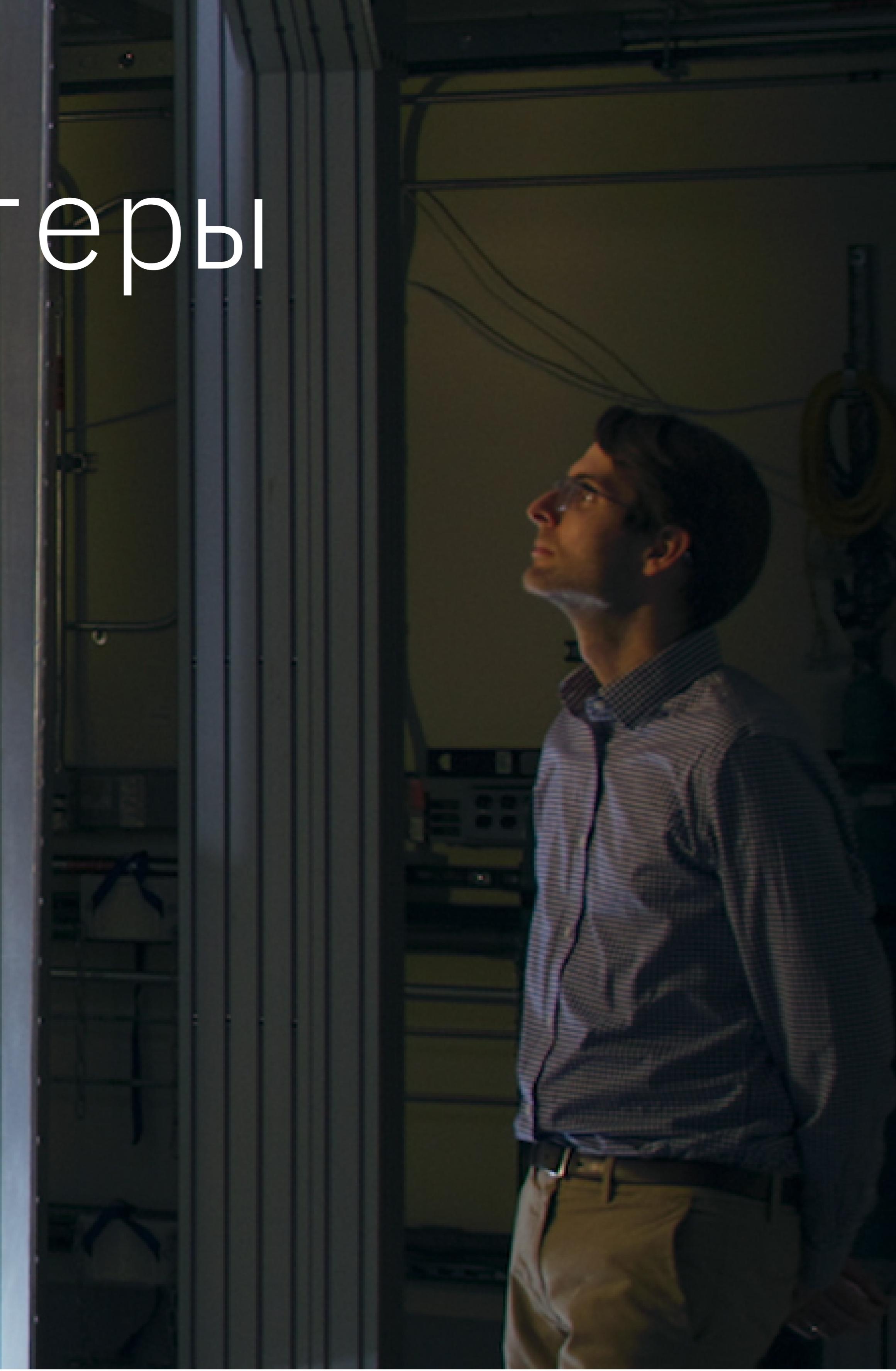
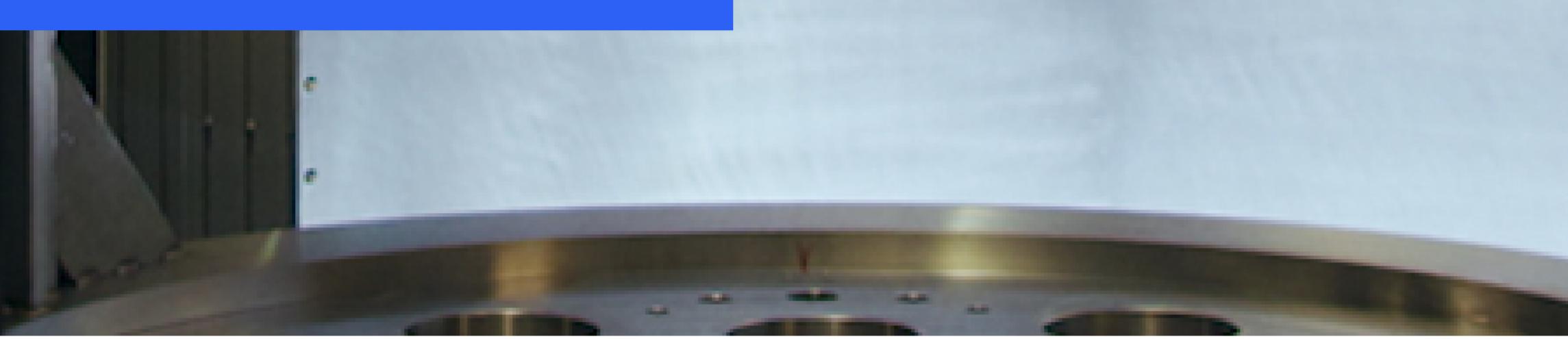


Квантовые компьютеры

Решение многих современных проблем требует чрезвычайно мощных вычислений, с которыми не могут справиться даже суперкомпьютеры

Результат работы ↓



Вступление

Существует множество задач, решение которых за полиномиальное время потенциально возможно только на квантовом компьютере. Одна из таких — алгоритм Шора.



Цель проекта заключается в изучении и написании квантового алгоритма факторизации чисел и квантово-классической нейронной сети на языке программирования Python и запуске алгоритмов на квантовом компьютере IBM Q.

Алгоритм Шора

С помощью квантового алгоритма факторизации чисел становится возможным взлом криптографических систем с открытым ключом.

Реализованный алгоритм раскладывает число 15 на простые множители, используя найденный период r , такой что $a^r \bmod N = 1$.

Пока квантовый компьютер не способен раскладывать большие числа, однако, учитывая стремительный темп развития современных технологий, эра крипtosистем с открытым ключом, судя по всему, подходит к концу.

Фаза	Дробь	Результат угадывания периода
0	0.50	1/2
1	0.00	0/1
2	0.25	1/4
3	0.75	3/4

Простые делители числа 15 : 3
Простые делители числа 15 : 5

Квантово-классическая нейронная сеть

Реализованная гибридная квантово-классическая нейронная сеть обучена классификации изображений с нарисованными от руки нулями и единицами.



Квантовая часть алгоритма — это скрытый слой, представляющий собой параметризованную квантовую цепь, в которой градус поворота для каждого вентиля схемы определяется компонентами классического входного вектора. Выходные данные предыдущего слоя нейронной сети используются в качестве входных данных параметризованной схемы.

В настоящее время классические нейронные сети настолько хороши, что применение квантовых технологий практически не улучшает результат, тем не менее, может уже завтра квантовые компьютеры смогут решать любые не решаемые сегодня задачи.