

Квантовые технологии: проблемы и перспективы

Сергей Кулик

14 Всероссийская летняя школа учителей физики

29 июня по 05 июля 2026 года



Физический факультет Московского государственного университета
имени М.В. Ломоносова

КВАНТОВЫЕ ТЕХНОЛОГИИ: три кита

Quantum Technologies



Ионы и нейтральные атомы
в ловушках

Оптоволоконные каналы

Сенсоры
электрических и
магнитных полей



Линейно-оптические
вычисления
(фотонные чипы)

Атмосферные/космические
каналы:
мобильные и стационарные

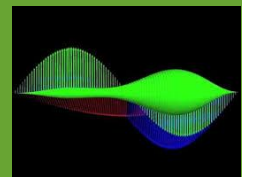
Часы,
гравиметры,
гироскопы



Сверхпроводниковые кубиты

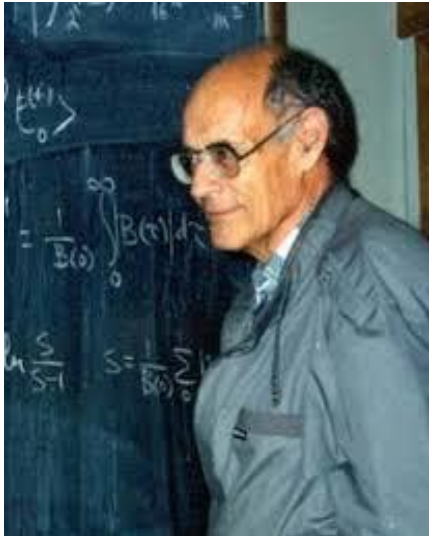
Квантовая память,
квантовые интерфейсы...

Квантовая
метрология



Россия

фундаментальный задел: научные Школы



Д.Н.Клышко
Квантовая
оптики



Л.В.Келдыш
Взаимодействие
излучения с веществом



В.Б.Брагинский
Квантовые измерения



К.К. Лихарев
Одноэлектронные
устройства

ОСНОВНЫЕ ЦЕЛИ И ПЕРСПЕКТИВЫ

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

Решение: использование квантовых технологий

Инструментарий: квантовые биты и суперпозиции;
квантовый параллелизм,
непрерывные квантовые переменные;
перепутывание как новый ресурс и т.д.

Примеры: кубиты вместо классических битов

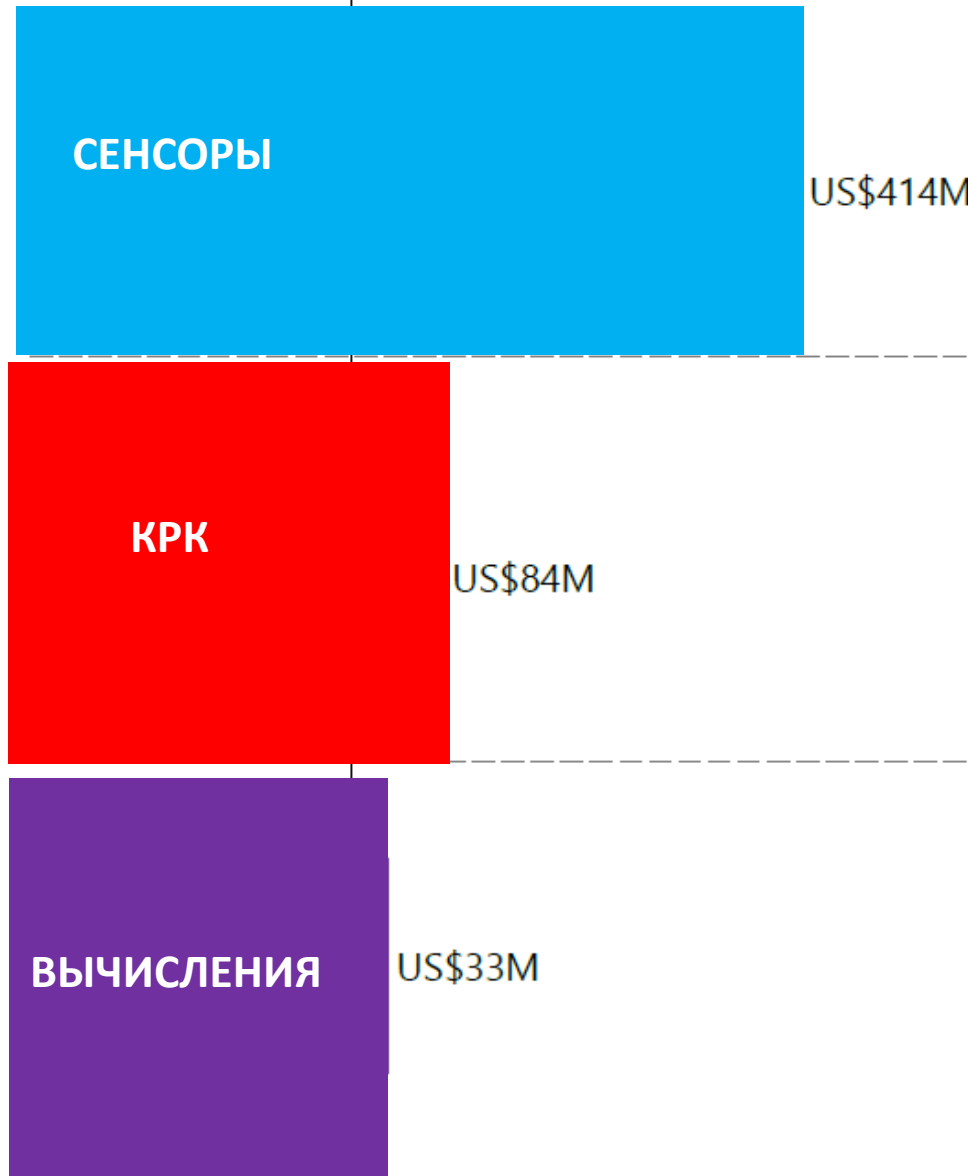
$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle$ (двухуровневая система) либо "0" либо "1" (trigger)

$|\Psi_{12}\rangle = \frac{1}{\sqrt{2}} \{ |0_1\rangle|1_2\rangle + |1_1\rangle|0_2\rangle \}$ перепутанное состояние нет аналогов

ВЛОЖЕНИЯ В ОТРАСЛЬ



ОБЪЕМ РЫНКА КТ (2020)



ПРОНОЗ (2030)

>2 миллиардов \$

>7 миллиардов \$

>50 миллиардов \$

ПЕРСПЕКТИВЫ ОТРАСЛИ



КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: QUANTUM COMPUTING



Что такое квантовый компьютер?

1. Это физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных преобразований (т.е. сохраняющих энергию), не нарушающих квантовые суперпозиции в процессе вычислений.

2. Это физический компьютер, работа которого:

основана на уникальных свойствах квантовой физики; принципиально отличается от практически всех существующих компьютеров (которые в совокупности называются классическими)

3. Это физическое устройство, использующее квантово-механические явления, такие как суперпозиция и запутанность, проекционный постулат (Борна и др.) и выполняющее последовательность унитарных преобразований с помощью квантовых вентилей, которая заканчивается **проекционным измерением**.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: QUANTUM COMPUTING



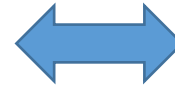
Проблема 1 - уменьшение размеров интегральных схем, т.е. отдельных элементов. Нанотехнологии.
Естественный предел здесь - характерный масштаб атома, когда вступают в силу законы микромира, т.е. квантовой механики.

Проблема 2 – уменьшение доли рассеиваемой энергии. Логически обратимые операции - те, которые не сопровождаются рассеянием энергии (Ландауэр, 1961г.).

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: QUANTUM COMPUTING



Универсальный квантовый
компьютер



Коды коррекции ошибок
(Quantum Error Correction)

Альтернативы

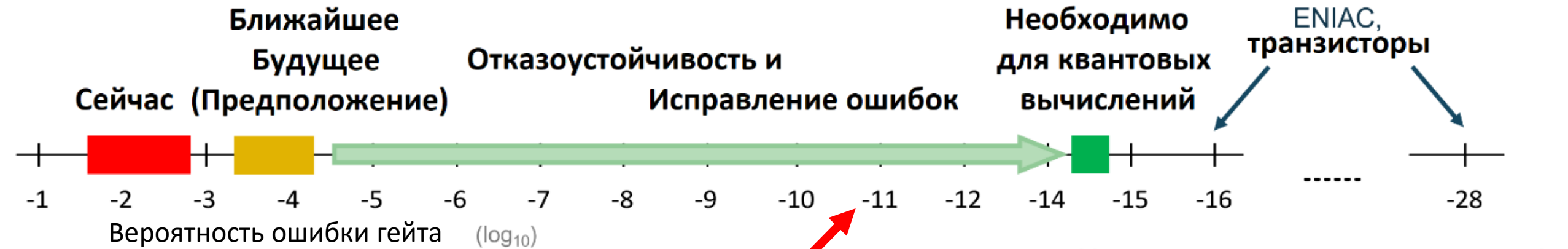
NISQ
(noisy intermediate-scale quantum)
компьютеры –
прядка сотни кубитов

Квантовый отжиг
(quantum annealing)

Сортировка бозонов
(boson sampling)

Квантовые симуляторы

ПРЕДЕЛЬНЫЙ УРОВЕНЬ ОШИБОК ДЛЯ ВЫПОЛНЕНИЯ ПОЛНОМАСШТАБНЫХ КВАНТОВЫХ ВЫЧИСЛЕНИЙ



Для поверхностных кодов:

Квантовые компьютеры для специальных приложений и ограниченного спектра задач

Квантовые компьютеры широкого применения: общецелевые, масштабируемые, точные

$$P_{\text{logical}} \approx C \left(P_{\text{physical}} / P_{\text{threshold}} \right)^{(d+1)/2} \quad d = \sqrt{n}, \quad C \approx 0.1, \quad P_{\text{threshold}} \approx .01$$

Пусть $P_{\text{physical}} = .001, P_{\text{logical}} = 10^{-11} \Rightarrow d = 19, n = 361$ физических кубитов на один логический

Если $P_{\text{physical}} = 10^{-4} \Rightarrow d = 9, n = 81$

John Preskill, US QIS Summer School July 2024

ОЦЕНКИ НЕОБХОДИМЫХ РЕСУРСОВ

(ЧИСЛА ЛОГИЧЕСКИХ КУБИТОВ, ЭЛЕМЕНТАРНЫХ КВАНТОВЫХ ВЕНТИЛЕЙ)

ДЛЯ ПОЛНОГО ПОИСКА КЛЮЧА ШИФРОВАНИЯ

ДЛЯ АЛГОРИТМА ШИФРОВАНИЯ AES С РАЗНОЙ ДЛИНОЙ КЛЮЧА*

*Для идеальных квантовых вентилей

длина ключа k	вентили		глубина схемы		число логических кубитов
	T	Клиффорд	T	всего	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6681

$$T\text{-gate} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$$

Клиффорд:

$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{pmatrix}; \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

ДАННЫЕ АНАЛИЗА ДЛЯ ОПТИМИЗИРОВАННЫХ КВАНТОВЫХ АЛГОРИТМОВ ПОЛНОГО ПЕРЕБОРА КЛЮЧЕЙ ДЛЯ АЛГОРИТМА ШИФРОВАНИЯ AES С РАЗНОЙ ДЛИНОЙ КЛЮЧА ПРИ РАЗЛИЧНЫХ ВЕЛИЧИНАХ ВЕРОЯТНОСТИ ОШИБКИ НА ВЕНТИЛЬ

AES-128 оценки 2020				оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	101.66	15265	7.17×10^8	98.95	10924	4.04×10^9
10^{-5}	97.19	2545	1.77×10^6	94.2	7564	1.74×10^7

AES-192 оценки 2020				оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	137.39	163793	2.93×10^9	135.29	62156	1.12×10^{10}
10^{-5}	132.81	23393	7.81×10^6	130.67	11756	6.53×10^7

AES-256 оценки 2020				оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	170.49	218465	6.56×10^9	167.67	63884	2.24×10^{10}
10^{-5}	166.0	34865	1.61×10^7	163.82	13484	1.15×10^8

Параметры: p_g вероятность ошибки на вентиль

n_ℓ число логических кубитов

n_p число физических кубитов

s_q параметр секретности 2^{s_q}

Gheorghiu V., Mosca M. A resource estimation framework for quantum attacks against cryptographic functions. 2018-2021

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ:



Сегодня имеется несколько физических платформ для реализации квантовых вычислений. Ни одна из этих платформ не удовлетворяет в полной мере этим критериям.



P.N. Lebedev
Physical Institute



1. Ядерный магнитный резонанс

2. Ионы в ловушках

3. Нейтральные атомы в микродипольных ловушках

4. Квантовая электродинамика резонаторов

5. Линейные (и нелинейно) оптические вычисления (фотонные чипы)

6. Твердотельные системы на основе квантовых точек

7. Сверхпроводниковые цепи



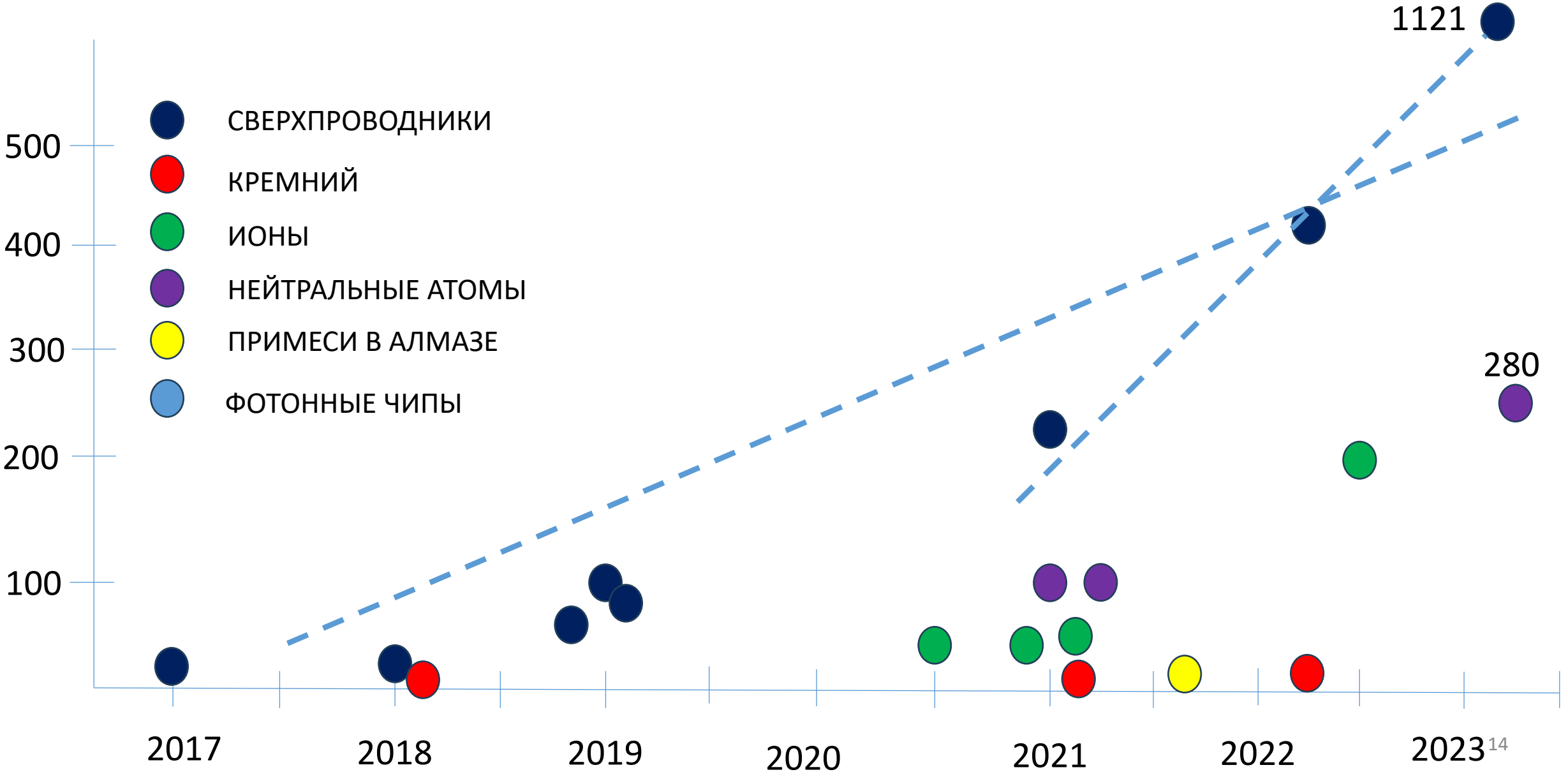
FMN
Laboratory

8. Твердотельные системы на основе спинов

9. Биологические и высокомолекулярные системы



ПРОГРЕСС В ОБЛАСТИ КВАНТОВЫХ ВЫЧИСЛЕНИЙ: ЧИСЛО КУБИТОВ



СПЕЦИАЛИЗИРОВАННЫЙ КВАНТОВЫЙ СОПРОЦЕССОР

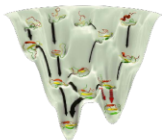
Квантовый отжиг



ПРИМЕНЕНИЕ
глобальная оптимизация

УНИВЕРСАЛЬНОСТЬ
ограниченная

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
ограниченная



Универсальный квантовый компьютер



ПРИМЕНЕНИЕ
защищенные вычисления
машинное обучение
криптография
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика
задачи поиска

УНИВЕРСАЛЬНОСТЬ
полная, математически обоснованное ускорение

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
очень высокая



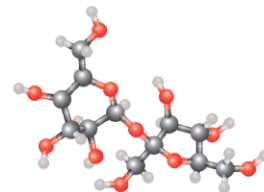
Noisy Intermediate-Scale Quantum

NISQ устройство

ПРИМЕНЕНИЕ
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика

УНИВЕРСАЛЬНОСТЬ
частичная

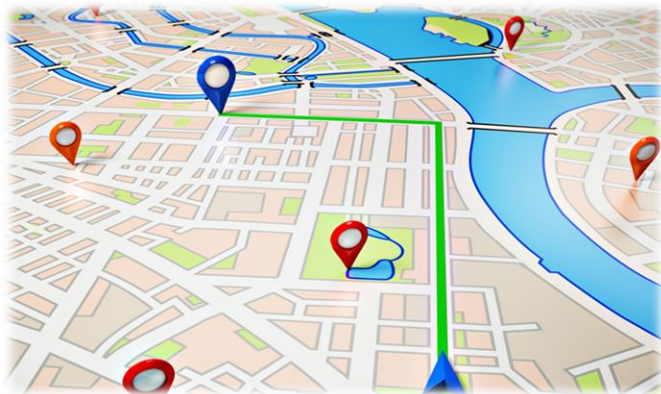
ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
высокая?



Сегодня обозначена возможность использования квантового компьютера для решения практически значимых задач

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: практически значимые задачи

Странствующий коммивояжёр

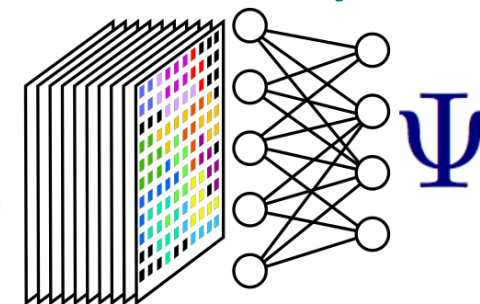


NP сложные задачи

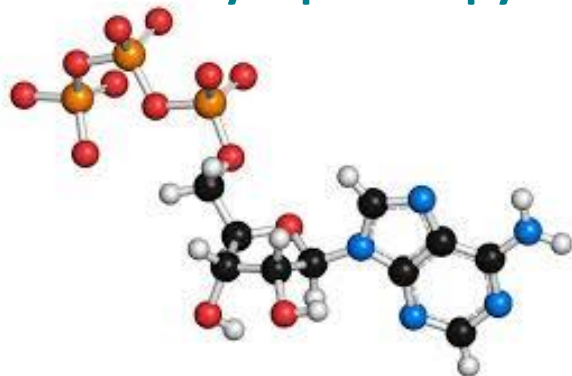
Комбинаторная оптимизация



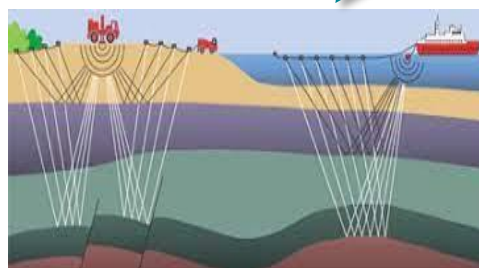
Машинное обучение



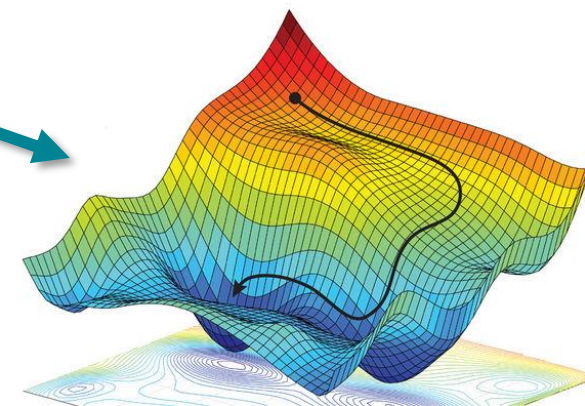
Молекулярная структура



«Сейсмика»



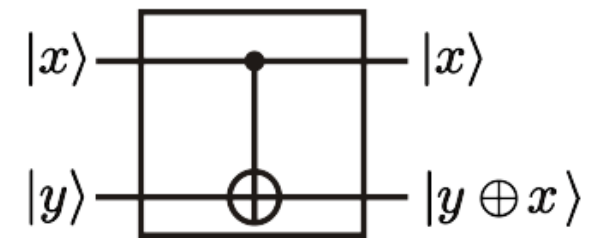
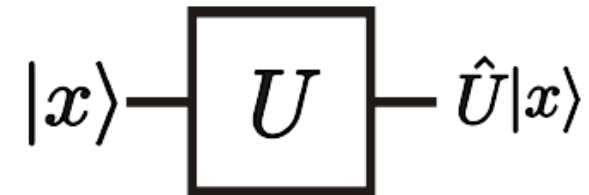
Глобальная оптимизация



Геологоразведка

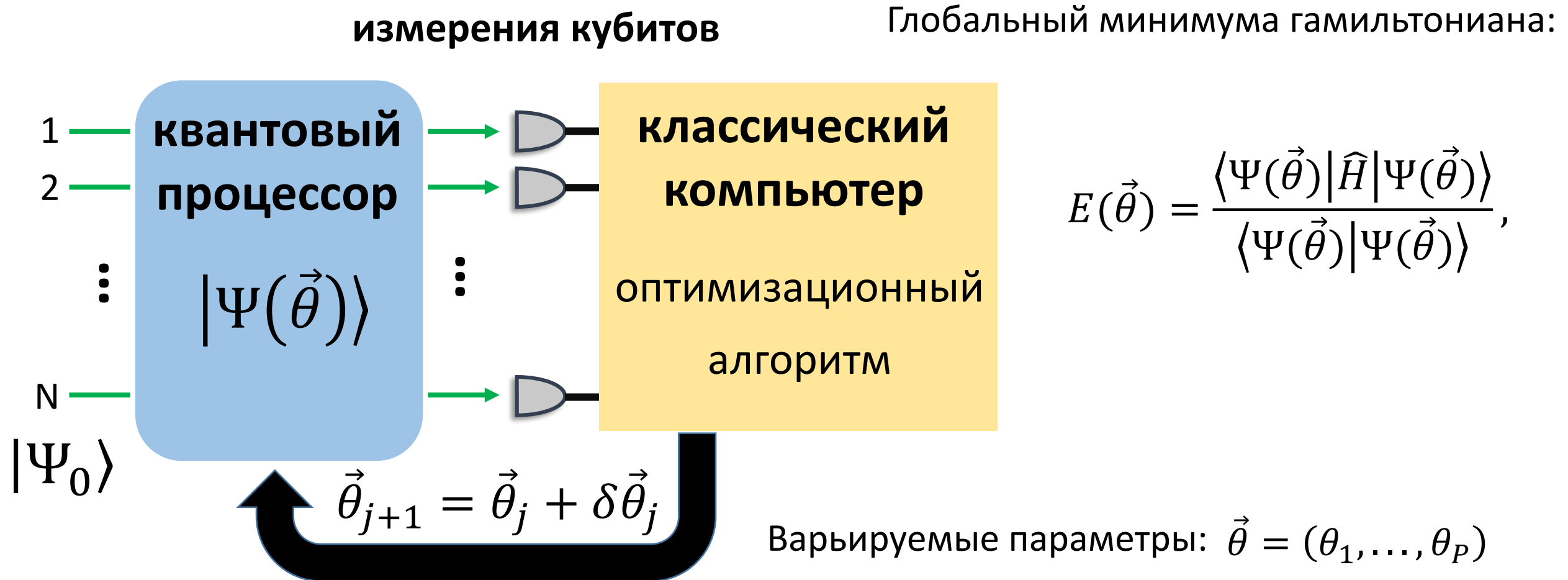
Универсальный набор гейтов¹

- ▶ Arbitrary single qubit gates
(H,S,T set is sufficient)
- ▶ Entangling two-qubit gate - for
example, a CNOT



¹A.Barenco, *et al.*, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995)

Линейно-оптические вычисления: вариационный алгоритм (VQE)



Критерии Ди Винченцо:

- масштабируемость;**
- надежная инициализация;**
- большие времена декогеренции (релаксации)
по сравнению с временем срабатывания
отдельных гейтов;**
- возможность манипуляций;**
- передача и считывание состояний кубитов**

СРАВНЕНИЕ МЕЖДУ РАЗНЫМИ ПЛАТФОРМАМИ



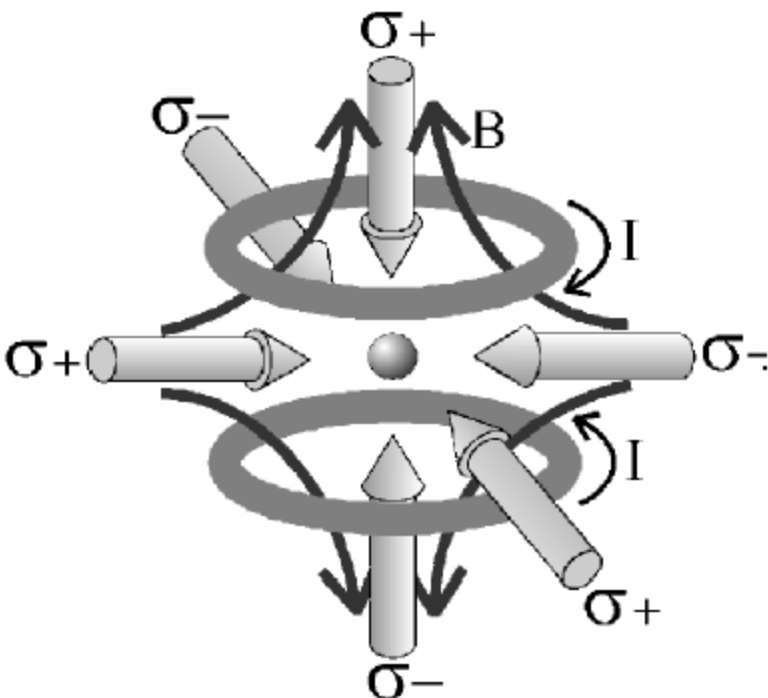
P.N. Lebedev
Physical Institute

	Ионы	Нейтральные атомы	Сверхпроводники	Фотоны	Примеси в кремнии
Масштабируемость	Симуляторы - 53 кубита 1D-2D Вычислители - 11 кубит (попарно связанных) [1,2]	Симуляторы – 51 кубит 1D-3D [5]	Вычислители - 72 кубита 1D-2D [9]	100 кубитов	2 кубита (2e ⁻)[12] 3 кубита (2 ядра+1e ⁻)
Время когерентности	До 10 мин [3]	До 7 с [6]	До 320 мкс [10]	«бесконечное»	30 с спин ядра 0.5 с спин e ⁻
Время срабатывания гейта	От 1 мкс	400 нс	10 нс	Менее 1 нс	0.8 нс
Fidelity (достоверность)	99.996% один кубит [4] 99.9% два кубита [4]	99.6% один кубит [7] 97.4% два кубита [8]	99.92 % один кубит[11] 99.4% два кубита [11]	99,9 один кубит 99,9 два кубита*	99.99 - 1 кубит 99.37 - 2 кубита
R-фактор	До 10⁹	До 10⁷	До 10⁴	«бесконечное»	До 10⁹

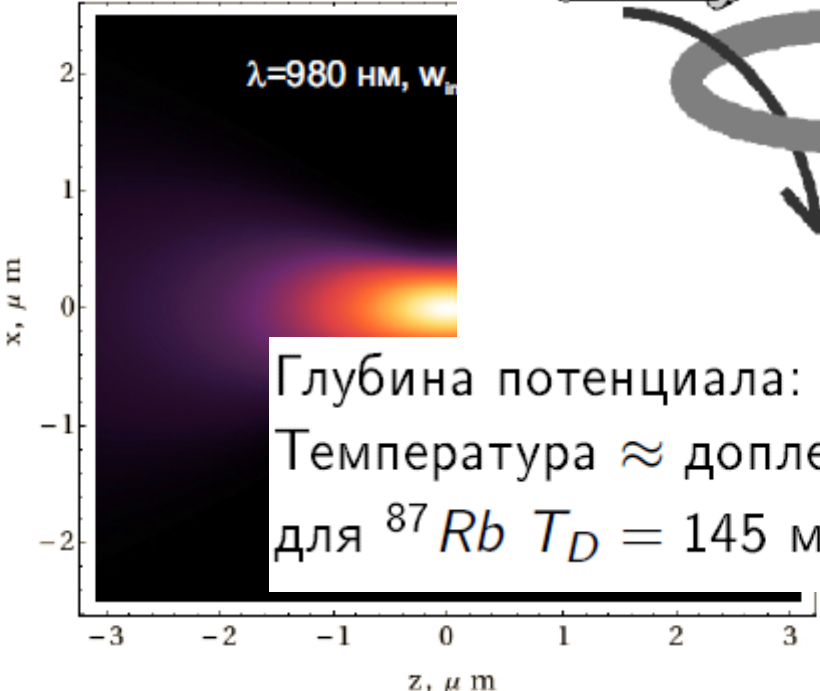
* Вероятностная модель – 10%

ВЫЧИСЛЕНИЯ НА НЕЙТРАЛЬНЫХ АТОМАХ: ХАРАКТЕРНЫЕ МАСШТАБЫ

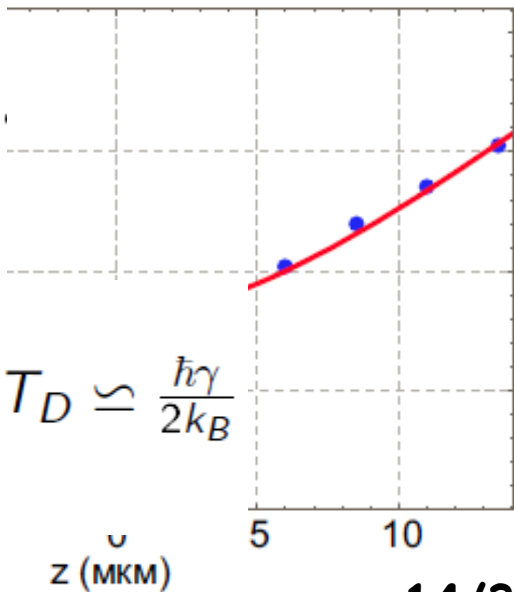
- ▶ Диодный лазер
- ▶ Фокусировка
- ▶ Глубина потенциала



мощность 30 мВт
 диаметр 3.1 мм
 охлаждение

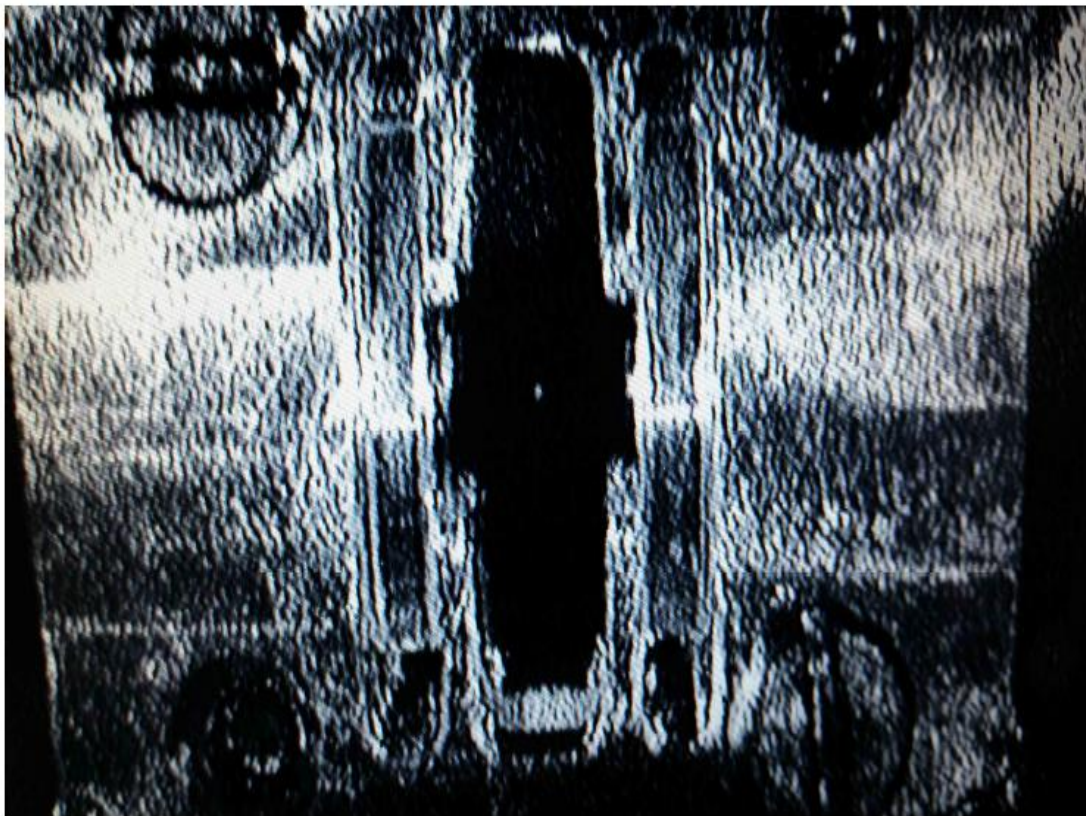


Глубина потенциала: $\sim 1 \text{ K}$
 Температура $\approx$ доплеровский предел
 для ^{87}Rb $T_D = 145 \text{ мкК}$

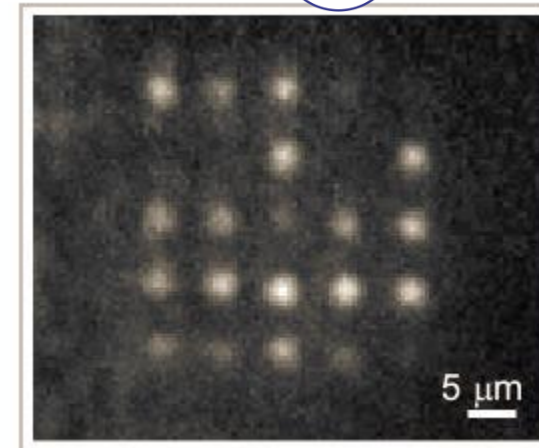


$$T_D \simeq \frac{\hbar \gamma}{2k_B}$$

ВЫЧИСЛЕНИЯ НА НЕЙТРАЛЬНЫХ АТОМАХ: РЕГИСТРЫ

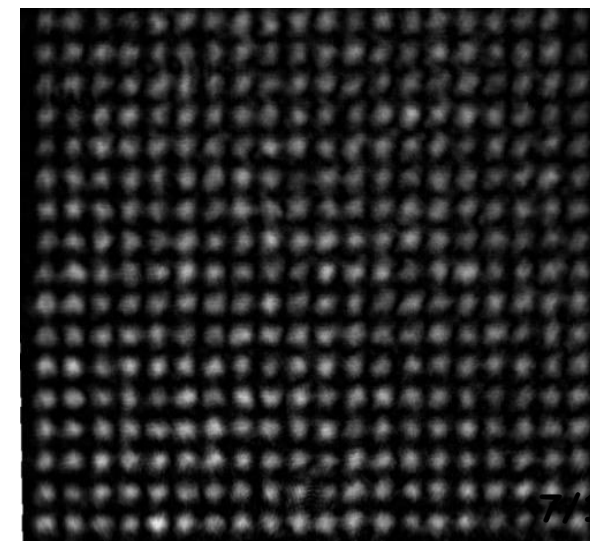


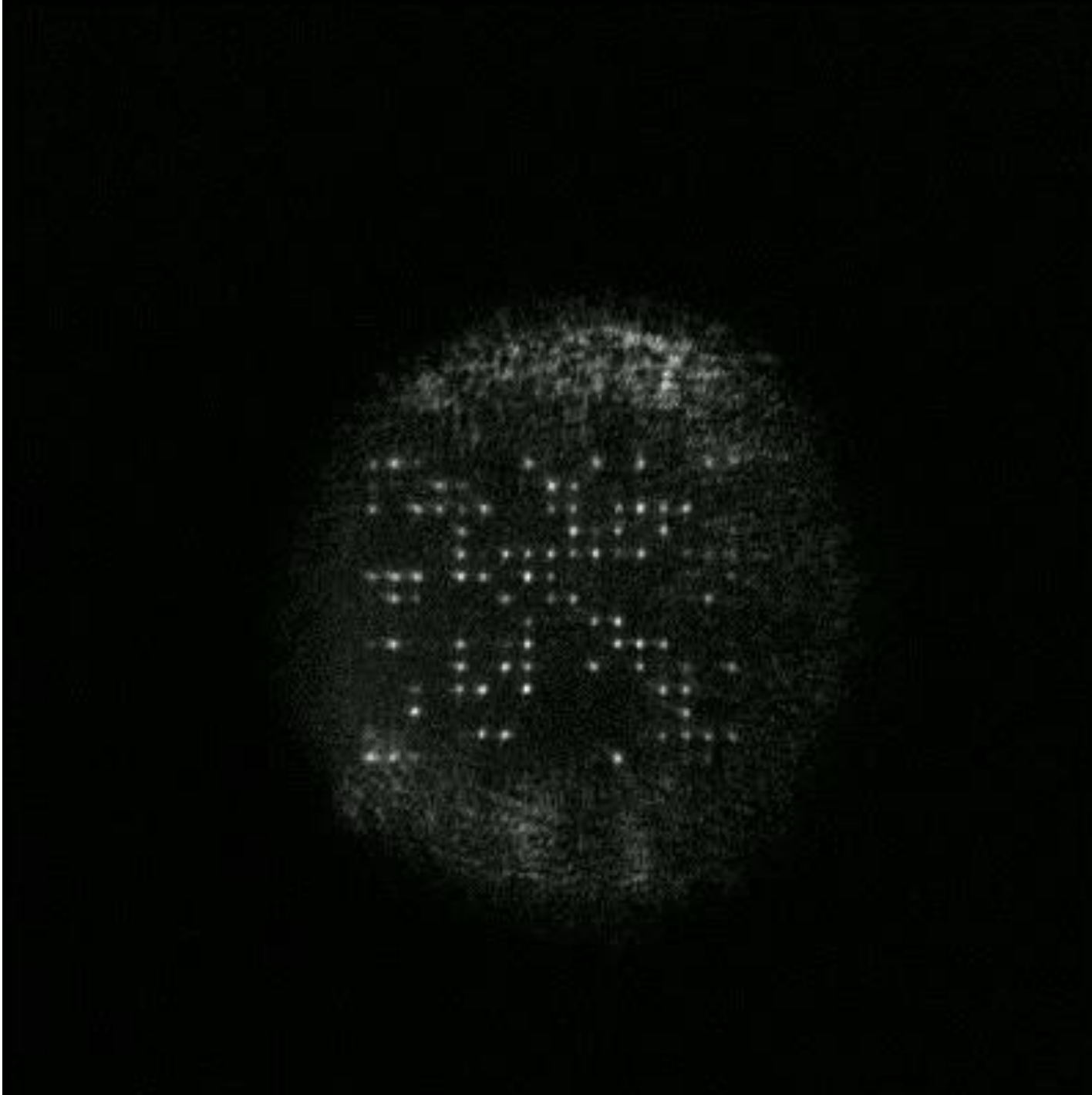
Экспериментальный комплекс по охлаждению,
удержанию и оптическому мониторингу одиночных
атомов в дипольной микроловушке



Время удержания в ловушке
одиночного атома рубидия
около 100 с.

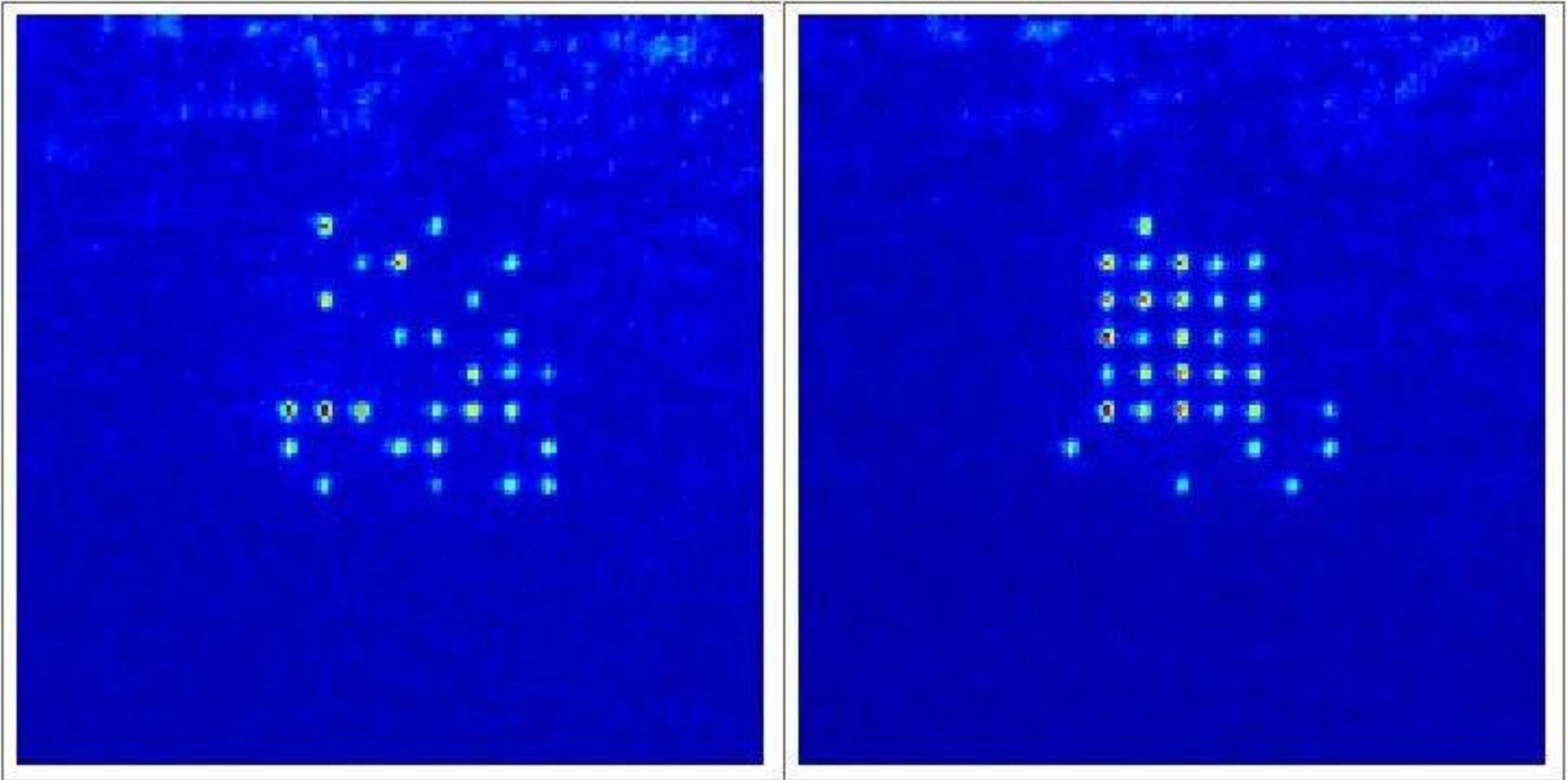
Создание квантовых регистров
для задач квантовой симуляции
и квантовых вычислений

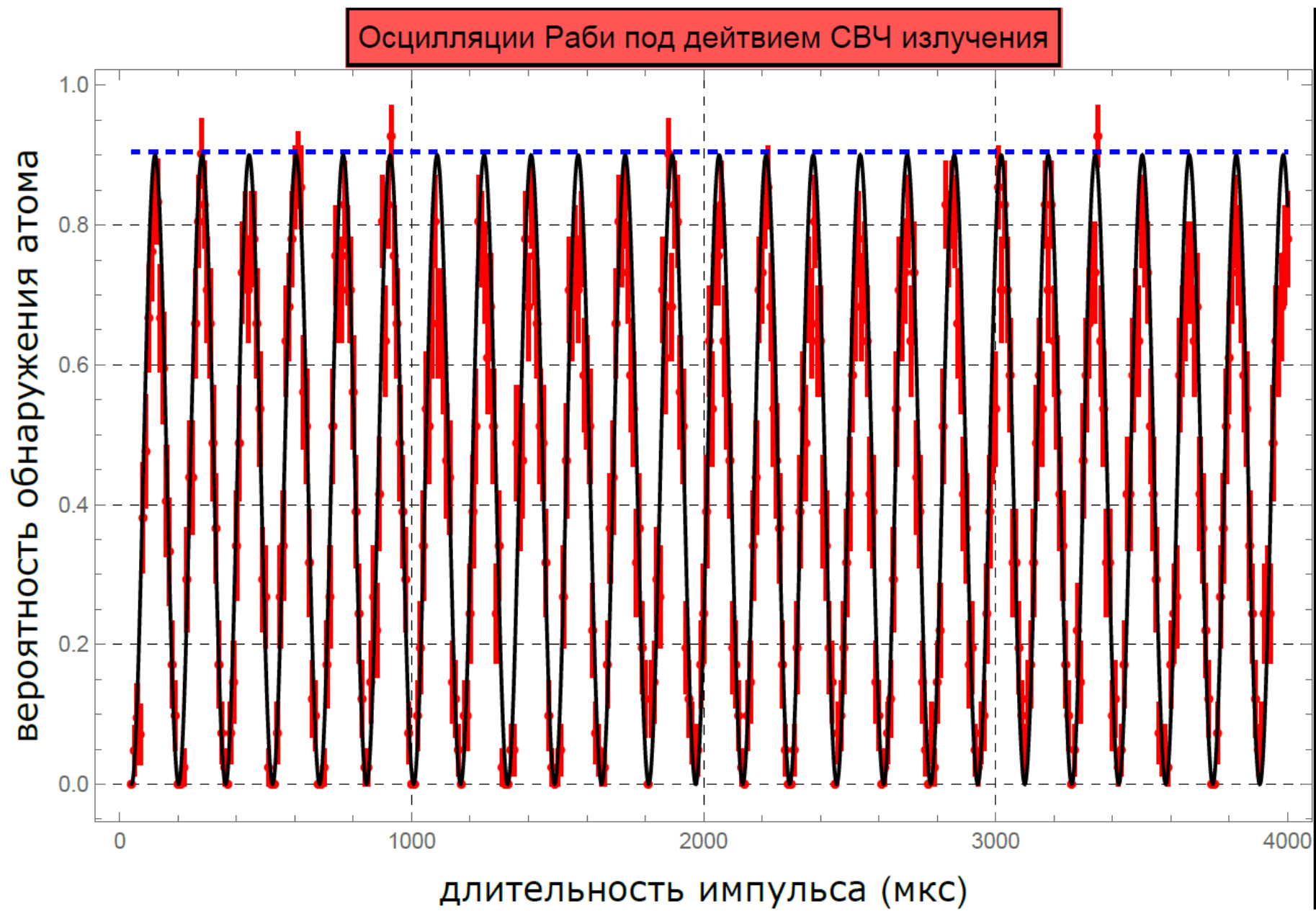




25 мкм

ВЫЧИСЛЕНИЯ НА НЕЙТРАЛЬНЫХ АТОМАХ: РАЗУПОРЯДОЧЕННЫЕ И УПОРЯДОЧЕННЫЕ РЕГИСТРЫ





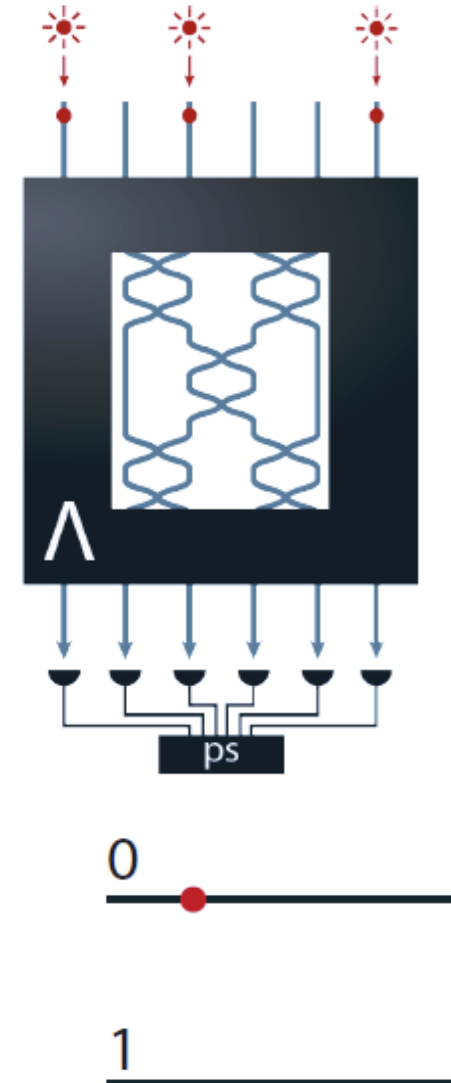
Основные блоки:

-  Однофотонный (N-фотонный) источник;
-  Линейные преобразования (интерферометры);
-  Однофотонные (N-фотонные) приемники.

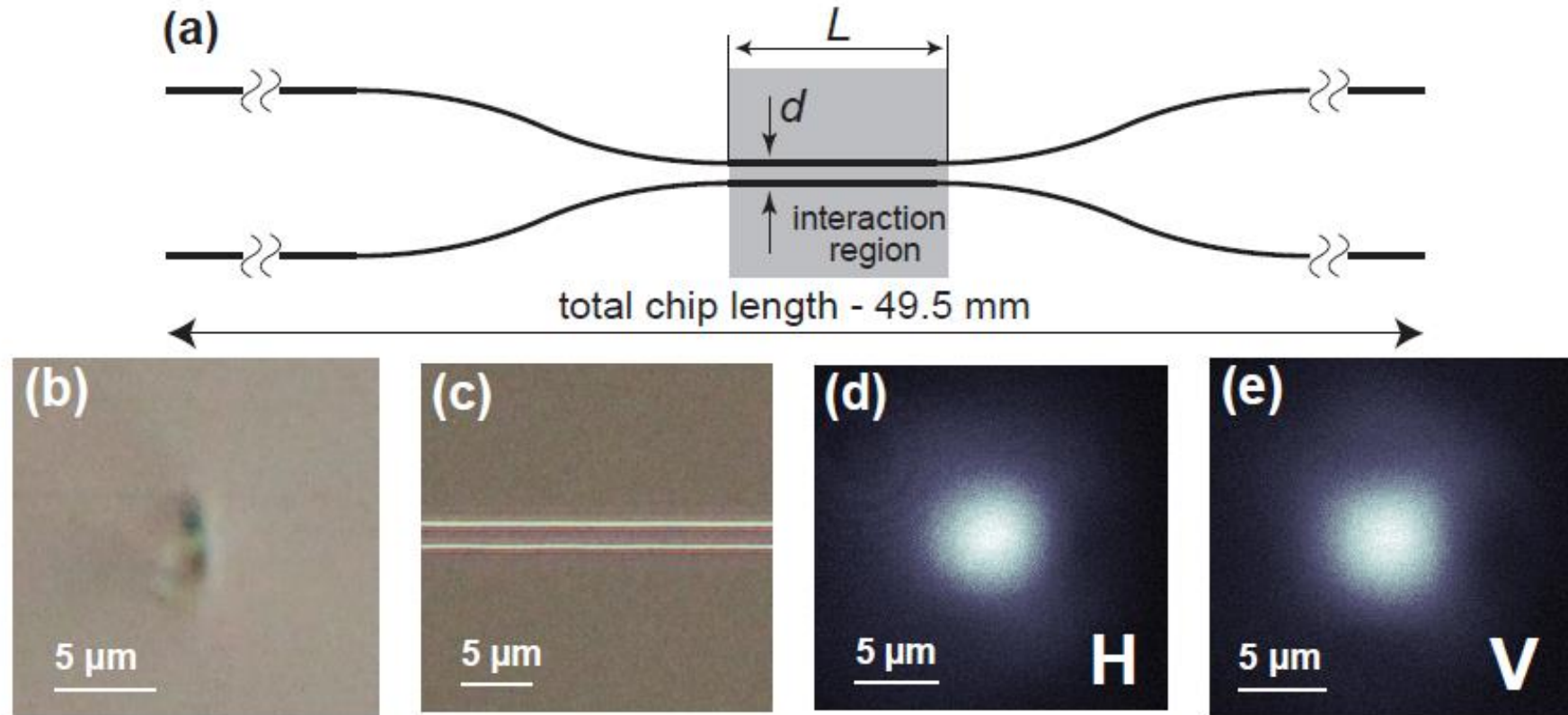
Dual-rail qubit encoding

$$|10\rangle = |0\rangle$$

$$|01\rangle = |1\rangle$$



ВЫЧИСЛЕНИЯ НА ФОТОННЫХ ЧИПАХ: СВЕТОДЕЛИТЕЛЬ

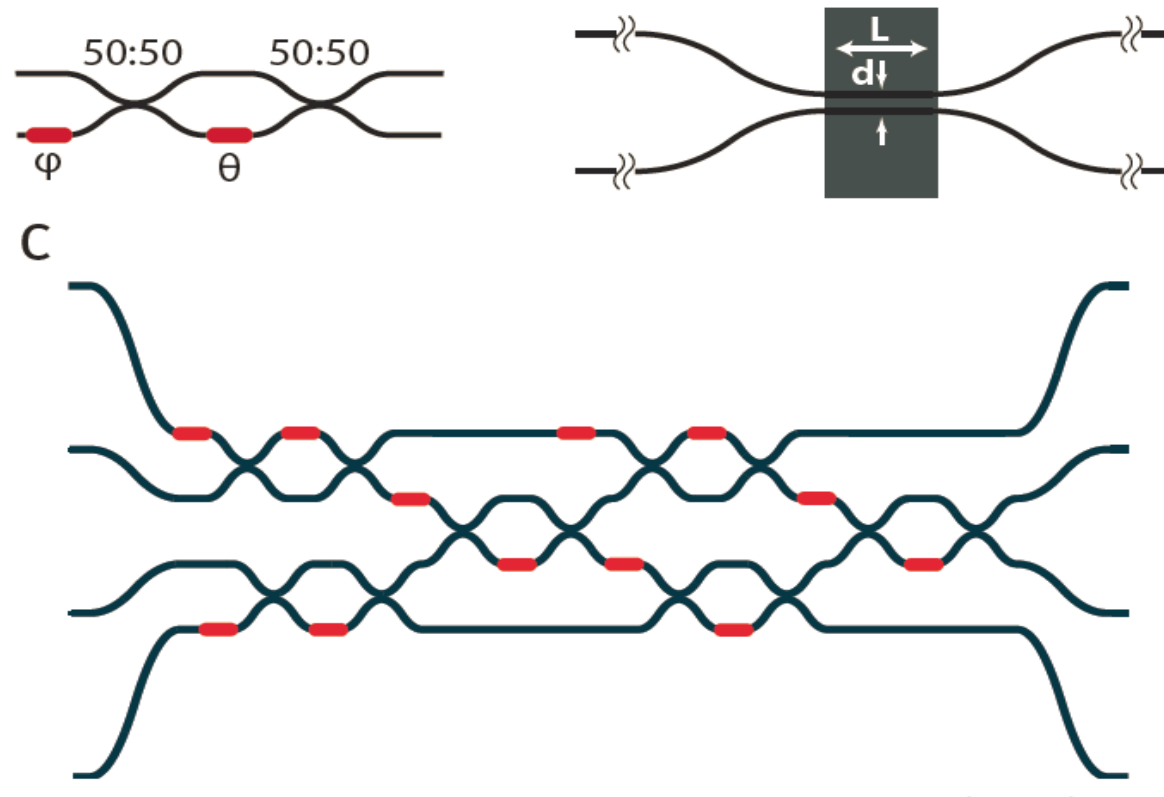


I.V.Dyakonov et al. Opt. Lett. **42**, 4231 (2017)

ВЫЧИСЛЕНИЯ НА ФОТОННЫХ ЧИПАХ: ИНТЕРФЕРОМЕТРЫ



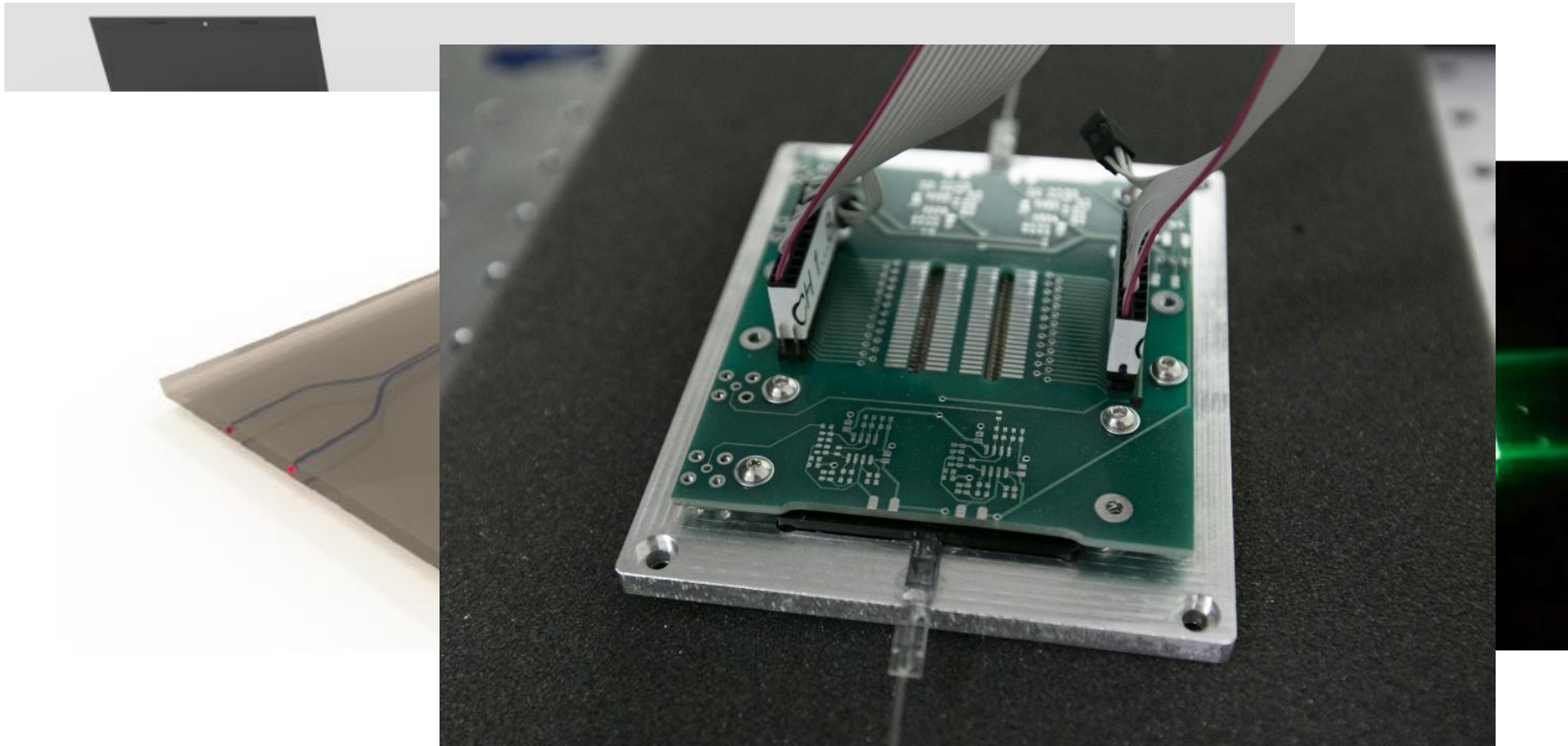
Произвольное преобразование 4X4



ВЫЧИСЛЕНИЯ НА ФОТОННЫХ ЧИПАХ: ПРОГРАММИРУЕМЫЕ СХЕМЫ

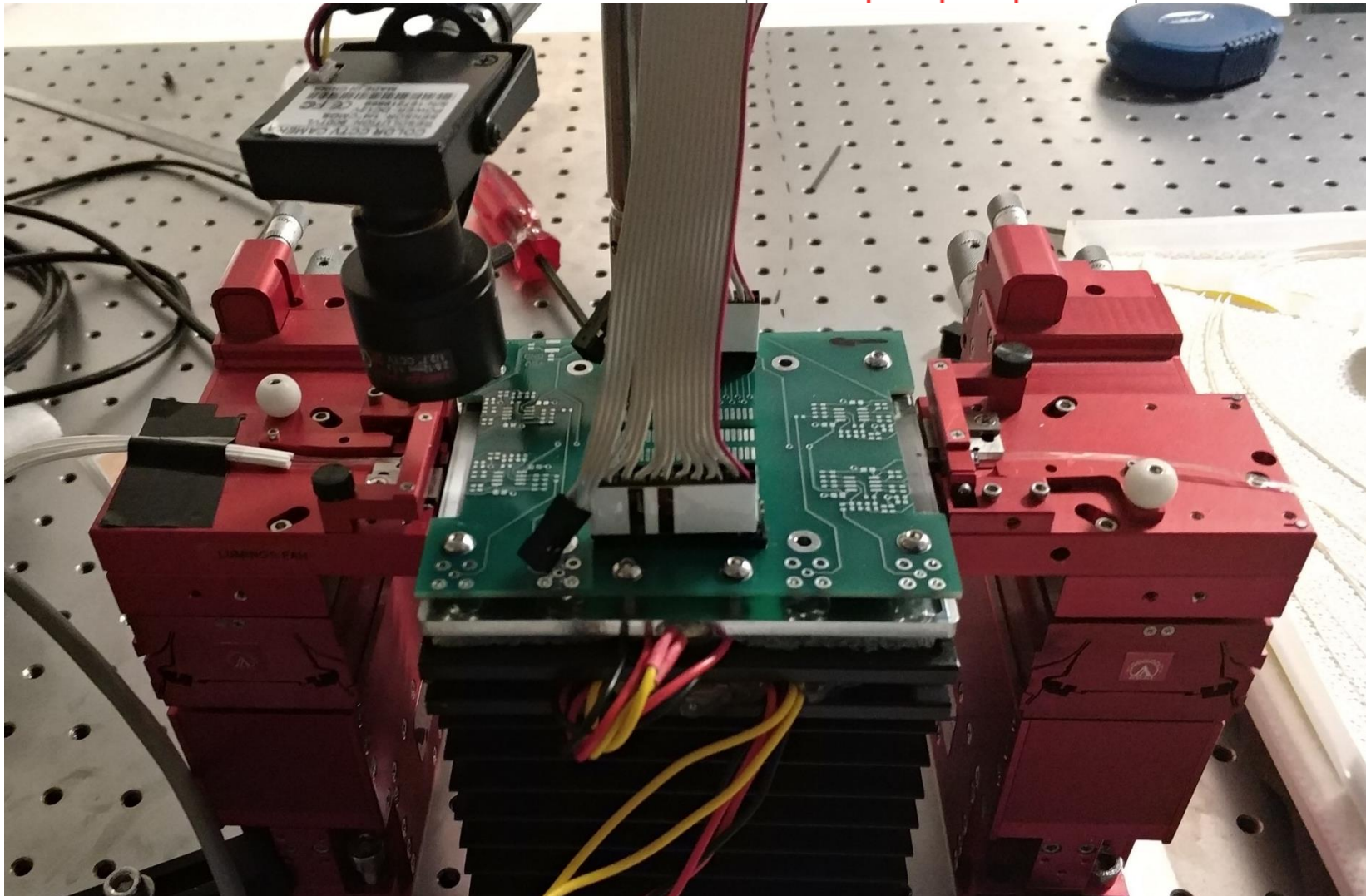


Прототип программируемого оптического чипа – основной элемент линейно-оптического квантового симулятора

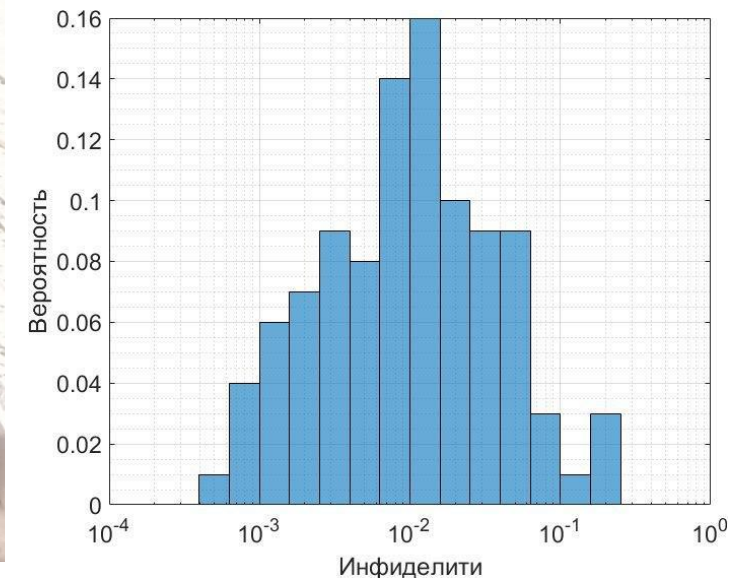


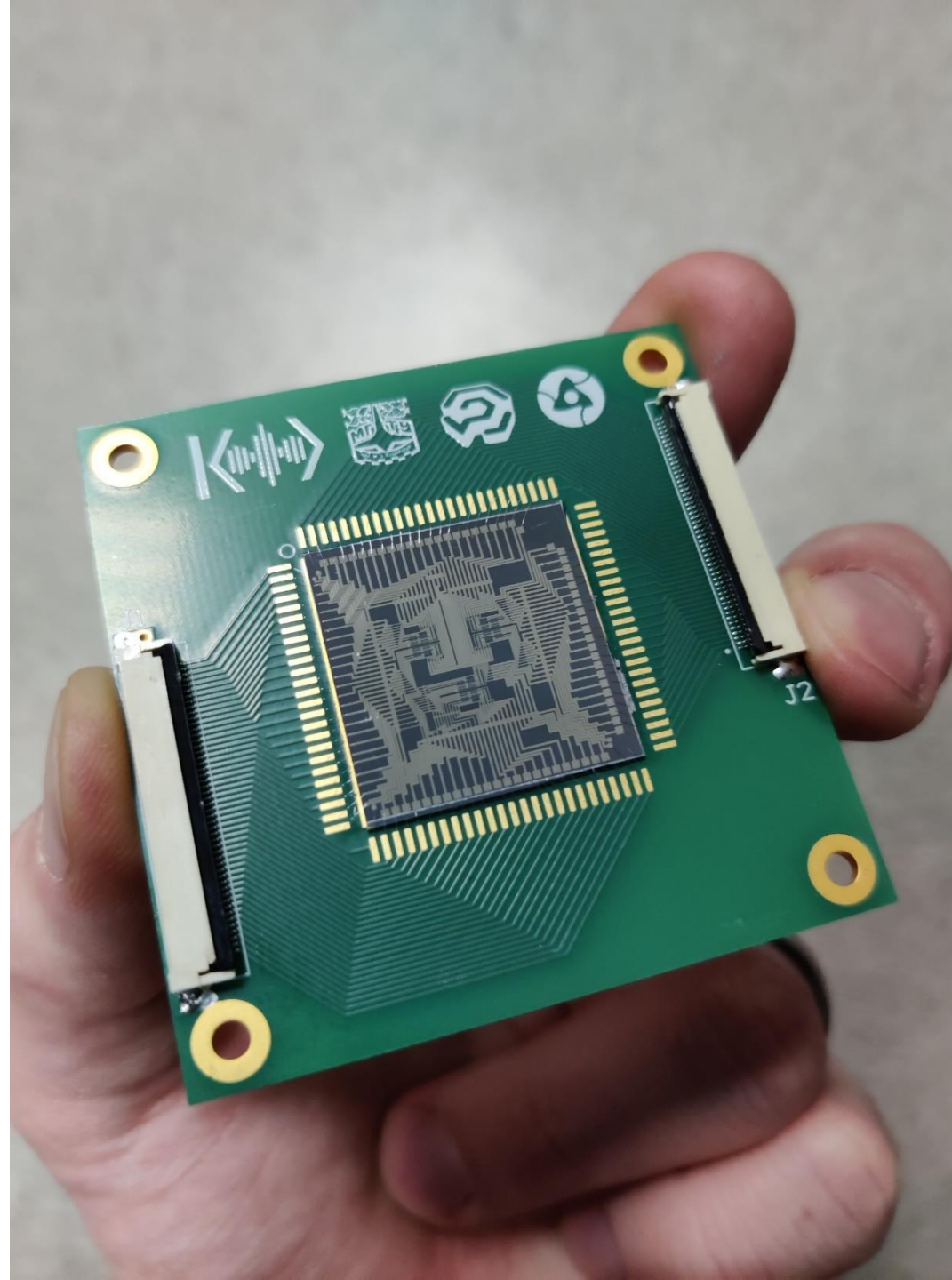
Восьмиканальный программируемый интерферометр (56 термоэлементов)

Сборка реконфигурируемого чипа



Точность реализации
унитарных преобразований 98%





Чип, содержащий 3
двухкубитных
схемы
(однокубитные
гейты +
двухкубитный для
приготовления и
однокубитные
проекторы).
Металл –
титан/аллюминий

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ : ВЫВОДЫ

- Число кубитов и качество логических операций в квантовых вычислителях стабильно растёт
- Квантовое вычислительное превосходство уже продемонстрировано
- Есть основания полагать, что даже небольшие NISQ устройства могут дать преимущество в практически важных задачах
- Квантовые алгоритмы в целом и в приложении оптимизационным задачам в частности – активно развивающаяся область

Волоконно-оптические системы

**ЗАЩИТА ИНФОРМАЦИИ НА
ПРИНЦИПИАЛЬНО ИНОМ
УРОВНЕ**

Квантовые интерфейсы
Квантовая память

Квантовая коммуникация – область науки и техники по передачи информации между удаленными пользователями посредством квантовых состояний

Кто владеет информацией - тот владеет миром!

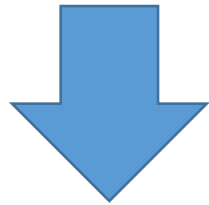
Натан Ротшильд



Уинстон Черчилль

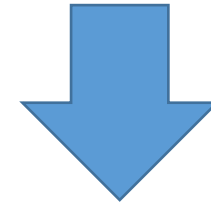


Технологии связи без использования
распределения перепутывания
(*entanglement distribution*)

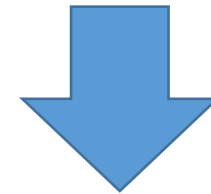


Квантовое распределений ключей
(quantum key distribution)*

Технологии связи с использованием
распределения перепутывания
(*entanglement distribution*)

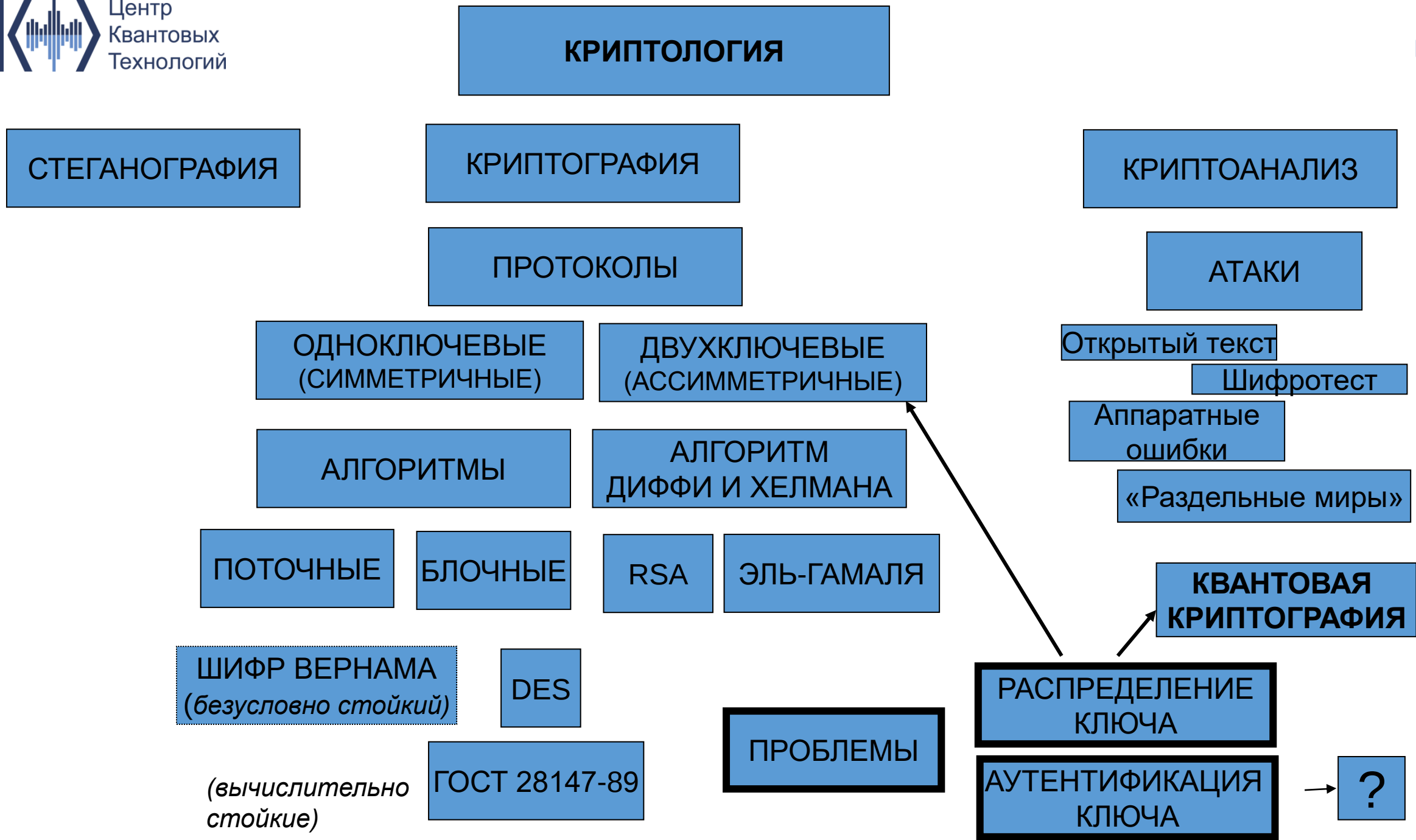


Квантовые сети
(quantum networks)

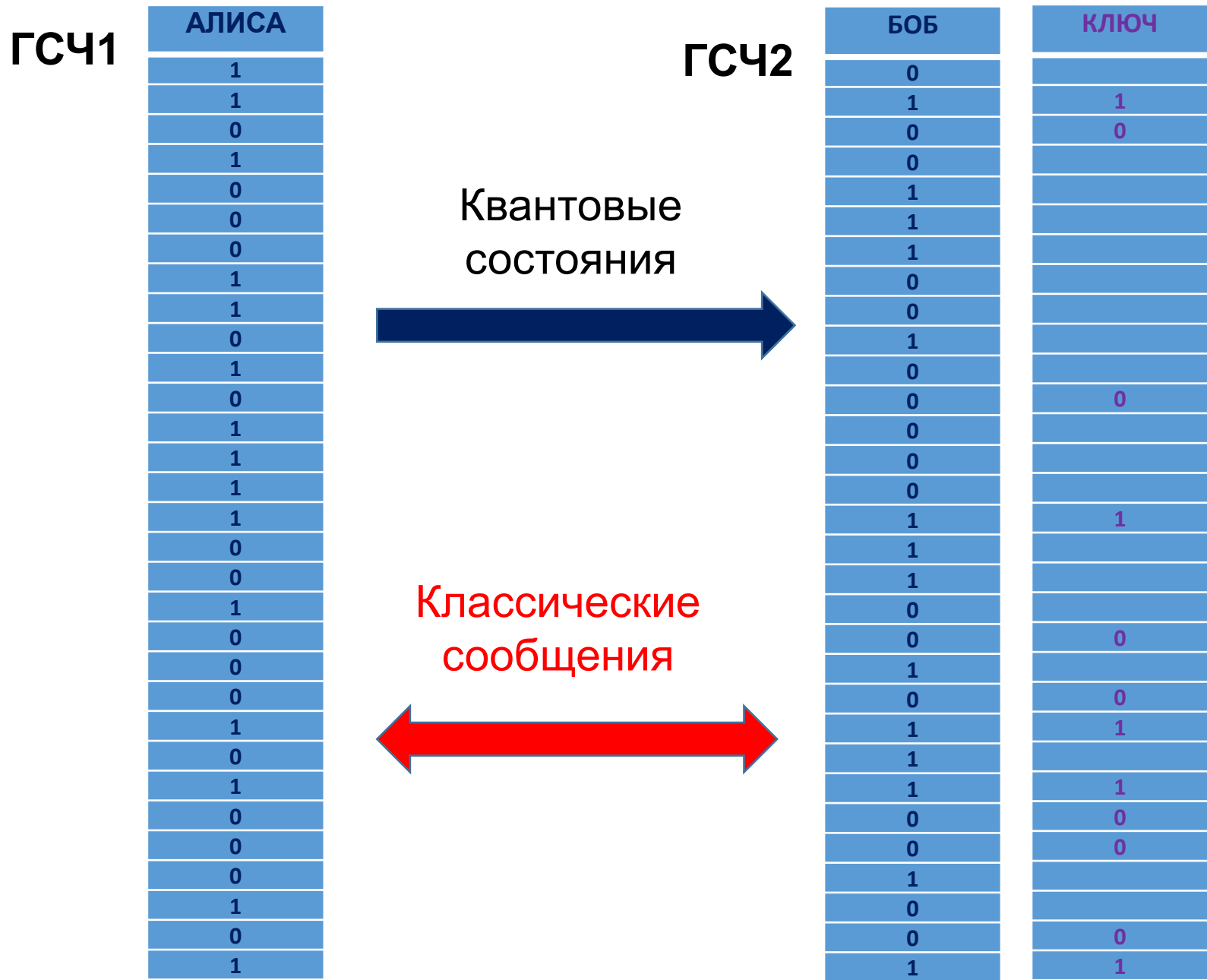


Квантовый интернет
(quantum internet)

***“U.S. Department of Defense’s (DoD’s) Defense Science Board has publicly concluded that “QKD has not been implemented with sufficient capability or security to be deployed for DoD mission use”**
(Defense Science Board, “Applications of Quantum Technologies — Executive Summary,” October 2019.)



ПРИНЦИП ФОРМИРОВАНИЯ КЛЮЧА
В КВАНТОВОЙ КРИПТОГРАФИИ



1. **Носители** информации - фотоны
2. Информация кодируется в **состояниях** фотонов
степенях свободы поля
(фаза, поляризация, момент прихода и проч.)
3. На практике – измерение фотона всегда сопровождается его **уничтожением**.
4. **Принципиально невозможно** измерить неизвестное состояние фотона

КВАНТОВАЯ СВЯЗЬ: ОСНОВНЫЕ НАПРАВЛЕНИЯ МИРОВЫХ РАЗРАБОТОК

1. Волоконно-оптические линии связи:

- шифрование квантовыми ключами данных, передаваемых по магистральным линиям связи;
- создание локальных защищенных сетей с электронным документооборотом;
- создание крупномасштабных сетевых структур через доверенные узлы.

2. Атмосферно-космические каналы связи:

- распределение квантовых ключей между мобильными и стационарными объектами;
- распределение ключей между низкоорбитальными спутниками и наземными объектами;
- распределение ключей между низко- и высокоорбитальными спутниками;
- создание глобальных квантовых сетей, охватывающих значительные территории.

Цель: обмен секретными сообщениями

Схема: сообщение – шифрование – передача – расшифровка - сообщение

Участники:

Алиса и Боб – легитимные пользователи;

Ева — злоумышленник - *осведомлен об используемых криптографических приемах, алгоритмах, протоколах, владеет современными вычислительными ресурсами и пытается скомпрометировать их.*



Принцип Керхгоффа:

стойкость шифра должна быть обеспечена в том случае, когда злоумышленнику известен весь алгоритм шифрования, за исключением секретного ключа

КВАНТОВАЯ КРИПТОГРАФИЯ на кубитах

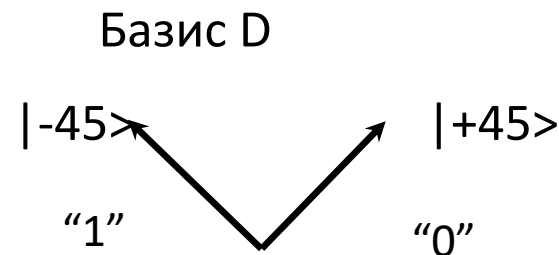
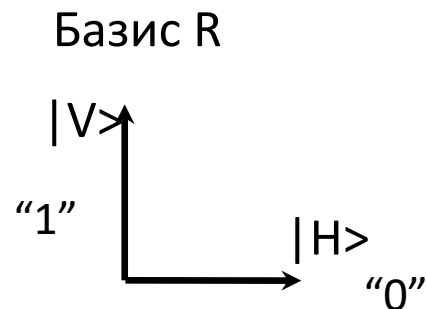


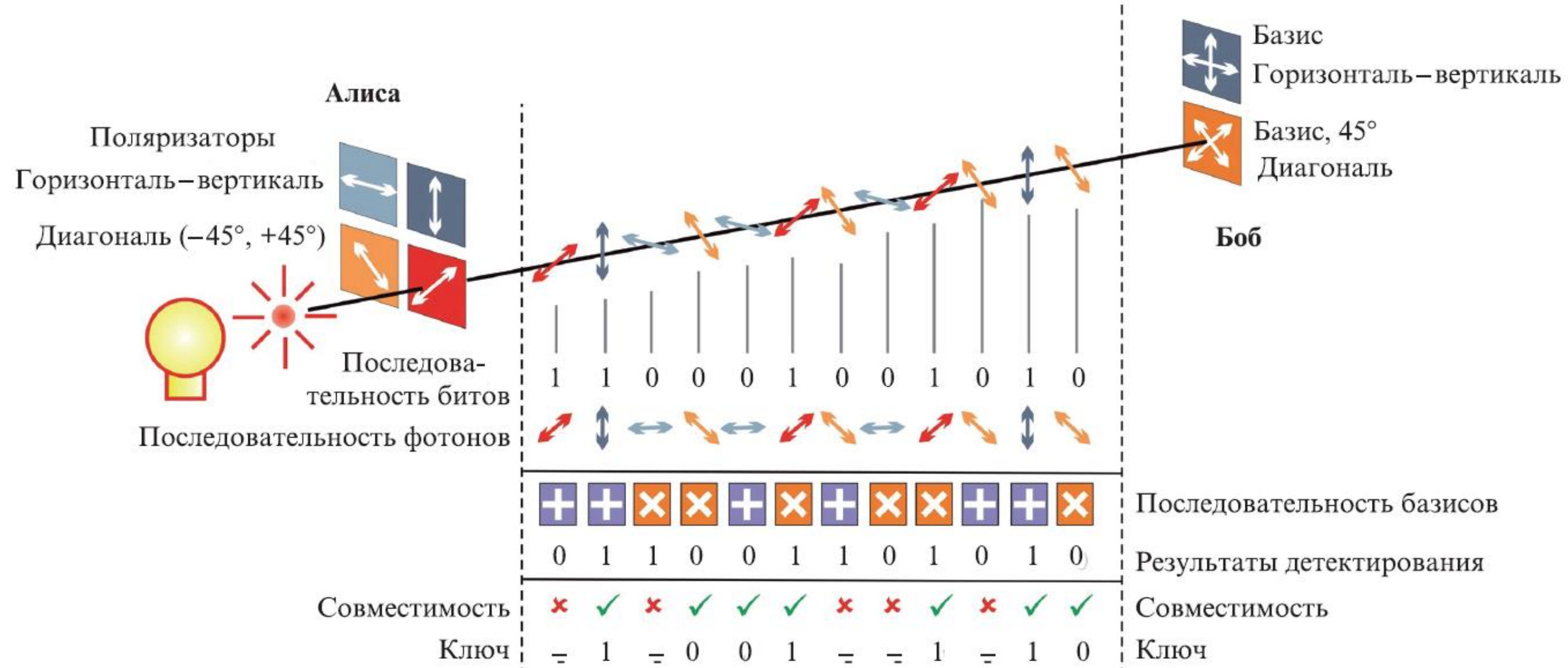
1. Неизвестное квантовое состояние нельзя копировать (no-cloning theorem)
2. Измерение неизвестного состояния вносит возмущение (no-cloning theorem)
3. Случайный выбор из двух неортогональных состояний (базисов)

Взаимно-несмещенные базисы; базис определяется D ортогональными состояниями

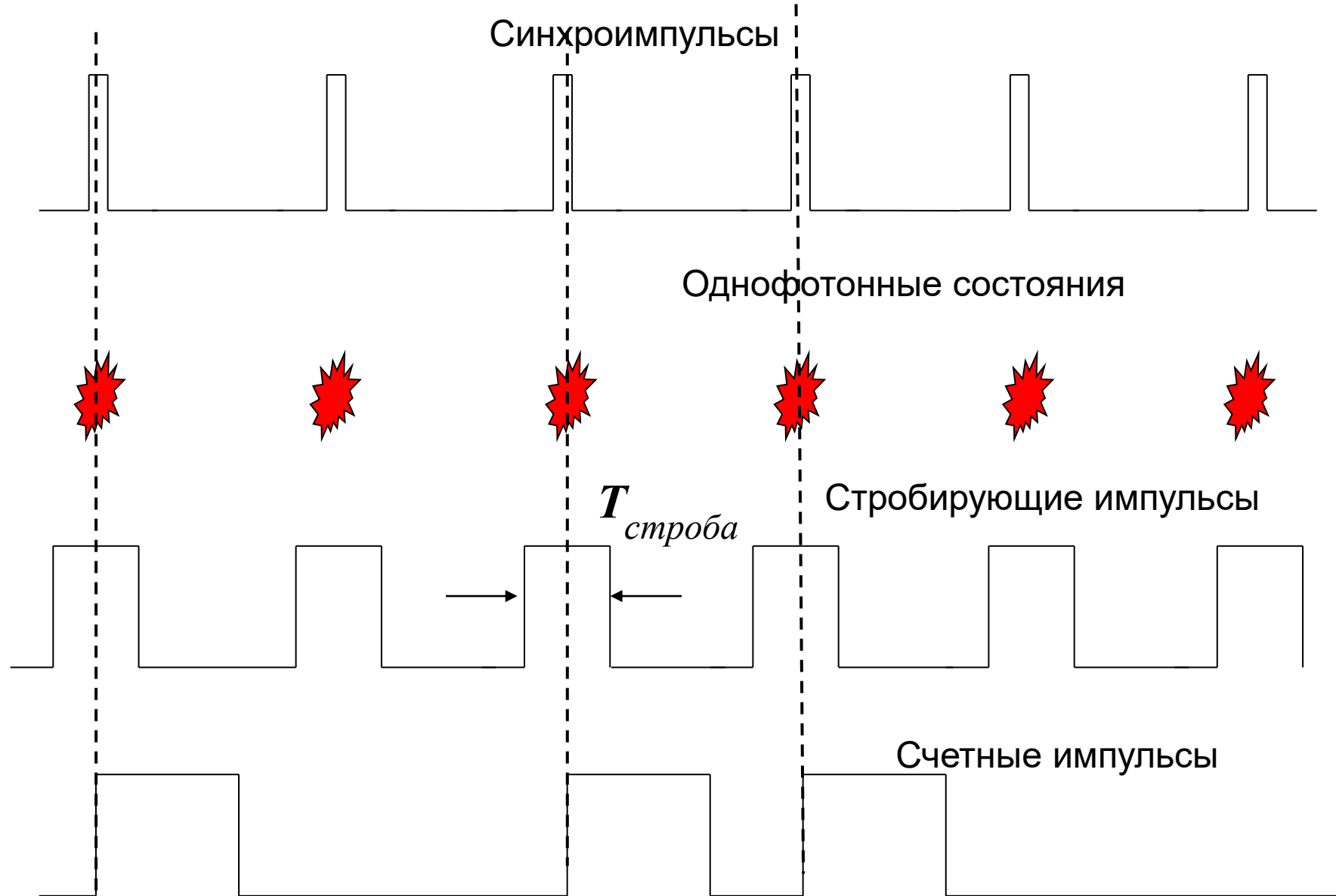
$$\left| \langle e_i | e_j \rangle \right|^2 = \left\{ \begin{array}{ll} 1/D, & \text{если состояния выбраны из разных базисов} \\ 0, & \text{если состояния выбраны из одного базиса} \end{array} \right\}$$

Например, если $D = p^k$, где p простое число, k - целое, то имеется набор **$M = D + 1$** взаимно-несмещенных состояний





ИДЕЯ ОДНОФОТОННОЙ РЕГИСТРАЦИИ В КВАНТОВОЙ КРИПТОГРАФИИ



Лазерное излучение соответствует **когерентному состоянию** или **пуассоновской статистике фотонов**.

Вероятность найти n фотонов при среднем значении числа фотонов μ дается распределением Пуассона:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

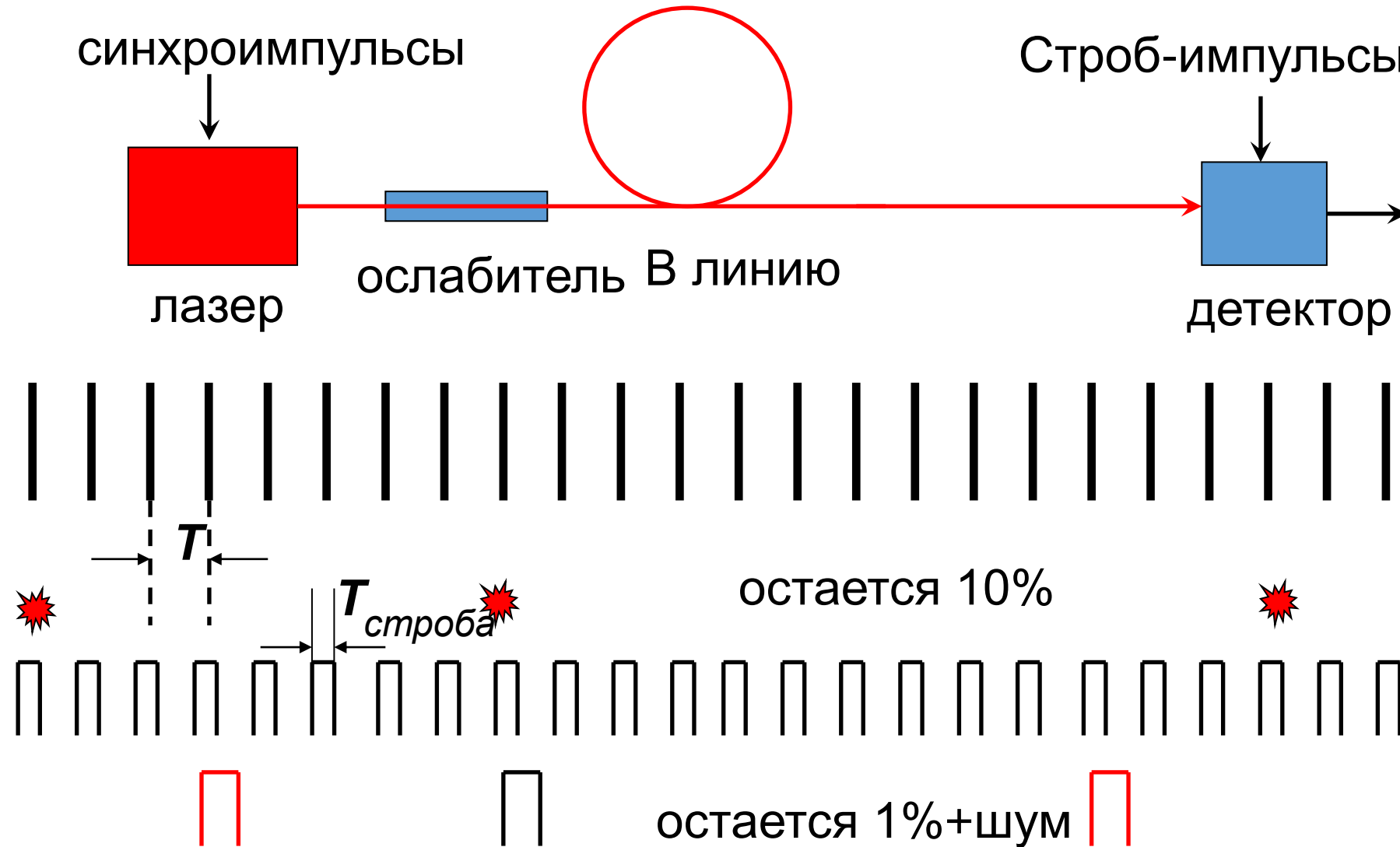
Принято выбирать среднее число фотонов на уровне $\mu = 0.1$, что примерно дает однофотонное состояние на каждый десятый синхроимпульс.

При этом 5% непустых импульсов содержит **> 1 фотона**

Этот уровень оценивается из соотношения:

$$\mu = \frac{W}{\hbar \omega} T_{gate}$$

где W – средняя мощность лазера в непрерывном режиме генерации,
 ω - частота излучения



Проблема – темновые отсчеты однофотонного приемника

КВАНТОВАЯ СВЯЗЬ: ТРИ КРУПНЫХ ПРОЕКТА В МГУ



1. Квантовый шифратор 10G



МОСКВА, 11 апр 2017 — TADVISER.

«На базе технологии, созданной в рамках проекта Фонда перспективных исследований Физический факультет МГУ имени М.В.Ломоносова и ОАО ИнфоТеКС разработают высокопроизводительный шифратор с квантовым каналом распределения криптографических ключей».

2. «Квантовый телефон»



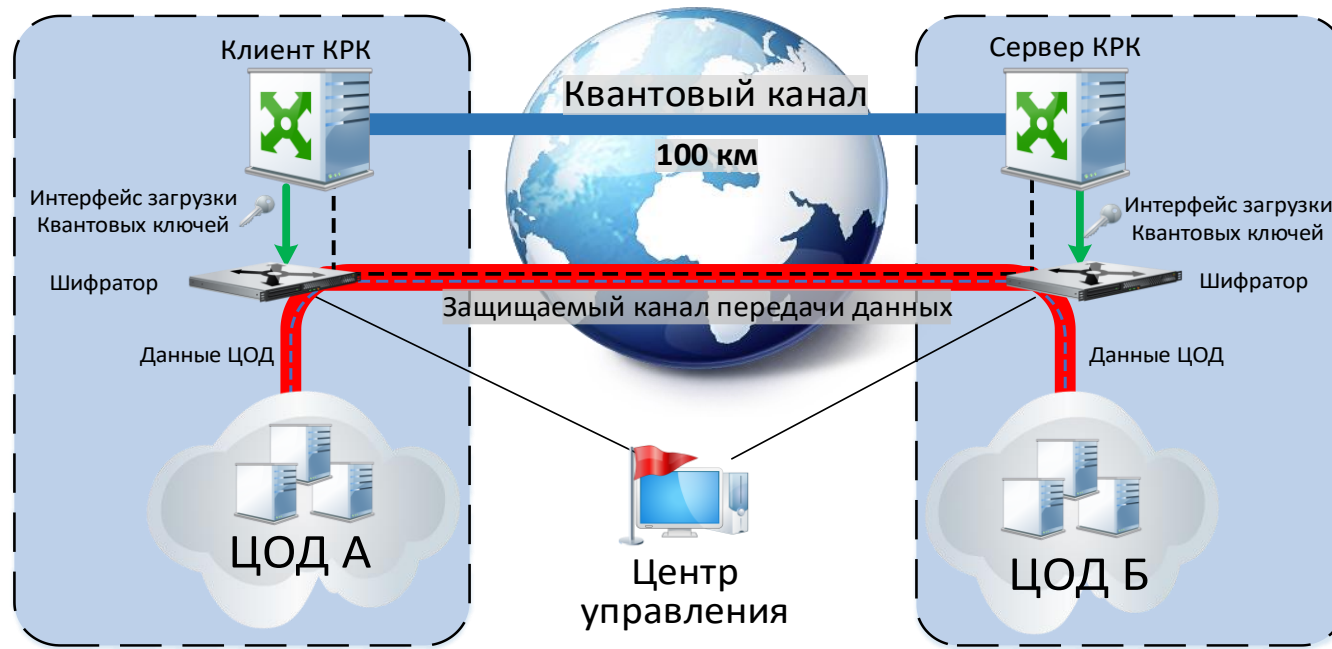
МОСКВА, 13 дек 2017 — РИА Новости.

«Ученые из Московского государственного университета создали и проверили на практике линию телефонной связи, защищенную от прослушивания системой квантового шифрования, сообщает пресс-служба вуза».

3. Квантовая космическая связь

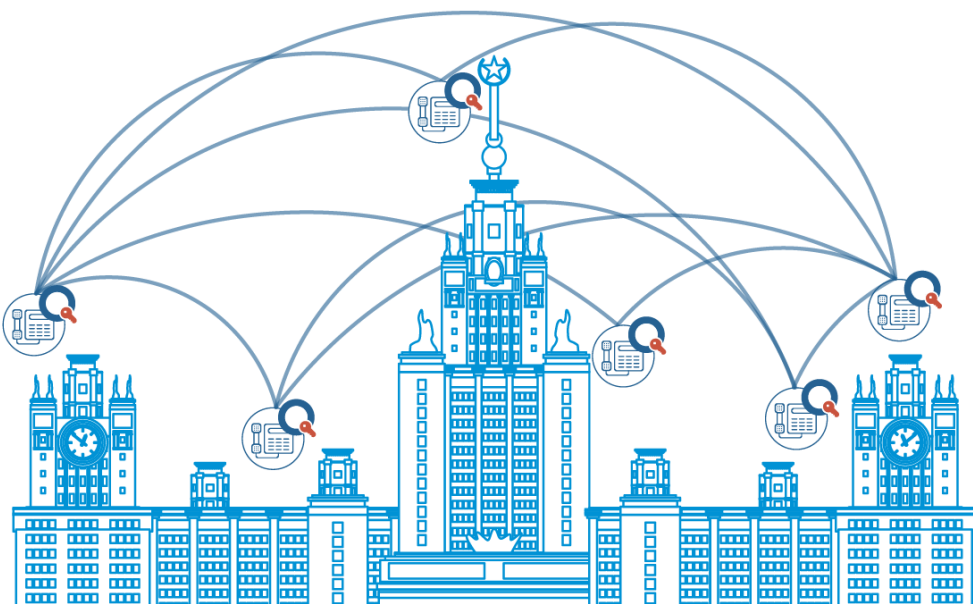
Проект ФТИ «Звезда» - совместно с РКК Энергия, РФЯЦ-ВНИИЭФ (г. Саров)

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 QSS — совместная разработка ИнфоТеКС и Центра квантовых технологий физфака МГУ имени М.В.Ломоносова.

Университетская квантовая сеть:

- Пять квантовых устройств
- Двадцать абонентских терминалов
- Длина каналов квантово-защищенной связи в рамках проекта достигла 50 км
- **Серийное оборудование производства ИнфоТеКС**
- Перспектива интеграции с магистральными сетями

МЕЖУНИВЕРСИТЕТСКАЯ КВАНТОВАЯ СЕТЬ (МУКС)

Курчатовский научный Центр, Иннопрактика, Министерство образования и науки: Консорциум



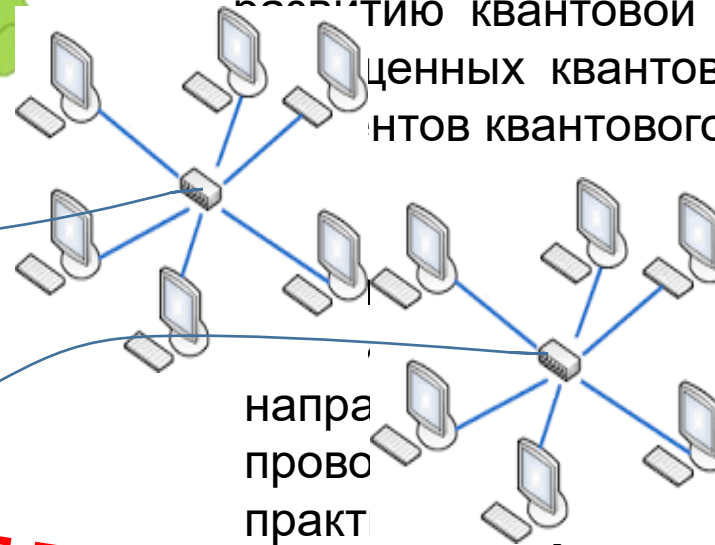
Иннопрактика



МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ И ЭКСПЛУАТАЦИИ МУКС:

- образовательные и научные проекты по развитию квантовой сети для передачи данных, ценных квантовыми ключами и разработке протоколов квантового интернета;



- пилотных проектов - инструмент апробации перспективных технологий квантовых коммуникаций, являющихся в рамках подготовки к запуску оборудования КРК и продвижения концепции квантового интернета;

Томск

- стартапы в рамках программы технологического предпринимательства.



КВАНТОВАЯ АТМОСФЕРНАЯ СВЯЗЬ: ПРОЕКТЫ

Распределение ключей между стационарным объектом (Ш) и мобильными летательными аппаратами (К1, К2, К3...) через мобильный летательный аппарат (К).

ПРОТОКОЛ: на перепутанных парах фотонов
Расстояние до 100 м (проект 2019-2020гг)



РОССИЙСКИЕ КОМПАНИИ-ВЕНДОРЫ В ОБЛАСТИ КВАНТОВОЙ СВЯЗИ



<https://infotecs.ru/>



<https://goqrates.com/>



СМАРТС
КВАНТТЕЛЕКОМ

<https://quanttelecom.ru/>



Сертифицированный продукт(ы)



Имеется Заключение Регулятора

СХЕМА ПРОВЕДЕНИЯ КОСМИЧЕСКОГО ЭКСПЕРИМЕНТА

Квантовый канал КРК $\lambda = 852 \text{ нм}$

Служебный канал КРК $\lambda = 1550 \text{ нм}$

Канал треккинга, маяки,
идентификация:
 $\lambda = 808 \text{ нм}$

Пассивные бортовые маяки
 $\lambda = 630 \text{ нм}$

Космический аппарат

квантовый канал

квантовый канал

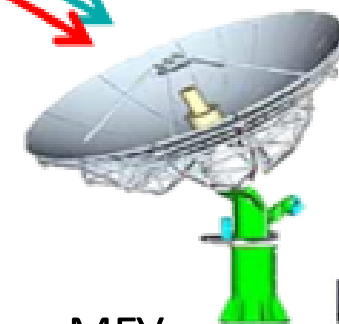
Высота орбиты ~ 600 км

расстояние ~ 1400 км

канал передачи данных



Экспериментальное кольцо ВНИИЖТ
г. Москва



Кавказская горная обсерватория МГУ
г. Кисловодск

Технические характеристики

Наименование параметра

Значение параметра

Длина секретного квантового ключа, сформированного из данных, полученных за один сеанс квантовой связи, не менее

256 бит

Типоразмер космического аппарата класса «Cubesat», не более

16U

Параметры ЭО БТ

- типоразмер, не более

11U

- масса, не более

17 кг

- энергопотребление, не более

100 Вт

Диаметр апертуры телескопа в составе наземного терминала, не менее

От 1 м до 1,2 м

Расстояние между ЭО НТ и ЭО БТ

- в случае расположения ЭО НТ в надир по отношению к ЭО БТ

не менее 500 км

- при организации каналов связи на наклонных трассах

до 1000 км и более

Функционирование платформы

солнечно-синхронная орбита, 600±100 км

Параметры квантового канала связи

- тактовая частота следования импульсов излучения, не менее

10 МГц

- расходимость излучения квантового канала связи, не более

15 мкрад

- квантово-криптографический протокол (в том числе среднее число фотонов в импульсе, длина волны и длительность оптических импульсов)

определяется на этапе проведения специальных исследований

Срок службы КА на орбите, не менее

3 года

**Системы, разработанные и созданные в МГУ
содержат все требуемые составляющие:**

- 1) Поддержка автоматического режима работы без участия оператора.**
- 2) Физический генератор (квантовый) истинно случайных последовательностей.**
- 2) Протоколы с доказуемой криптографической стойкостью.**
- 3) Исправление ошибок в первичных ключах.**
- 4) Сжатие очищенных ключей – усиление секретности универсальными хеш-функциями.**
- 5) Конечный продукт работы – общий секретный ключ.**

КВАНТОВЫЕ СЕНСОРЫ: ОБЗОР ТЕХНОЛОГИИ



Что это?	Квантовые сенсоры - это высокоточные инструменты, основанные на квантовых системах.
Зачем?	Предполагается, что квантовые сенсоры будут иметь характеристики намного превышающие имеющиеся у классических аналогов
Основные характеристики	Чувствительность (минимальное значение регистрируемого сигнала), пространственное и временное разрешение, рабочий диапазон измеряемых значений, время отклика или анализа, относительная воспроизводимость (например, частоты в стандартах времени), энергопотребление, габариты, сложность обслуживания, срок службы, стоимость производства и эксплуатации
Решение проблемы	Использование квантовых технологий
Инструментарий	Квантовые состояния света и вещества: взаимодействие между ними. Суперпозиции, запутывание и квантовые измерения.
Где и кому это нужно	ГЕОЛОГОРАЗВЕДКА, МЕДИЦИНА, НАВИГАЦИЯ И ТРАНСПОРТ и др.



СПЕЦИФИЧЕСКИЕ СВОЙСТВА КВАНТОВЫХ СОСТОЯНИЙ



основа для использования их при построении чувствительных сенсоров.

Квантовый объект – кубит – **зонд** для измерения физических свойств взаимодействующих систем.

СУПЕРПОЗИЦИИ

(квантовая когерентность):
волновые функции квантовых
объектов представляют собой
линейную комбинацию базисных
состояний

$$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle$$

ЗАПУТЫВАНИЕ:

квантовое состояние составной
системы определено лучше, чем
состояния подсистем

$$|\Psi_{12}\rangle = \frac{1}{\sqrt{2}} \{ |0_1\rangle|1_2\rangle + |1_1\rangle|0_2\rangle \}$$

ИЗМЕРЕНИЕ:

измерение приводит к
вероятностным исходам
классических состояний

$$p_m = \langle \Psi | M_m^\dagger M_m | \Psi \rangle.$$

$$E_m = M_m^\dagger M_m, \quad \sum_m E_m = I$$

ПРИМЕНЕНИЕ: ГЕОЛОГОРАЗВЕДКА, МЕДИЦИНА, НАВИГАЦИЯ И ТРАНСПОРТ и др.

ОПРЕДЕЛЕНИЯ КВАНТОВЫХ СЕНСОРОВ

I. Использование квантового объекта (зонда) для измерения физической величины (классической или квантовой). Квантовый объект характеризуется квантованной структурой энергетических уровней – электронные, магнитные, колебательные состояния сверхпроводящих или спиновых кубитов, нейтральных атомов или ионов.

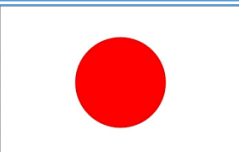


II. Использование квантовой когерентности (например, в виде пространственной или временной суперпозиции) для измерения физической величины.

III. Использование свойства запутанности для улучшения чувствительности измерений, т.е. с более высокой точностью/чувствительностью, чем это имеет место при классических измерениях.

КРИТЕРИИ ПРИМЕНИМОСТИ КВАНТОВОЙ СИСТЕМЫ КАК СЕНСОРА

1. Квантовая система имеет дискретные уровни энергии. В частности - двухуровневая система (или ансамбль двухуровневых систем) с нижним и верхним уровнями $|0\rangle$ и $|1\rangle$, разделенных энергией перехода $E = \hbar\omega$
2. Должна иметься возможность приготовления (инициализации) квантовой системы в известных состояниях и выполнения операции считывания (измерения) этих состояний.
3. Квантовой системой можно когерентно манипулировать - обычно с помощью полей, зависящих от времени. Это условие не является строго обязательным для всех протоколов; примеры, выходящие за рамки этого критерия - измерение времен релаксации.
4. Квантовая система взаимодействует с соответствующей физическим объектом $V(t)$, например электрическим или магнитным полем. Взаимодействие количественно оценивается параметром вида $\gamma = \partial^q E / \partial V^q$, который связывает изменения энергии перехода E_k с изменением внешнего параметра $V(t)$. В большинстве ситуаций связь либо линейная ($q = 1$), либо квадратичная ($q = 2$). Взаимодействие с $V(t)$ приводит к сдвигу энергетических уровней квантовой системы.

Страна		Объем затрат на исследования и разработки
Европейский союз		~37 млн евро/44 млн долл. (2018-2021): Integrated Quantum Clock, MetaboliQs, macQsimal, ASTERIQS
Канада		50 млн долл. (2014-2020): Quantum Photonics Sensing and Security (QPSS) R&D program
Германия		530 млн долл./450 млн евро (2021-2030)
Франция		250 млн евро/294,4 млн долл. (2021-2025)
Великобритания		94 млн фунтов стерлингов/110,9 млн долл. (2019-2024)
США		11 млн долл. (2021-2023)
Китай		0,15 млн долл. (2015)
Япония		200 млн долл. (2018-2030)

ПУБЛИКАЦИИ: РЕЙТИНГ СТРАН 2018-2020



Рейтинг стран по числу публикаций в научных журналах, индексируемых в Scopus в 2018-2020 гг. по ВТН «Квантовые сенсоры», ед.
Источник: НИУ ВШЭ, 2021.

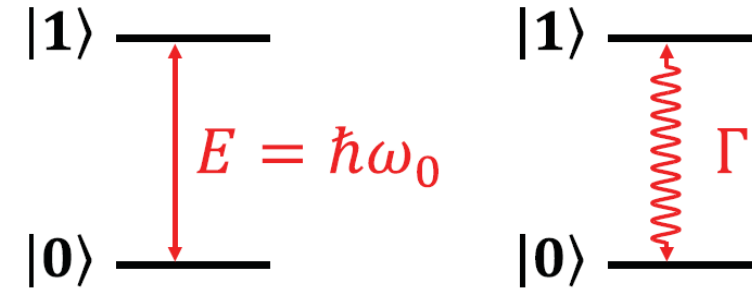
Физическая система/тип	Кубит	Измеряемая величина	Хар. частота	Инициализация	Чтение
Нейтральные атомы					
Атомный пар II-III	Атомный спин	Магнитное полое, Вращение, Частота/Время	DC-10ГГц	Оптическая	Оптическое
Холодные атомы II-III	Атомный спин	Магнитное полое, Ускорение, Частота/Время	DC-10ГГц	Оптическая	Оптическое
Ионы в ловушках					
II-III	Долгоживущее электронное состояние, Колебательная мода	Электрическое полое, Сила, Вращение, Частота/Время	МГц	Оптическая	Оптическое
			ТГц	Оптическая	Оптическая
Ридберговские атомы					
II-III	Ридберговские состояния	Электрическое поле	DC, ГГц	Оптическая	Оптическое
Твердотельные спины (ансамбли)					
ЯМР-сенсоры II	Ядерный спин	Магнитное поле	DC	Температурная	Pick-up coil
NV-сенсоры (ансамбли) II	Электронный спин	Магнитное поле, Электрическое поле, Температура, Давление, Вращение	DC-ГГц	Оптическая	Оптическое
Твердотельные спины (одиночные спины)					
P донор в Si II	Электронный спин	Магнитное поле	DC-ГГц	Термическая	Электрическая
Полупроводниковые квантовые точки I-II	Электронный спин	Магнитное поле	DC-ГГц	Электрическая, Оптико-электрическая, Оптическая	
Одиночный NV-центр II	Электронный спин	Магнитное полое, Электрическое поле, Температура, Давление, Вращение	DC-ГГц	Оптическая	Оптическое
Сверхпроводящие цепи					
SQUID I-II	Ток сверхпроводимости	Магнитное поле	DC-10ГГц	Термическая	Электрическая
Потоковый кубит II	Циркуляционный ток	Магнитное поле	DC-10ГГц	Термическая	Электрическая
Зарядовый кубит II	Зарядовые соб. состояния	Магнитное поле	DC-10ГГц	Термическая	Электрическое
Элементарные частицы					
Мюон II	Мюонный спин	Магнитное поле	DC	Радиоактивный распад	Радиоактивный распад
Нейтрон II	Ядерный спин	Магнитное поле, Гравитация	DC	Брэгговское рассеяние	Брэгговское рассеяние
Другие сенсоры					
Одноэлектронный транзистор I	Зарядовые соб. состояния	Электрическое поле	DC-100 МГц	Термическая	Электрическое
Оптомеханика I	Фононы	Сила, ускорение, Масса, Магнитное поле	кГц-МГц	Термическая	Оптическое
Интерферометр II-III	Фотоны, Атомы, Молекулы	Смещение, Показатель преломления			

«Внутренняя чувствительность» $\propto \frac{1}{\gamma \sqrt{T_\chi}}$

- минимальный регистрируемый
сигнал в единицу времени

γ - параметр взаимодействия;

T_χ - время релаксации системы

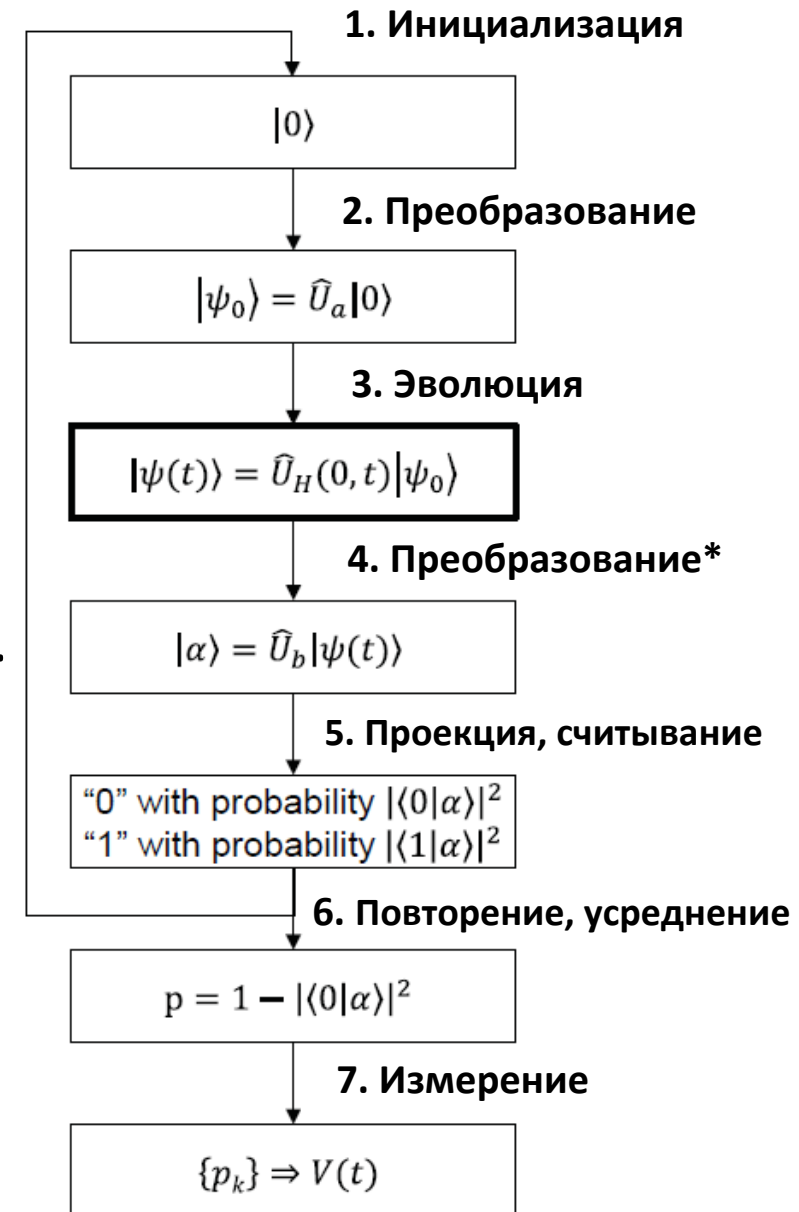


Сенсор основан на изменении или
энергии E , либо скорости Γ перехода

Для оптимизации чувствительности необходимо, чтобы параметр γ был достаточно большим (например путем выбора соответствующей физической системы в качестве сенсора), а время релаксации T_χ – достаточно долгим.

ПРОТОКОЛ РАБОТЫ КВАНТОВОГО СЕНСОРА

1. Инициализация в известном базисном состоянии $|0\rangle$
2. Преобразование к желаемому начальному состоянию $|\psi_0\rangle$
3. Эволюция под действием гамильтониана за время t .
$$|\psi(t)\rangle = \hat{U}_H(0, t)|\psi_0\rangle = c_0|\psi_0\rangle + c_1|\psi_1\rangle$$
4. Преобразование в суперпозицию наблюдаемых состояний.
$$|\alpha\rangle = \hat{U}_b|\psi(t)\rangle = c'_0|0'\rangle + c'_1|1'\rangle$$
5. Чтение (измерение) конечного состояния (POVM) по схеме Бернулли p' и $1-p'$.
6. Повторение циклов в 1-5 N раз для оценки вероятности p .
7. Измерение вероятности перехода p как функции времени для оценки величины сигнала V .



ПЕРЕЧЕНЬ/ГРУППЫ СЕНСОРОВ

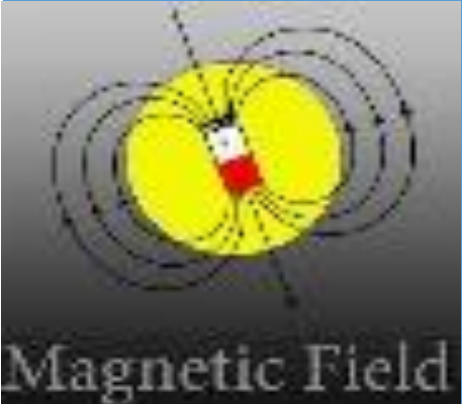


Группа сенсоров	сенсоры	Оценка ГОТОВНОСТИ
Часы, гравиметры, градиометры 	Атомный гравиметр 	2023
	Атомный градиометр	2024
	Компактный гироскоп	2024
	Компактная универсальная ультрастабильная лазерная система для опроса оптических стандартов частоты	2022
	Мобильный волоконный фемтосекундный синтезатор оптических частот	2022
	Малогабаритный квантовый стандарт частоты	2022
	Компактные атомные часы 	2021

 - НИР на 2020 год

ПЕРЕЧЕНЬ/ГРУППЫ СЕНСОРОВ



Группа сенсоров	Сенсоры	Оценка ГОТОВНОСТИ
Сенсоры электрического и магнитного поля 	Квантовые биосенсоры, работающие на квантовом уровне чувствительности	2022
	Квантовый магнитометр	2022
	Локальный сенсор электрического поля	2020
	Локальный сенсор химических реакций ⚡	2022
	Локальный зонд магнитного поля для биоманитных измерений	2021

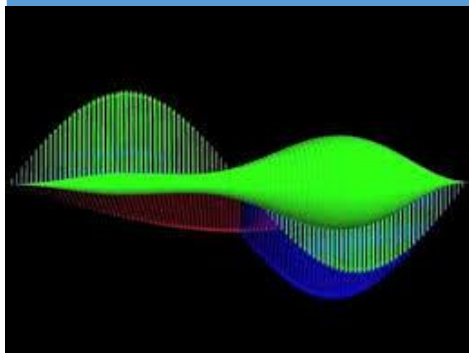


- НИР на 2020 год

ПЕРЕЧЕНЬ/ГРУППЫ СЕНСОРОВ



Группа сенсоров	Сенсоры	Оценка ГОТОВНОСТИ
Квантовая метрология	Генератор случайных чисел	2021
	Полупроводниковый счетчик фотонов в ближнем ИК-диапазоне	2023
	Однофотонный детектор видимого и ближнего ИК-диапазонов	2023
	Матричный фотоэлектронный умножитель	2022
	Безэталонный измеритель квантовой эффективности фотодетекторов	2022
	Маркерный сенсор на квантовых точках для диагностики биологических, вирусных и бактериальных элементов	2021
	Маркерный сенсор на квантовых точках для обнаружения химических и особо опасных веществ	2022

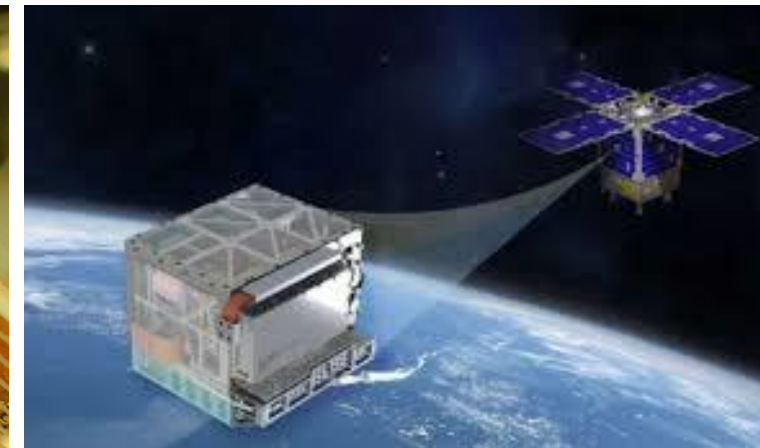
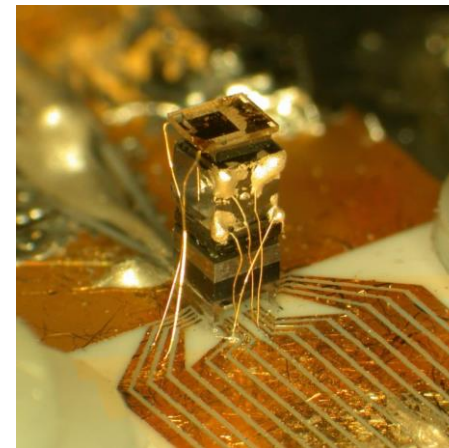


- НИР на 2020 год

Характеристики	Единицы	2020	2021	2022	2023	2024	2030
Кратковременная нестабильность частоты, за 1 сек	Ед.	Разработка	Разработка	3×10^{-11}	1.2×10^{-11}	8×10^{-12}	1×10^{-12}
Долговременная нестабильность частоты, за 1 сутки	Ед.			5×10^{-12}	1×10^{-12}	5×10^{-13}	1×10^{-13}
Объем	см ³			60	50	40	15

Применение: **НАВИГАЦИЯ**

- навигационные приемники;
- базовые станции систем дифференциальной коррекции и др.

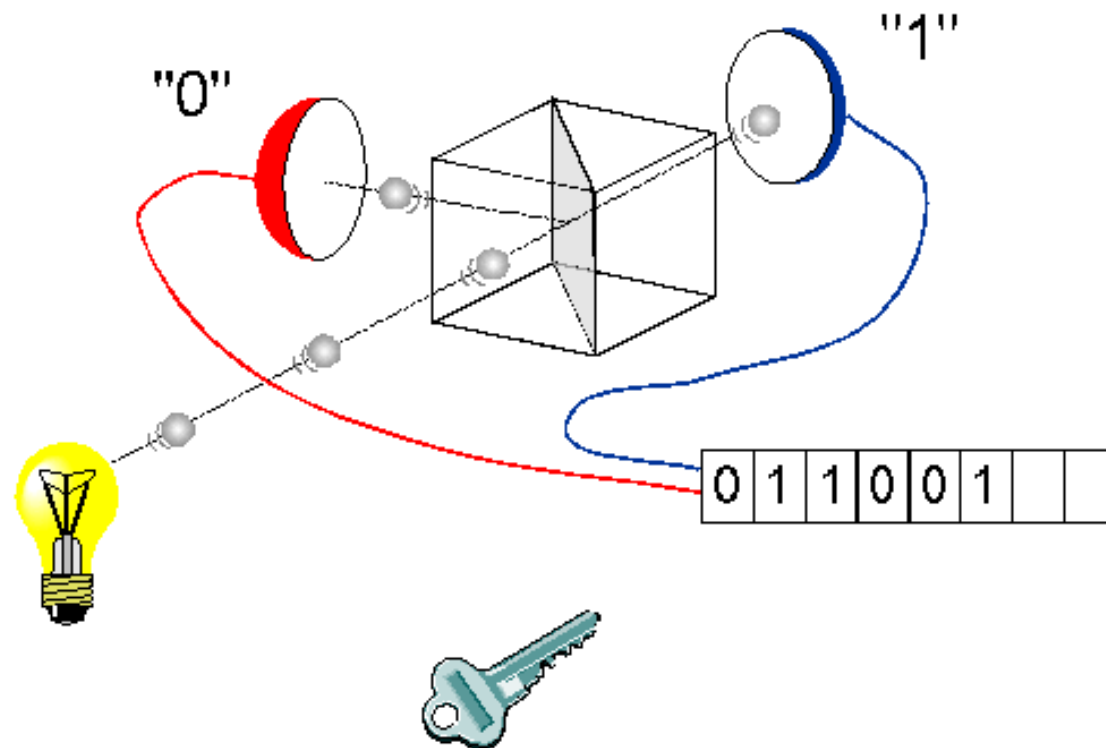


Характеристики	Единицы	2020	2021	2022	2023	2024	2030
Скорость генерации случайных чисел	Мб/с	200	300	1000	1000	1000	10 000
Габаритные размеры	см ³	25	20	20	20	20	20

Применение: **КРИПТОГРАФИЯ**

для использования в классических и квантовых
системах шифрования





Принцип действия генератора:

- детектирование ослабленного света однофотонным приемником;
- устранение корреляций, вызванных инертностью детектора;
- обработка полученной пуассоновской статистики;
- экстракция несмещенной последовательности независимых битов.

Основные требования к квантовому генератору случайных чисел:

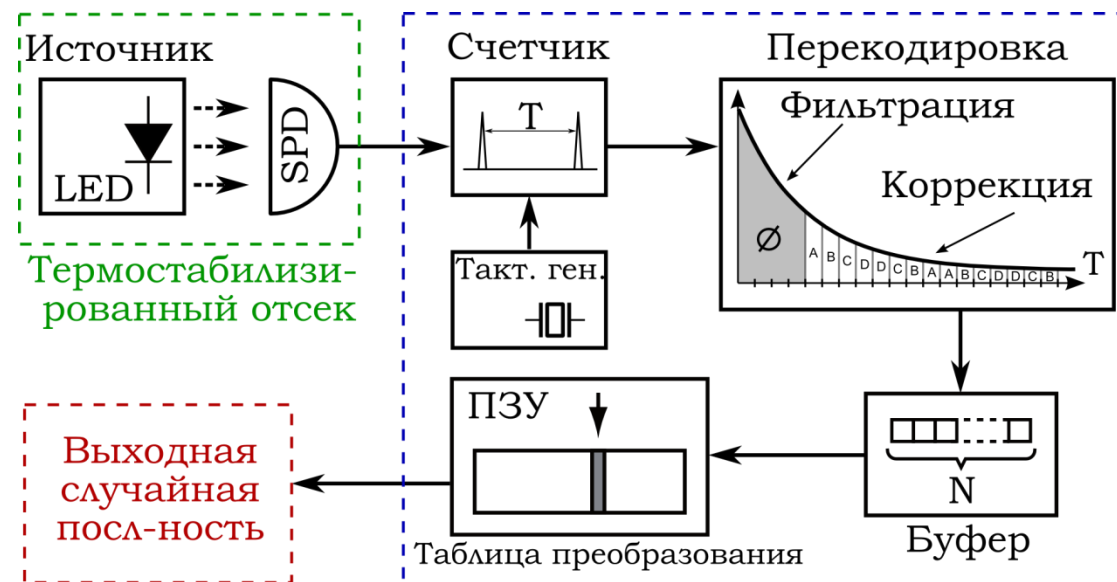
- использование случайных процессов квантовой природы;
- детерминистический алгоритм экстракции, гарантирующий независимость/несмещенность выходных значений;
- использование матрицы однофотонных детекторов повышения скорости генерации и надежности;
- простота реализации;
- компактное исполнение с использованием доступных компонентов (SiPM – заложен в Дорожной карте).

Источниками случайности являются:

- пуассоновская статистика когерентного излучения;
- процесс детектирования отдельных фотонов в непрерывном потоке света.

Измеряется длительность временных интервалов между зарегистрированными фотонами – это случайная величина, распределенная по экспоненциальному закону. Полученная последовательность преобразуется в строку случайных битов.

Блок-схема генератора (до 200 Мб/с):



ПЛИС и флеш-память на 2МБайт

ПОЛУПРОВОДНИКОВЫЙ ЛАВИННЫЙ ФОТОДЕТЕКТОР (СЧЕТЧИК ФОТОНОВ) В БЛИЖНЕМ ИК-ДИАПАЗОНЕ

Характеристики	Единицы	2020	2021	2022	2023	2024	2030
Спектральный диапазон	нм	1300-1550	1300-1550	1300-1550	1300-1550	1300-1550	1300-1550
Вероятность регистрации одиночного фотона в гейгеровском режиме	%	10	15	20	30	35	50
Частота темновых импульсов в гейгеровском режиме при температуре -60°C	кГц	50	20	10	10	10	5
Временное разрешение	пс	200	100	50	20	10	5
Обратное напряжение пробоя	В	70	60	60	60	60	50
Рабочая температура	К	200-250	200-250	200-250	200-250	200-250	200-250

Применение: **КРИПТОГРАФИЯ**

- для использования в системах
 квантовой коммуникации на основе
 ВОЛС

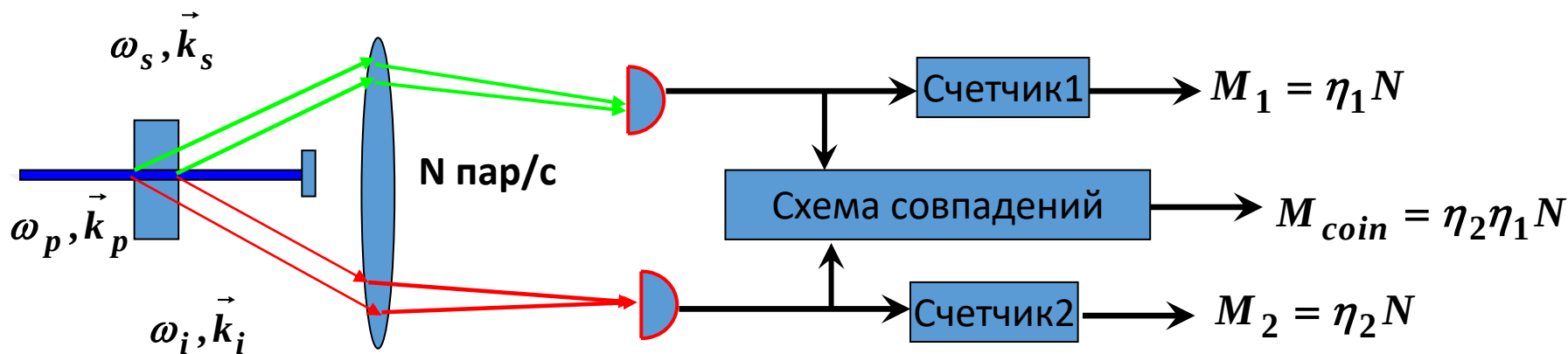


Характеристики	Единицы	2020	2021	2022	2023	2024	2030
Точность	мкГал	Разработка	Разработка	Разработка	10	5	0.5
Чувствительность	мкГал/Гц ^{1/2}	Разработка	Разработка	Разработка	50	30	3

Характеристики	Единицы	Значение
Точность	мкГал	несколько
Чувствительность	мкГал/Гц ^{1/2}	50 5 2 1
Оперативность измерения	мин	- 1.5 10 40
Стабильность	мкГал	Не более 1



АБСОЛЮТНАЯ КВАНТОВАЯ ФОТОМЕТРИЯ: безэталонное измерение квантовой эффективности детекторов



$$\eta_2 = \frac{M_{coin}}{M_1}$$

$$\eta_1 = \frac{M_{coin}}{M_2}$$

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

ПРИКАЗ

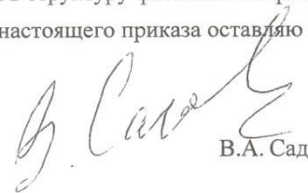
«12» февраля 2018 г. Москва № 125

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 положения 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. Садовничийприказом
-для осуществления
комитета создан
ий»
нной поддержки
ологий РФ

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 (подготовки специалистов, тематика специализации))

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

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.

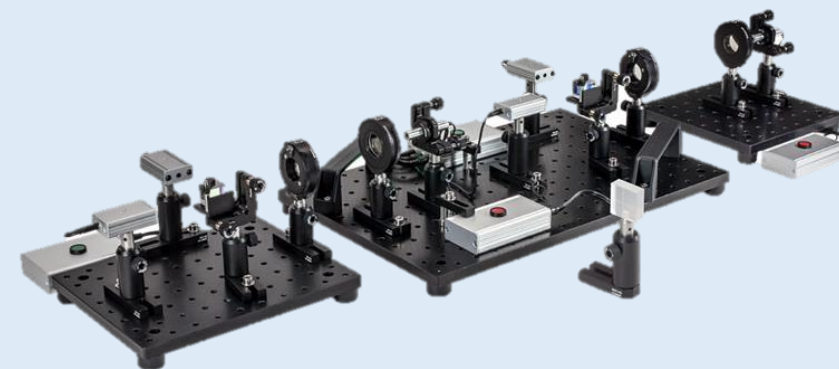
Для сотрудников и преподавателей вуза, имеющих высшее образование, предусмотрен дополнительный модуль повышения квалификации по методике преподавания в данной предметной области.

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

education@quantum.msu.ru

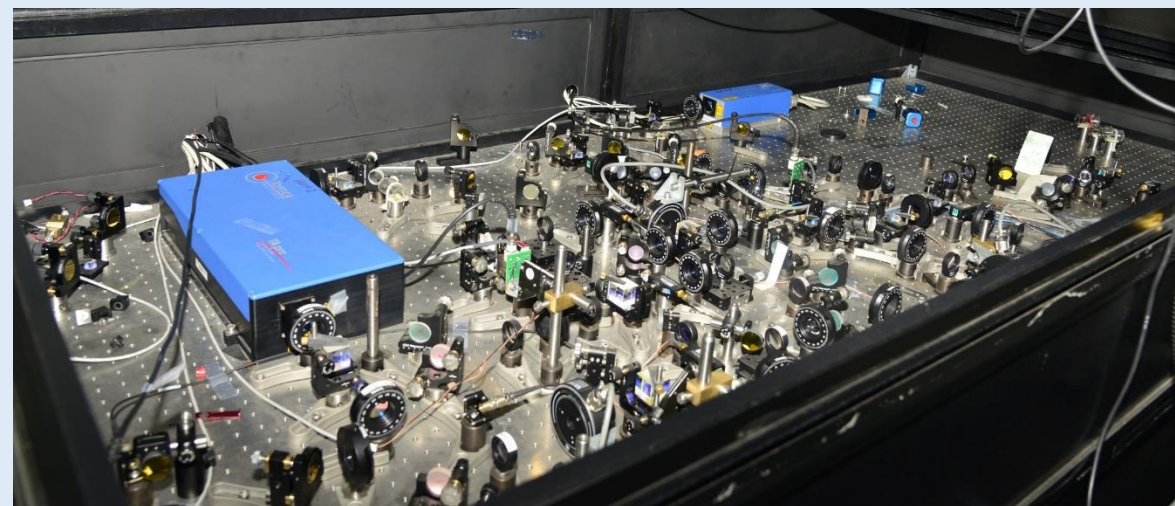
Поляризационная оптика

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 Мандела
8. Гомодинное детектирование

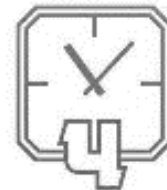
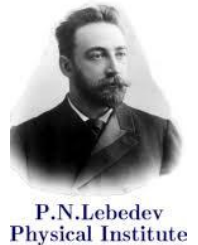


ПОДДЕРЖКА И КООПЕРАЦИЯ



Исследования и разработки в области квантовых технологий проводятся в нескольких университетах, институтах РАН и коммерческих организациях.

Индустриальную и организационную поддержку обеспечивают государственные корпорации Росатом, Ростех и ОАО «РЖД».



ВЫВОДЫ 1

- 1. В области квантовых вычислений**, речь идет о создании в ближайшие 5 лет среднемасштабных вычислителей, способных продемонстрировать «квантовое преимущество» перед классическими суперкомпьютерами в ряде задач.
- 2. В области квантовых коммуникаций**, речь идет о создании разветвленных сетевых структур управления потоками информации, космической квантовой связи и предоставлении операторами целого спектра услуг по защите информации.
- 3. В области квантовой сенсорики**, речь идет о разработке и внедрении чувствительных малогабаритных устройств для использования в навигации, геологоразведке, медицине и др.
- 4. В организационном плане** имеются существенные заделы в нескольких коллективах: - именно здесь должны концентрироваться передовые научные разработки в области квантовых технологий

ВЫВОДЫ 2

- «Если плохо учить физику в школе, мир будет казаться сплошным чудом» (Народная мудрость);
- Квантовые технологии: Не лишайте детей детства!

Центр квантовых технологий, физический
Sergei.kulik@physics.msu.ru



СПАСИБО ЗА ВНИМАНИЕ!

ПЕРЕДАЧА КВАНТОВЫХ ДАННЫХ																			
АЛИСА																			
Случайная последовательность битов у Алисы	1	1	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	0
Базис, случайно выбираемый Алисой	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R	D	R	R	D
Состояние, которое посылает Алиса	□	↓	□	↔	↓	↓	↔	↔	□	□	↓	□	□	□	↓	□	↔	↓	□
БОБ																			
Базис, случайно выбираемый Бобом	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R	R	R	D	D
Биты, регистрируемые Бобом (сырой ключ)	1	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0
Учли технические потери	1	×	1	×	1	1	0	0	×	1	1	1	×	0	1	×	0	0	0
ОТКРЫТОЕ ОБСУЖДЕНИЕ																			
Боб сообщает базис, в котором зарегистрирован бит	R		D		R	D	D	R	×	R	D	D	×	D	R	×	R	D	D
Алиса сообщает, какой базис совпадает с ее базисом	-		Д а		Д а	-	-	Д а	-	-	-	Д а	Д а	Д а	Д а		Д а	-	Д а
Предварительная распределенная информация (подслушивания нет) - просеянный ключ			1		1			0				1		0	1		0		0
КОРРЕКЦИЯ ОШИБОК																			
Боб сообщает случайно выбранные биты					1										1		0		
Алиса сравнивает их с соответствующими своими					Д а										Д а		Д а		
ИТОГ																			
Распределенный ключ			1					0				1		0					0

Таблица 1. Протокол BB84 (нет подслушивания, без усиления секретности)