



**Прорыв в  
КВАНТОВЫХ  
ТЕХНОЛОГИЯХ**

---

<https://www.cbsnews.com/news/google-quantum-computing-quantum-supremacy-claim-by-google-disputed-by-ibm/>

**GOOGLE SAYS IT HAS ACHIEVED QUANTUM S**

**BSN**

# ДОСТИЖЕНИЯ

- 200 секунд вместо тысяч лет.
- Не университеты, не правительство, а коммерческая компания.
- Скоро эти технологии придут в нашу жизнь.

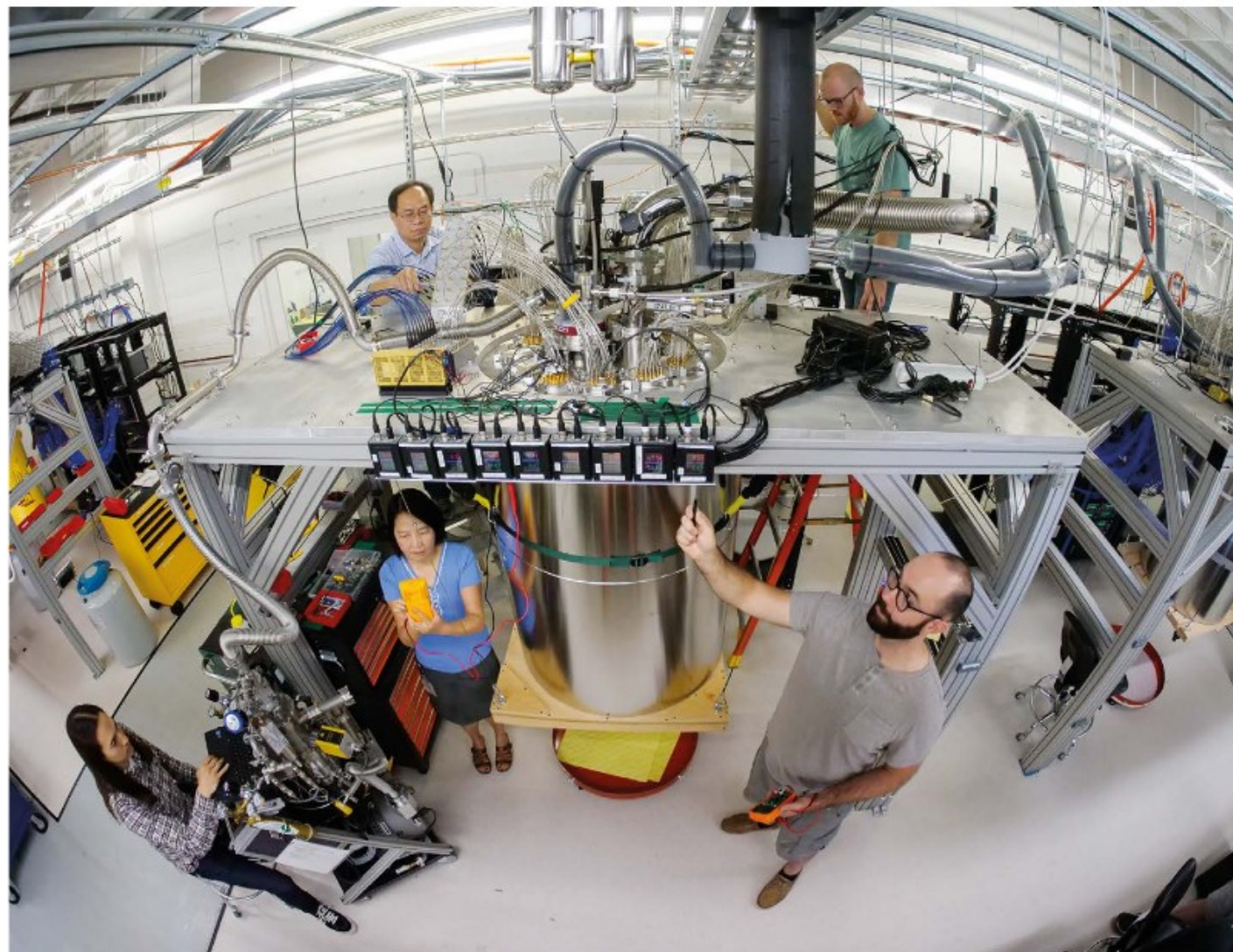




Financial Times.  
«Google  
утверждает, что  
достиг  
квантового  
превосходства»

---

## News in focus



Google's quantum computer excels at checking the outputs of a random-number generator.

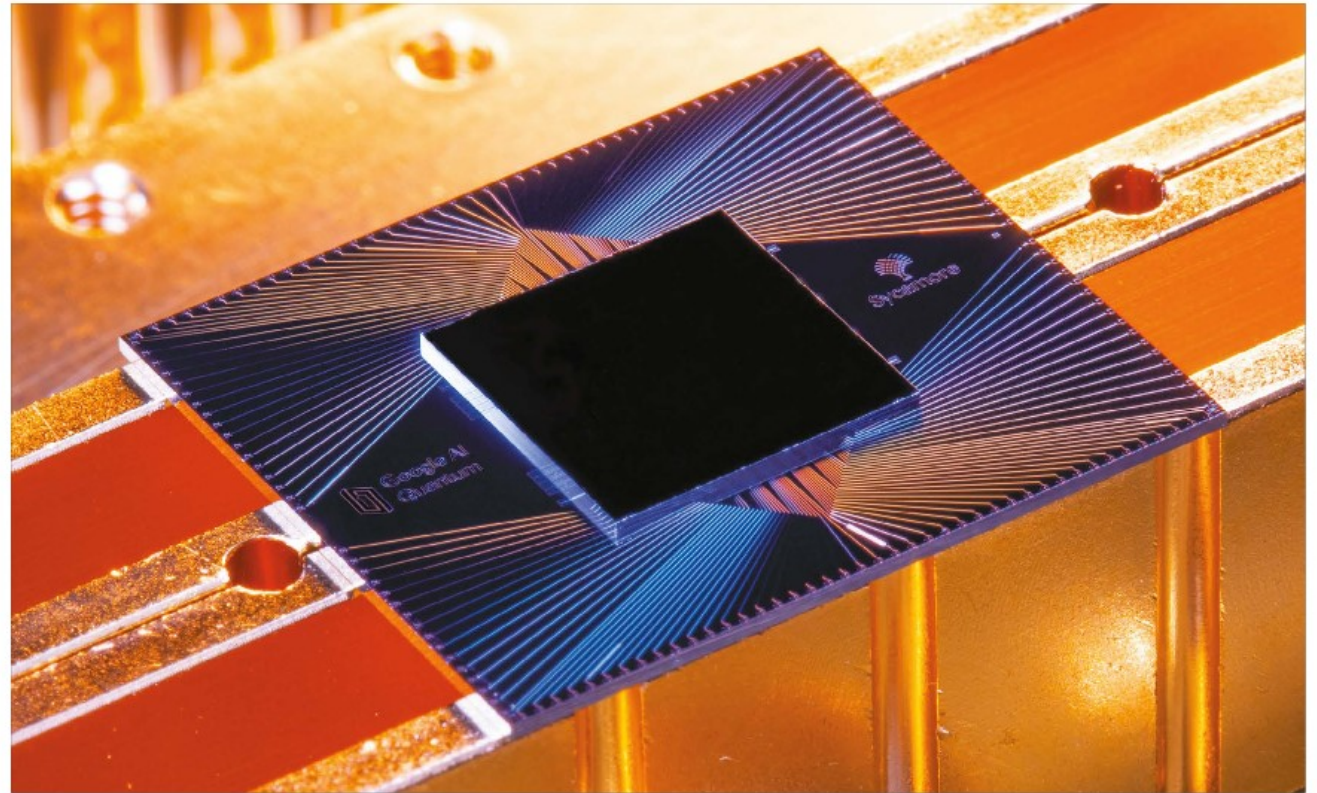


# Quantum Computing

---

Google опубликовал заявление о своем превосходстве.

## News in focus



The Sycamore chip is composed of 54 qubits, each made of superconducting loops.

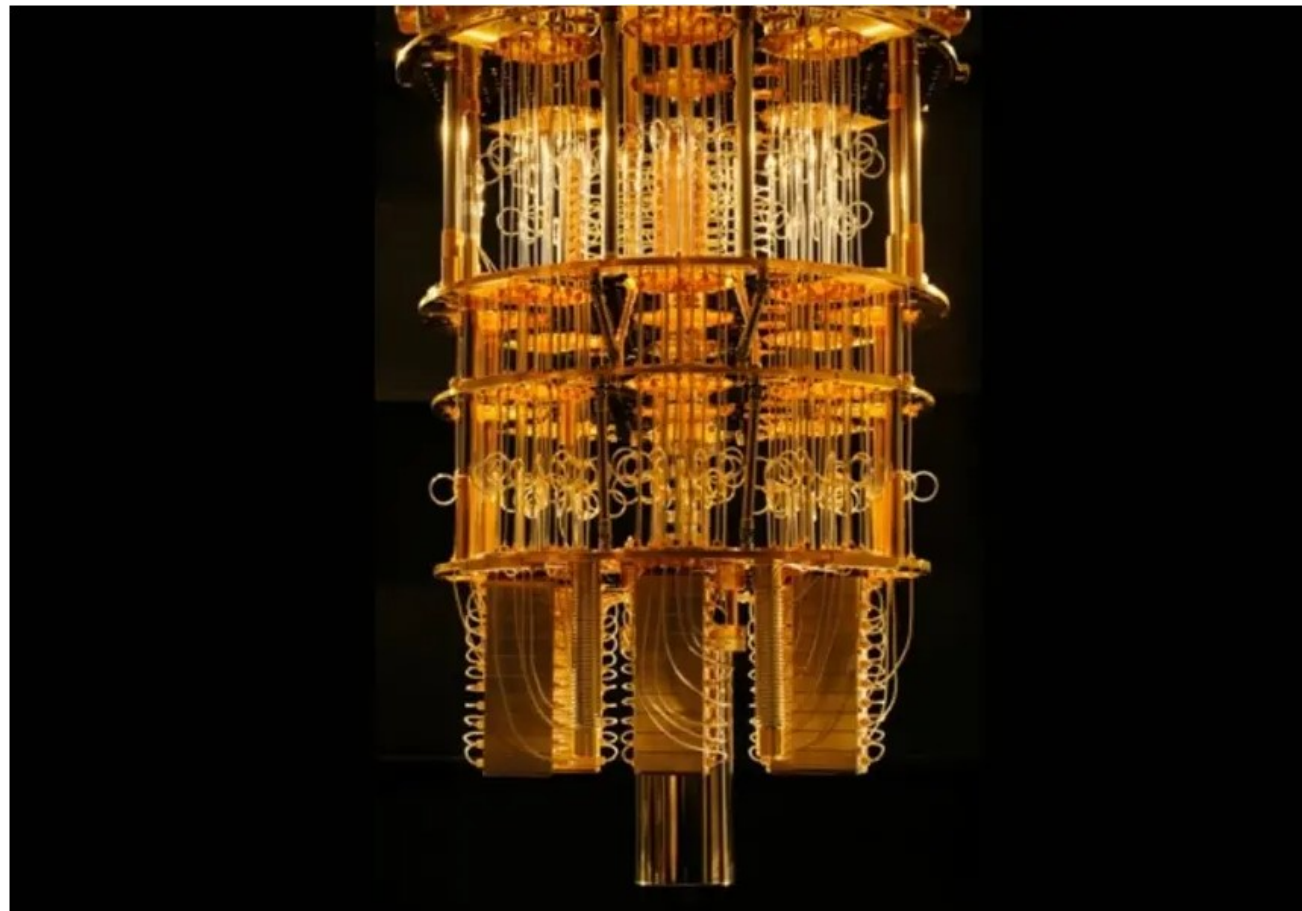
**GOOGLE PUBLISHES  
LANDMARK QUANTUM  
SUPREMACY CLAIM**

# Квантовый компьютер Google оказался ненамного лучше обычных


IBM его раскритиковала

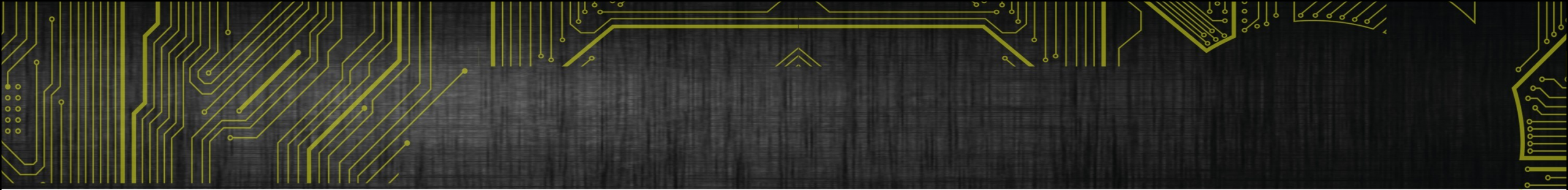
 Обсудить

Недавно СМИ заявили о достижении Google квантового превосходства. Это значит, что компания разработала самый мощный квантовый компьютер в мире. По крайней мере, так говорили журналисты. Сотрудники же IBM раскритиковали это заявление, проанализировав разработку.





- 
- Что же случилось на самом деле?
  - Имеет ли место квантовое превосходство?
  - Что вообще такое квантовый компьютер?
  - Как он работает и почему он такой быстрый?

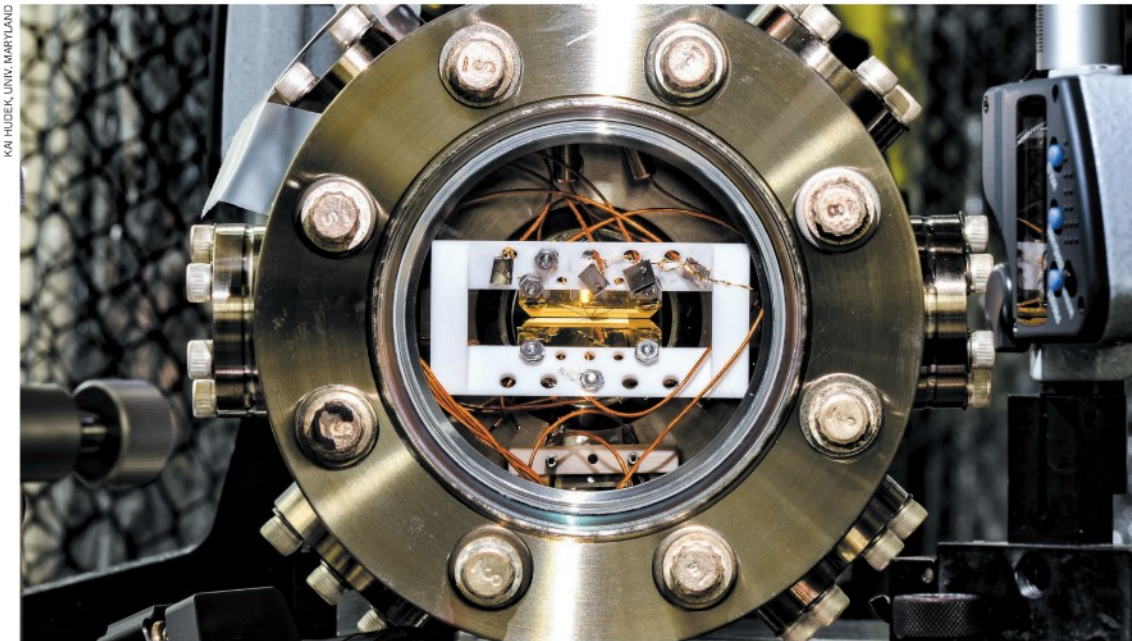
- 
- История развития квантовых компьютеров.
  - Где ожидаются прорывы в связи с появлением квантовых компьютеров и какие в связи с этим есть преимущества
  - Какие угрозы несут квантовые компьютеры
  - Как противостоять этим угрозам

# Содержание

- Вовлечение в квантовые исследования коммерческих компаний означает ускорение получения практических результатов
- Что такое квантовый компьютер, биты, кубиты, регистры
- Возможности квантового компьютера для решения инновационных задач
- Возможности квантового компьютера для решения хакерских задач
- История развития квантового компьютера
- В чем состоит взлом. Формула ключей RSA.
- На сколько ослабнет криптографическая защита при широкой доступности квантовой атаки
- Направления защиты от квантового взлома классических алгоритмов защиты критической инфраструктуры информации
  - Квантовое распределение ключей
  - Квантово-устойчивые алгоритмы защиты данных



# Quantum Computing



KAI HUDEK, UNIV. MARYLAND

A front runner in the pursuit of quantum computing uses single ions trapped in a vacuum.

PHYSICS

## Quantum computers ready to leap out of the lab

*The race is on to turn scientific curiosities into working machines.*

Квантовые компьютеры находятся на выходе из лабораторий.

Гонка превращает научное любопытство в рабочие машины

Nature 541 (2017)

Можно быстро выполнять быстрые вычисления.  
В том числе связанные с безопасностью

Плюсы:

- **Квантовый компьютер как следующий шаг в развитии ИТ**

<https://nauka.vesti.ru/article/1238158> . Пример – прорыв Google, квантовый компьютер впервые превзошёл обычный

- Достижения Google могут принести пользу квантовым вычислениям, привлекая больше ученых и инженеров в этой области.

[\\*https://www.nature.com/magazine-assets/d41586-019-03213-z/d41586-019-03213-z.pdf](https://www.nature.com/magazine-assets/d41586-019-03213-z/d41586-019-03213-z.pdf)



# Будущее наступило: когда без квантовых компьютеров не получится обойтись



№11 ноябрь 2019

## НАУКА И ЖИЗНЬ (/)

Оформить (/)

Портал функционирует при финансовой поддержке Федерального агентства по печати и массовым коммуникациям.

[Новости \(/news/\)](/news/) [События \(/info/\)](/info/) [Факт дня \(/facts/\)](/facts/)

[Открытый формат \(/open/\)](/open/) [Новости партнеров \(/prtnews/\)](/prtnews/) [Архив \(/archive/\)](/archive/)

[Видео \(/video/\)](/video/) [Подписка \(/shop/842/\)](/shop/842/) [Магазин \(/shop/\)](/shop/)

[Библиотеки \(/shop/library/\)](/shop/library/) [Реклама \(/advert/\)](/advert/) [Форум \(/forum/\)](/forum/)

[НАУКА И ЖИЗНЬ \(/\)](/) / [Архив журнала «НАУКА И ЖИЗНЬ» \(/archive/\)](/archive/) / [Наука на марше \(/articles/rubric/5/\)](/articles/rubric/5/) /  
Наука. Вести с переднего края



### Квантовые компьютеры

Кандидат физико-математических наук Л. ФЕДИЧКИН (Физико-технологический институт Российской академии наук.

№1, 2001

[\(/archive/469/5305/\)](/archive/469/5305/)

Используя законы квантовой механики, можно создать принципиально новый тип вычислительных машин, которые позволят решать некоторые задачи, недоступные даже самым мощным современным суперкомпьютерам. Резко возрастет скорость многих сложных вычислений; сообщения, посланные по линиям квантовой связи, невозможно будет ни перехватить, ни скопировать. Сегодня уже созданы прототипы этих квантовых компьютеров будущего.

# Применение квантовых компьютеров: примеры\*

- ✓ Искусственный интеллект
- ✓ Молекулярное моделирование
- ✓ Финансовое моделирование
- ✓ Прогнозирование погоды
- ✓ Физика частиц
- ✓ Транспортная задача
- ✓ ? ✗ Криптография



\* [https://issa-cos.org/wp-content/uploads/2017/11/ISSA Journal November 2017.pdf](https://issa-cos.org/wp-content/uploads/2017/11/ISSA_Journal_November_2017.pdf)

\* <https://econet.ru/articles/169065-polza-kvantovyh-kompyuterov>



# CES 2019: первый в мире сверхдоступный квантовый компьютер

- Компания IBM представила на выставке CES квантовый компьютер IBM Q, который смогут приобрести коммерческие компании, научные организации и учебные заведения.

IBM Q предлагает 20-кубитное вычисление с использованием классических компьютерных компонентов и квантовых решений. Компьютер довольно массивный — воздухонепроницаемая квадратная «коробка» около трех метров в ширину и глубину, в центре которой висит «люстра», в которой производятся сложнейшие вычисления. В стандартный комплект поставки входит система охлаждения.

И хотя IBM рассматривает компьютер IBM Q в качестве пробного шага в доступном квантовом вычислении, компания постаралась сделать его максимально привлекательным даже внешне. Он смотрится очень эффектно — как яркая декорация из научно-фантастического фильма.

- <https://youtu.be/LAA0-vjTaNY>
- [https://www.iguides.ru/main/gadgets/pervyy\\_v\\_mire\\_sverkhдоступnyy\\_kvantovyy\\_kompyuter/](https://www.iguides.ru/main/gadgets/pervyy_v_mire_sverkhдоступnyy_kvantovyy_kompyuter/)

## Ограничение приложений (результат не на любых задачах)

### Минусы:

- новости могут создать впечатление, что квантовые компьютеры ближе к основным практическим приложениям, чем они есть на самом деле.\*
- Важен способ исправления ошибок - метод исправления ошибок, вызванных шумом, которые в противном случае могли бы испортить вычисления.
- Физики считают, что это важно для обеспечения масштабируемости работы квантовых компьютеров.

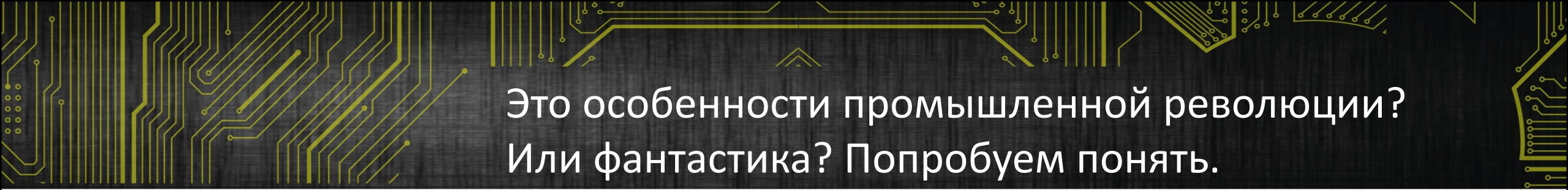
\*<https://www.nature.com/magazine-assets/d41586-019-03213-z/d41586-019-03213-z.pdf>



# Мнения разных ученых

- Мартинис – “Google работает над обоими этими вехами и обнародует результаты своих экспериментов в ближайшие месяцы.”
- Ааронсон - эксперимент, разработанный Google для демонстрации квантового превосходства, может иметь практическое применение. Создан протокол для использования таких вычислений, чтобы доказать пользователю случайность битов, генерируемых генератором квантовых случайных чисел. Это может быть полезно, например, в криптографии и некоторых криптовалютах, безопасность которых зависит от случайных ключей.
- Инженерам Google пришлось выполнить ряд усовершенствований своего оборудования, чтобы запустить алгоритм, включая создание новой электроники для управления квантовой схемой и разработку нового способа соединения кубитов. «Это действительно основа того, как мы будем расширяться в будущем. Мы считаем, что эта базовая архитектура - путь вперед » \*

\*<https://www.nature.com/magazine-assets/d41586-019-03213-z/d41586-019-03213-z.pdf>



Это особенности промышленной революции?  
Или фантастика? Попробуем понять.

## Сегодня мы обсудим вопросы

- **Что такое квантовые вычисления?**
- **За какое время квантовый компьютер может узнать открытый ключ классической сильной криптографии?**
- **Как подготовиться такому развитию событий?**



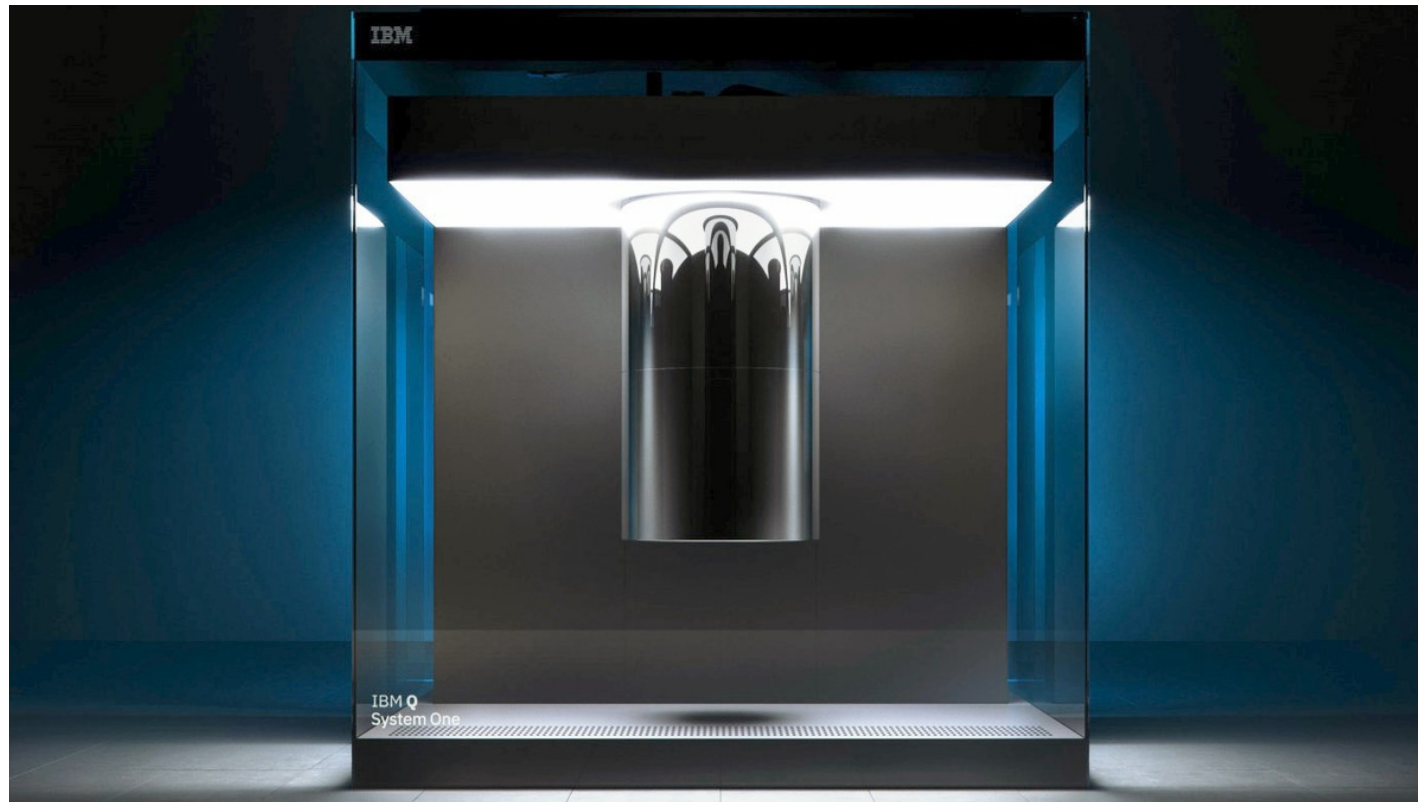
Forbes. Госкорпорация «Росатом» объявила о запуске проекта по созданию отечественного квантового компьютера



**Квантовый компьютер поможет России войти в число стран-лидеров «квантовой гонки».**



## IBM представила новый квантовый компьютер



**Компания IBM представила на проходящей в Лас Вегасе выставке CES 2019 квантовый компьютер IBM Q System One.**

**Согласно заявлению компании, это первая в мире интегрированная квантовая вычислительная система, пригодная для коммерческого применения, сообщает IKS MEDIA.**

<https://www.computerra.ru/234158/ibm-predstavila-novyj-kvantovyj-kompyuter/>



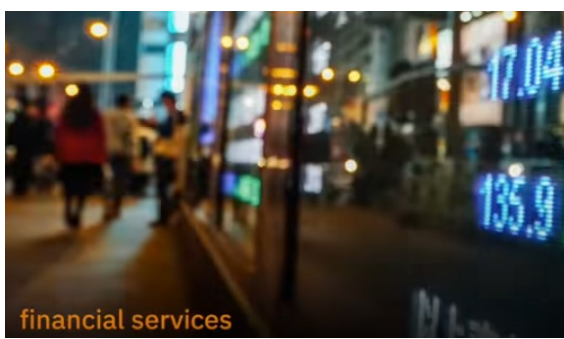
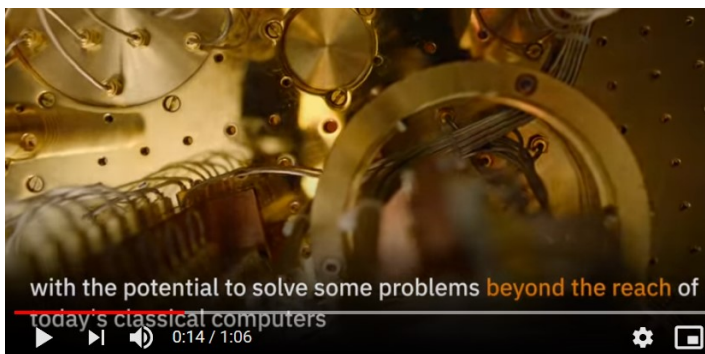
# Q System One



- Q System One включает систему из 20 кубитов, заключенную в большой герметичный корпус кубической формы.
- Корпус выполнен из боросиликатного стекла толщиной 1,27 см, отличающегося высокой термоустойчивостью.
- Передняя и задняя стенки куба могут открываться, обеспечивая инженерам доступ к «внутренностям» компьютера
- помимо квантового процессора в корпусе Q System One располагаются различные управляющие модули, а также высокопроизводительная криогенная система

<https://youtu.be/LAA0-vjTaNY>

<https://www.computerra.ru/234158/ibm-predstavila-novyj-kvantovyj-kompyuter/>



IBM Q System One позволяет универсальным приближенным сверхпроводящим квантовым компьютерам впервые работать за пределами исследовательской лаборатории.

Это важный шаг вперед в коммерциализации квантовых вычислений, который может однажды сделать прорыв в таких областях, как открытие материалов и лекарств, финансовые услуги и искусственный интеллект.



# “Эффективность квантовых компьютеров



Система обладает 20-кубитным квантовым чипом и "тысячами" других компонентов. Модульная конструкция позволяет легко модернизировать и обслуживать компьютер, говорят в IBM. Камера охлаждается она сверху вниз: температура в самой верхней части составляет 4 Кельвина ( $-269,15^{\circ}$  по шкале Цельсия), в нижней — 10 милликельвинов. Однако купить Q System One "с улицы" нельзя: сначала он будет доступен исключительно партнерам IBM. Стоимость компьютера не разглашается.



Нельзя считать состояние квантовой системы без воздействия на нее



Квантовые компьютеры взломают все нынешние шифры, но обеспечат собственную безопасную связь. [\(иллюстрация Centre for Quantum Technologies, National University of Singapore\).](#)



# Квантовый взлом (Quantum Break)

Вскоре квантовые компьютеры могут сломать большинство традиционных открытых ключей крипто и каждый защищаемый классической криптографией секрет.

- RSA, DH, ECC, PKI, цифровые сертификаты, цифровые подписи, TLS, HTTPS, VPN, защита WiFi, смарт-карты, HSM, криптовалюты, двухфакторная аутентификация, основанная на цифровых сертификатах (например, FIDO ключи, ключи безопасности Google и т. д.)