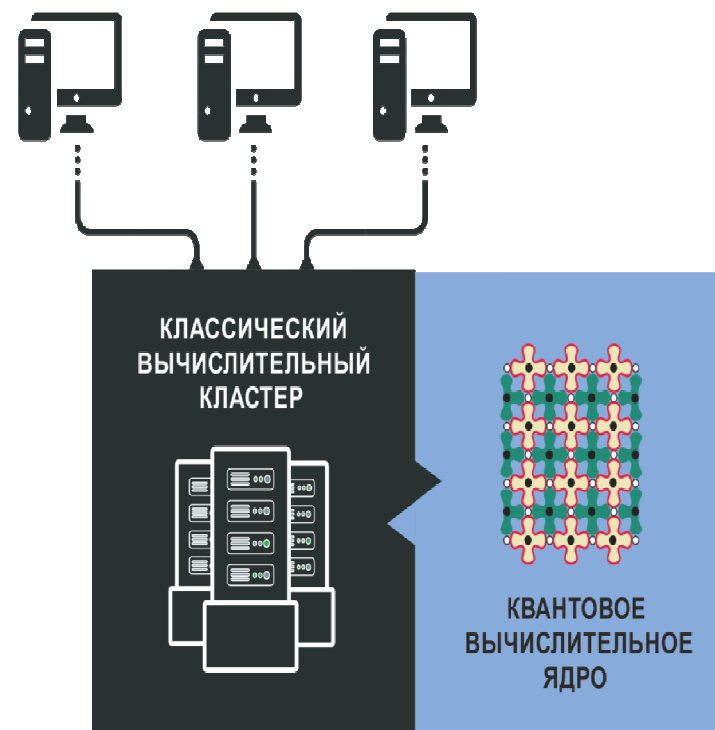
КВАНТОВЫЕ ВЫЧИСЛЕНИЯ НА ОСНОВЕ ЛИНЕЙНОЙ ОПТИКИ

Прототип программируемого оптического чипа – базовый элемент
квантового линейно-оптического симулятора/вычислителя



Разработка и создание квантовых симуляторов среднего масштаба (10-50 кубитов)

- Создание специализированного квантового симулятора **на основе одиночных атомов в оптических ловушках**;
- Создание **линейно-оптического квантового симулятора**
- Разработка универсальной аппаратно-независимой управляющей системы
- Разработка специализированных квантовых алгоритмов и их адаптация под прикладные задачи



**Некоторые задачи переборного типа:
сопоставление производительности классического
суперкомпьютера и квантового компьютера**

| Наименование задачи | Время вычисления на классическом компьютере эксафлопсной (10^{18} флопс) производительности | Время вычисления на квантовом компьютере мегафлопсной (10^6 флопс) производительности |
|--|--|--|
| Разложение натурального числа с количеством десятичных знаков K на простые сомножители (факторизация). Алгоритм Шора | $K=250$ 200 часов $K=500$ 10 млн. лет $K=1000$ $4 \cdot 10^{17}$ лет | $K=250$ 4 с $K=500$ 18 с $K=1000$ 84 с |
| Вычисление дискретного логарифма для чисел с количеством десятичных знаков K | Ускорение сопоставимо с алгоритмом Шора | |
| Быстрый поиск в большой базе данных, содержащей N элементов. Алгоритм Гровера Ускорение \sqrt{N} раз | $N=10^6$ 10 с $N=10^9$ 3 часа $N=10^{15}$ 4 месяца | $N=10^6$ 10мс $N=10^9$ 0,3 с $N=10^{15}$ 10 с |
| Нахождение подстроки длины M в строке длины N (алгоритм Амбайниса), | Ускорение сопоставимо с алгоритмом Гровера | |

Квантовая коммуникация/связь

Волокна

*Вывод защиты
информации на
принципиально иной
уровень!*

одное простран

Квантовые интерфейсы
и память

Квантовая коммуникация – это область знаний/техники
о передаче квантовых состояний между удаленными объектами



КВАНТОВАЯ СВЯЗЬ И КВАНТОВАЯ КРИПТОГРАФИЯ: мировые разработки

- ★-Разработка высокоскоростных магистральных шифраторов для передачи больших объемов данных между ЦОД.
- ★-Разработка волоконных сетей с квантовым распределением ключей в реконфигурируемой топологии: объединение в локальные сети и магистральные линии передачи данных в защищенном режиме
- ★-Разработка скоростных квантовых генераторов случайных чисел
- ★-Генерация секретных ключей через открытое пространство между стационарными и подвижными объектами, между несколькими подвижными объектами.
- ★-Построение глобальной системы распределения ключей, включающей элементы волоконных систем и систем, работающих через открытое пространство, включая спутники.

По всем направлениям работа ведется на физическом факультете МГУ при поддержке

Фонда перспективных исследований, Министерства обороны РФ, ФСБ России, Министерства науки и высшего образования и др.

| № | Наименование | Краткое описание проекта |
|----|--|--|
| 1. | Квантовый телефон VipNet | <p>Сеть с квантовым распределением ключей (далее – КРК) является расширением классической сети VipNet. Она представляет собой виртуальную защищенную сеть, которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология VipNet обеспечивает защищенное взаимодействие между сетевыми узлами по схеме «клиент-клиент».</p> |
| 2. | Высоко-скоростной квантовый шифратор 10G | <p>Единая интегрированная система, включающая устройства квантового распределения ключей и классические шифраторы. Комплекс квантово-криптографической аппаратуры защиты информации предназначен для передачи через сеть связи общего пользования информации и её криптографической защиты. Защищаемая информация передается от источника к приемнику, находящихся за пределами Комплекса в доверенных сетях передачи.</p> |

3. Многокубитный
квантовый
симулятор

Многокубитный квантовый симулятор представляет собой вычислительную систему с открытым доступом по сети Internet. Вычислительное устройство включает в себя два процессора на основе двух различных физических систем: холодные атомы в оптической ловушке и одиночные фотоны в линейно-оптических сетях. Каждый из процессоров может быть использован по отдельности, либо, если возможно разбиение задачи, могут работать параллельно.

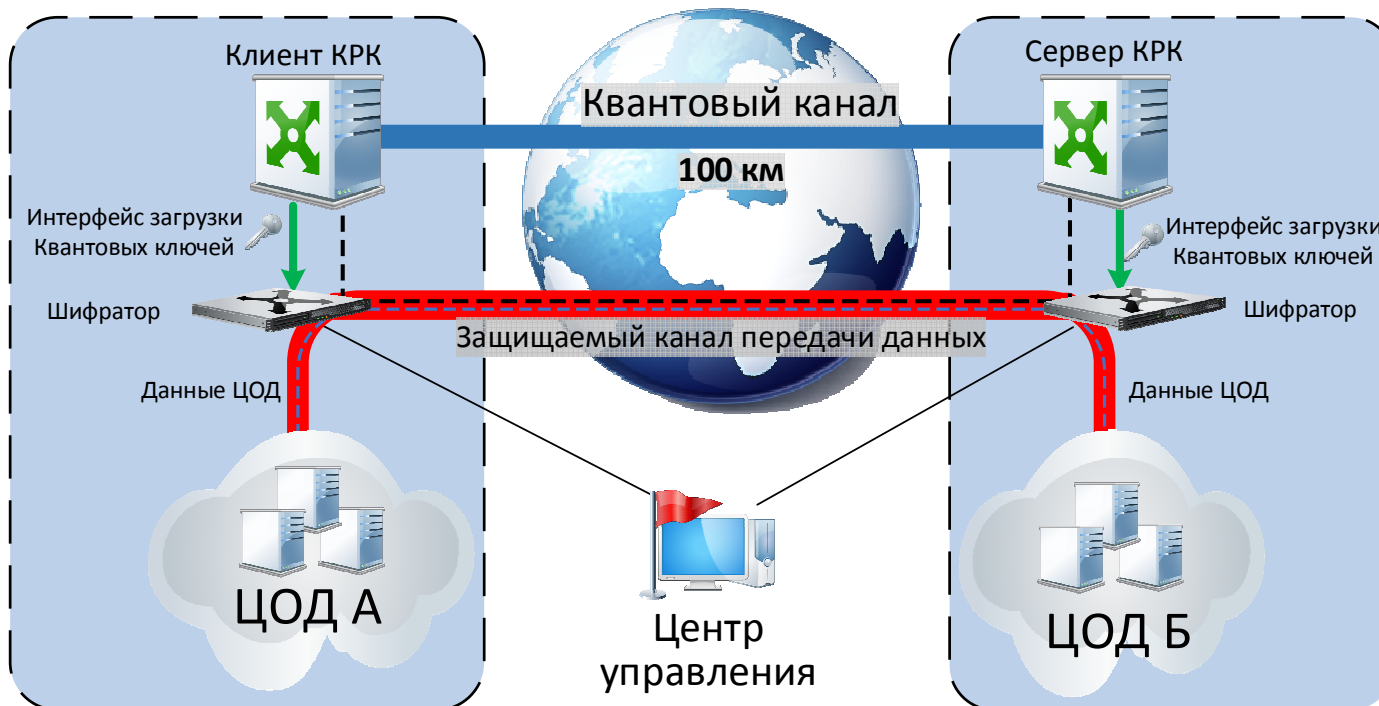
4. Научно-
образовательный
практикум по
квантовой оптике
и квантовой
информатике

Будет создан практикум по квантовой оптике и квантовой информатике, в рамках которого студенты ВУЗов или сотрудники учебных, научных и промышленных компаний, проходящие курсы повышения квалификации по направлениям, связанным с квантовыми технологиями, смогут на практике увидеть, как работают законы квантовой физики в реальном эксперименте. Такой опыт позволит обучающимся понять принципы квантовой физики на примере задач квантовой информатики.

ViPNet Quandor



Комплекс квантово-криптографической аппаратуры защиты информации, состоящий из 10G шифратора канального уровня (L2) и оборудования квантового распределения ключей (КРК)



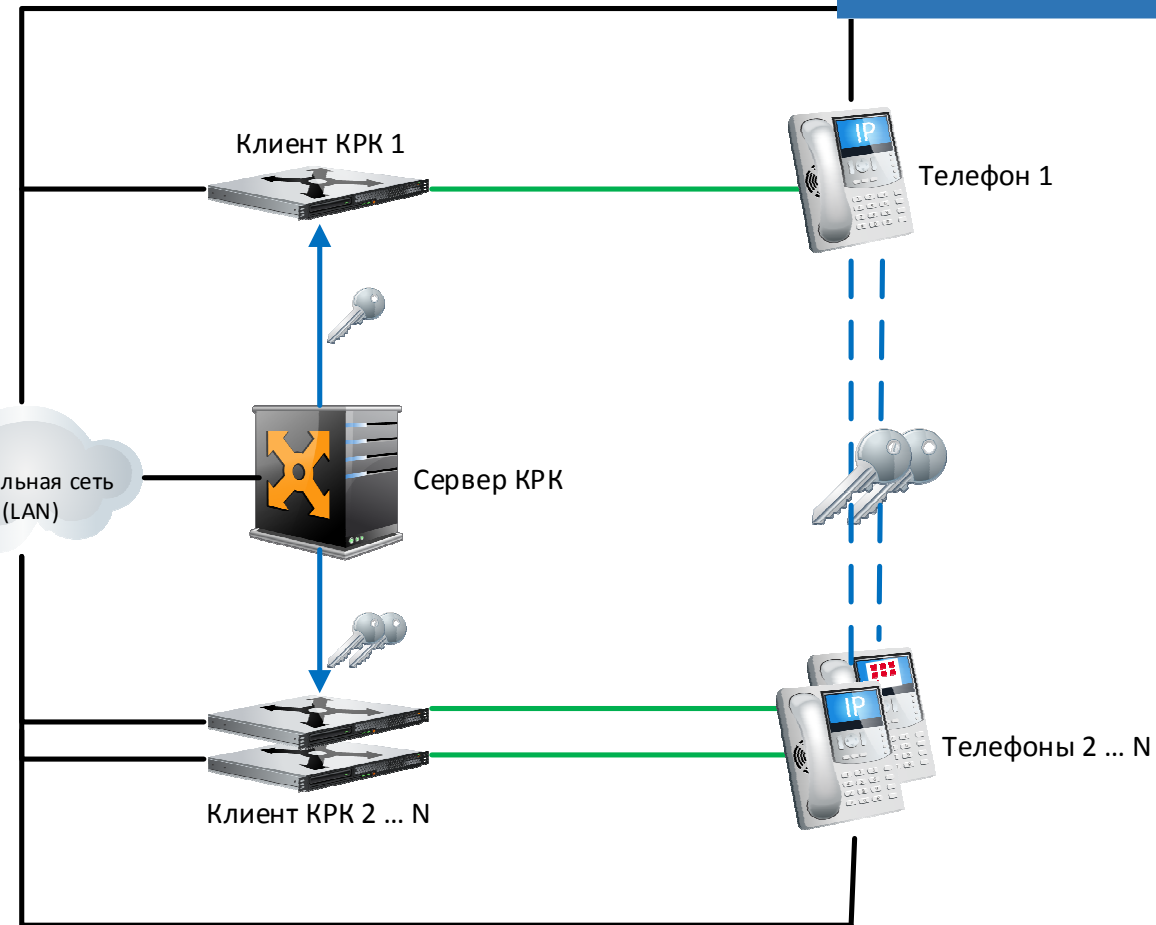
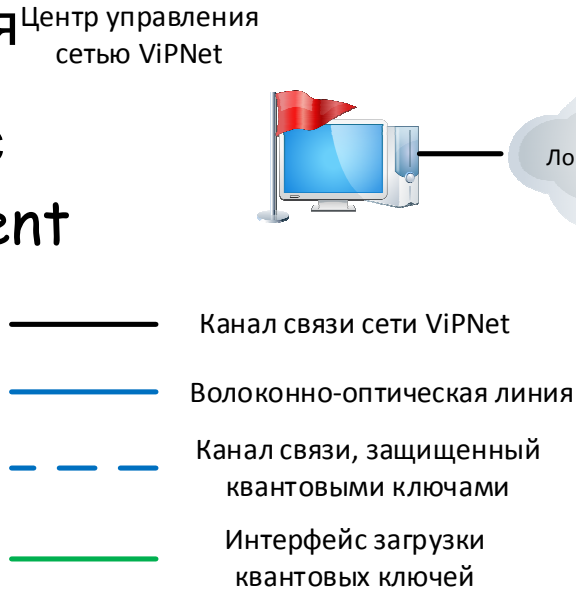
- ✓ скорость шифрования по ГОСТ 34.12-2015 «Кузнечик»:
 - 20 Гбит/с дуплекс
- ✓ имитозащита
- ✓ задержка ~15 мкс

- ✓ длина линии квантовой связи 100 км
- ✓ воздушное охлаждение
- ✓ автоматический режим работы

VIPNet Quantum Security System



Оборудование
 квантового
 распределения
 ключей (КРК)
 сопряженное с
 ПО ViPNet Client
 и Connect
 на телефонах
 абонентов



Предложение: технология «QUANTEL»



QS

Phone



ОБРАЗОВАНИЕ

преимущества

вовлеченность в образовательный процесс
нескольких факультетов МГУ:



физического,

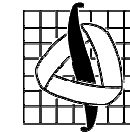
- вычислительной математики и кибернетики,



ВМК МГУ

Факультет вычислительной математики и кибернетики
Московского государственного университета имени М. В. Ломоносова

- механико-математического



планируется открытие трех специализированных магистерских программ, он-лайн практикума и программ дополнительного образования:

«инженерный уклон»



*базовая часть
вариативная часть*



«алгоритмический уклон»

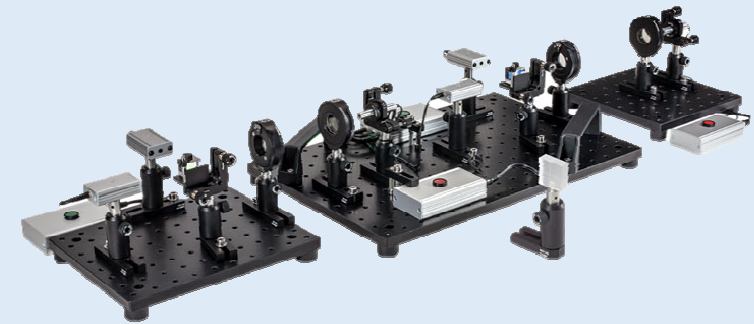
«КВАНТОВАЯ КРИПТОГРАФИЯ И КВАНТОВАЯ СВЯЗЬ»;

«КВАНТОВЫЕ ВЫЧИСЛЕНИЯ»;

«КВАНТОВЫЕ ОПТИЧЕСКИЕ ТЕХНОЛОГИИ»

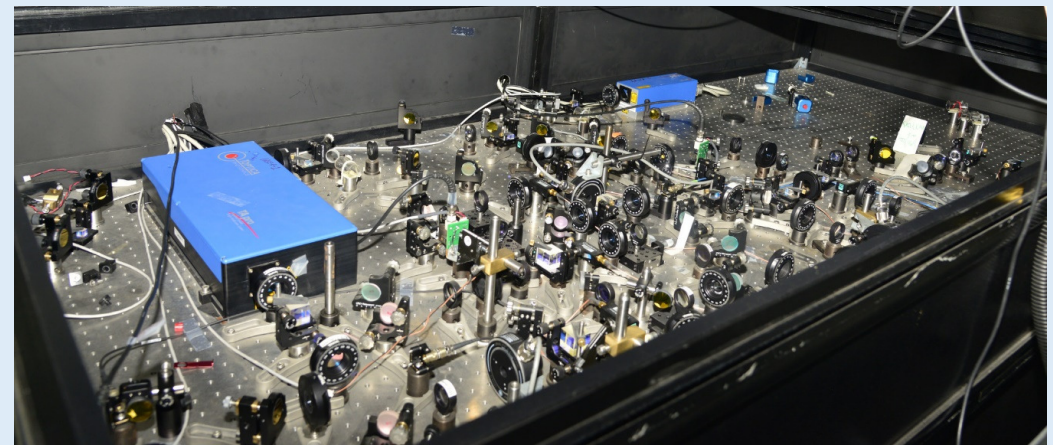
Поляризационная оптика

1. Поляризация света
2. Поляризационные элементы
3. Томография поляризационного кубита
4. Протоколы квантовой криптографии
5. Томография однокубитного квантового процесса



Квантовая оптика

1. Спонтанное параметрическое рассеяние
2. Неравенства Белла
3. Томография квантовых состояний
4. Квантовое распределение ключа
5. Квантовый генератор случайных чисел
6. Статистика фотонов
7. Провал Манделя
8. Гомодинное детектирование



Онлайн-курс «Квантовая электроника»



Автор курса— Сергей Павлович Кулик, д.ф.-м.н. профессор, научный руководитель Центра квантовых технологий физического факультета МГУ имени М.В.Ломоносова



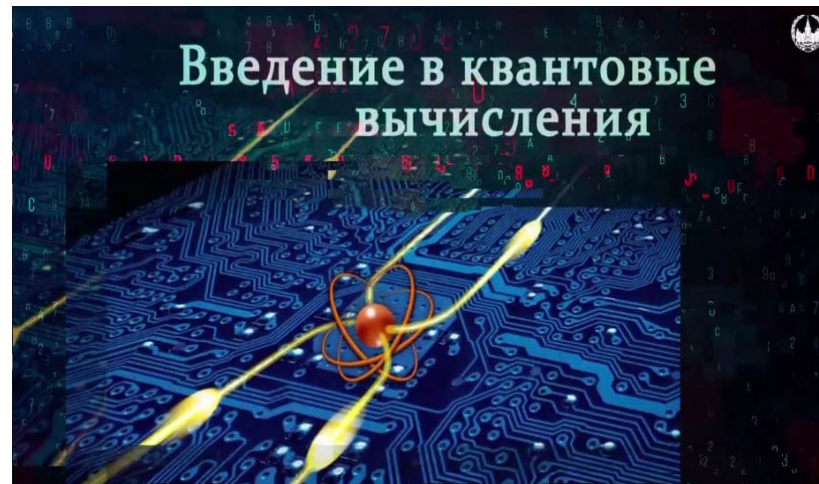
Курс посвящен физическим основам квантовой электроники, освоению основных понятий теории взаимодействия поля и вещества (вынужденное излучение и поглощение, инверсия населенностей и отрицательная температура, сечение взаимодействия, диэлектрическая восприимчивость, релаксация, спонтанные переходы, когерентное взаимодействие).

Основные разделы программы: вероятность перехода в случае когерентного и некогерентного поля, коэффициент поглощения и усиления, линейная поляризация среды, эффект насыщения, нестационарные эффекты (самоиндуцированная прозрачность, оптическое эхо, сверхизлучение).

Онлайн-курс «Введение в квантовые вычисления»



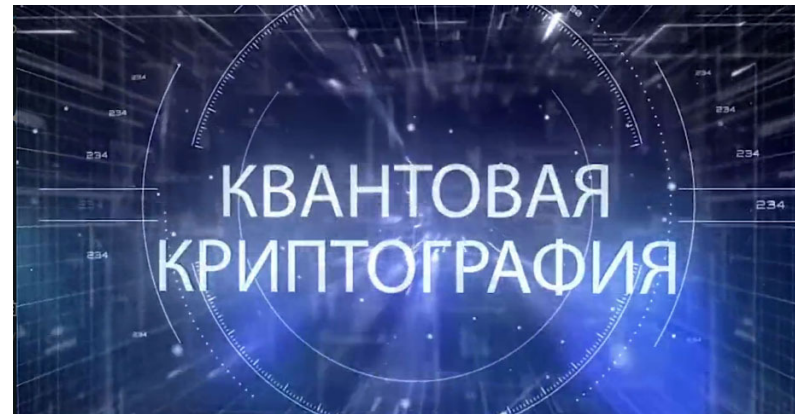
Автор курса - **Станислав Сергеевич Страупе**,
к.ф.-м.н., ведущий научный сотрудник Центра квантовых технологий
физического факультета МГУ имени М.В.Ломоносова



В курсе рассмотрены такие темы, как гейтовая модель квантовых вычислений и универсальные наборы квантовых логических вентилей, основные типы квантовых алгоритмов; проблемы борьбы с декогеренцией и ошибками в квантовых вентилях, вопросы построения квантовых кодов коррекции ошибок. Рассмотрены варианты архитектуры квантового компьютера, устойчивого к ошибкам. Также в рамках курса будут обсуждаться вопросы принципиальной возможности создания устойчивого к ошибкам квантового компьютера и реальное положение дел при современном уровне развития технологий.

Автор курса - **Сергей Николаевич Молотков**

-профессор, д.ф.-м.н., ведущий научный сотрудник Центра квантовых технологий МГУ, профессор кафедры суперкомпьютеров и квантовой информатики факультета вычислительной математики и кибернетики МГУ имени М.В.Ломоносова



На лекциях рассмотрены базовые протоколы квантового распределения ключей; основные фундаментальные принципы работы и устройство современных систем квантового распределения криптографических ключей, понятийный и математический аппарат, используемый при доказательстве стойкости систем квантовой криптографии, как в оптоволоконном варианте, так и работающих через открытое пространство; различные виды атак на такие системы, а также методов противодействия им. Также определены принципиальные отличия и новые возможности, по сравнению с классическими методами распределения ключей. Слушатели курса научатся анализировать криптографическую стойкость таких систем по отношению к различным атакам на них и применять полученные знания при решении и постановке типовых задач в области квантовой криптографии.

Онлайн-курсы ЦКТ

реализуются Центром развития электронных образовательных ресурсов МГУ на платформе «Открытое образование» <https://openedu.ru>, начиная с весеннего семестра 2019 года.

По итогам обучения, в случае успешной аттестации, выдаётся сертификат об освоении курса, который может быть засчитан студентами в части освоения образовательной программы вуза.

Для сотрудников и преподавателей вуза, имеющих высшее образование, предусмотрен дополнительный модуль повышения квалификации по методике преподавания в данной предметной области.

Любые вопросы по онлайн-курсам вы можете задать по электронной почте

education@quantum.msu.ru

**Программы дополнительного образования:
курсы повышения квалификации**



РОССИЙСКАЯ ФЕДЕРАЦИЯ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В.Ломоносова

УДОСТОВЕРЕНИЕ
о повышении квалификации

ПК МГУ № **015153**

Удостоверение является документом установленного образца

Регистрационный номер **0318a9007**
Дата выдачи **28 февраля 2018 г.**
Город Москва

Настоящее удостоверение подтверждает, что _____
(фамилия, имя, отчество)
проходил(а) обучение в Московском государственном университете
имени М.В.Ломоносова на (в) **Физическом факультете**
(наименование структурного подразделения)
по программе **«Квантовая обработка информации и
квантовые технологии»**
(наименование программы повышения квалификации, тема стажировки)
в объеме **68 часов**
с «**21**» ноября **2017** г. по «**13**» февраля **2018** г.
Решение аттестационной комиссии от «**12**» февраля **2018** г.

Ректор Московского университета _____ М.П.
Секретарь
аттестационной комиссии _____

International school on quantum technology



Школы по квантовым технологиям:
2018, 2019 - Сочи, Красная Поляна

<http://qutes.org/>

А
В

Севастополь
2%

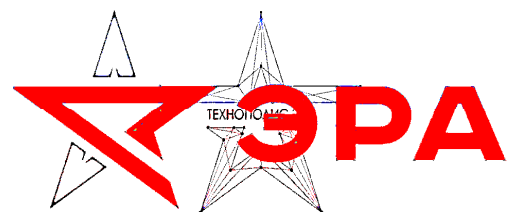
Владимир
2%

Долгопрудный
2%



2-я Рос

Потенциальные потребители



Санкт-Петербургский
государственный
университет

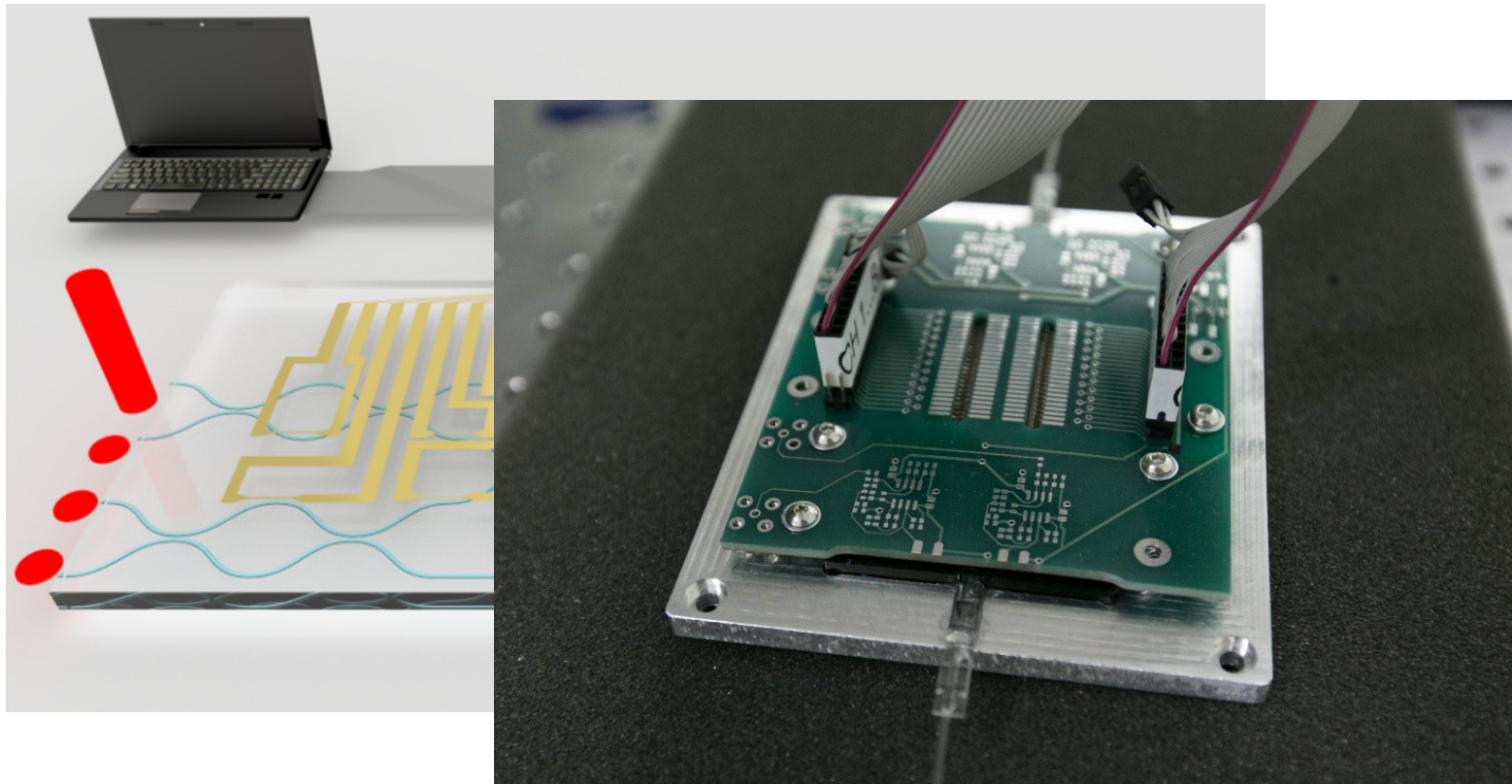


СПАСИБО ЗА ВНИМАНИЕ!

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ НА ОСНОВЕ ЛИНЕЙНОЙ ОПТИКИ



Прототип программируемого оптического чипа – базовый элемент
квантового линейно-оптического симулятора/вычислителя



Квантовый датчик случайных чисел 100 Мб/с

