Квантовая угроза объектов критической информационной инфраструктуры РФ: Как защититься от атак с использованием квантового компьютера?

Академия АйТи, CISO Сергей Петренко

Академия АйТи

Входит в ГК Softline

Основана в 1995 г.

EdTech:
разработка e-learning контента и технологичных решений для обучения

Направления обучения:

Информационная безопасность

Информационные технологии
Цифровая трансформация и MBA CDTO

Управление проектами

Разработка и тестирование ПО и др.

Москва, Санкт-Петербург, Казань, Уфа, Челябинск, Хабаровск, Красноярск, Тюмень, Нижний Новгород, Волгоград

Ресурсы более 400 высококлассных экспертов и преподавателей, методистов, педагогических дизайнеров

Член Консорциума 2035
по развитию цифровой грамотности и компетенций цифровой экономики

6 место в ТОП-15 школ ДПО 2022
рейтинг РБК и Smart Ranking

Школа ИТ-кадры:
стажерская программа обучения команд под задачи заказчика

Сервис Академия АйТи онлайн:
Платформа LMS, библиотека контента, бесшовная интеграция с сервисами

Крупные заказчики

СБЕР, РЖД, Билайн, TATNEFT, НОРНИКЕЛЬ

100+
сотрудников

Оценка текущего состояния

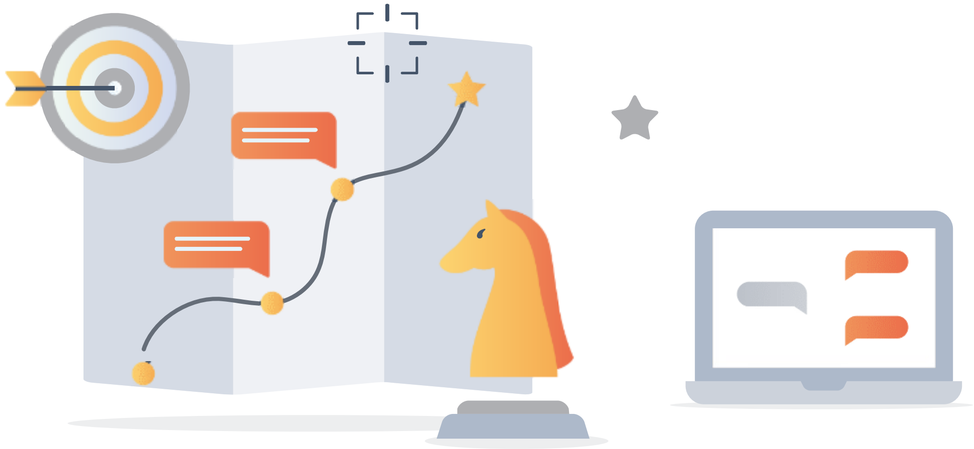
Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»

- **Быстрое развитие** информационно-телекоммуникационных технологий повышает вероятность возникновения угроз информационной безопасности
- **Использование** информационно-коммуникационных технологий **для вмешательства** во внутренние дела государства

  Увеличение числа **компьютерных атак** на российские информационные ресурсы
- Отработка действий по выведению из строя **объектов КИИ** вооруженными силами иностранных государств
- Размещение и распространение **недостоверной** и противоправной **информации** в сети Интернет
- Стремление ТНК закрепить своё **монопольное положение** в сети Интернет и контролировать информационные ресурсы с помощью цензуры и блокировки интернет-платформ
- **Анонимность** за счёт использования ИКТ облегчает совершение преступлений
- Использование в РФ **иностранных** информационных технологий и телекоммуникационного оборудования повышает **уязвимость** российских информационных ресурсов (особенно объектов КИИ)

Несколько событий по теме

В апреле 2022 года Директор АНБ (National Security Agency, NSA) США Пол М. Накасоне заявил о том, что «криптоаналитически значимый квантовый компьютер может поставить под угрозу системы гражданской и военной связи и подорвать боеспособность стратегических систем контроля и управления критической информационной инфраструктуры США и их союзников по НАТО. Для нейтрализации этой квантовой угрозы потребовал создать постквантовые схемы асимметричного шифрования (Public-Key Encryption) и электронной подписи (Digital Signatures)» **Источник**



В мае 2022 года администрация Президента США Джо Байдена выпустила две новые директивы о подготовке государства и бизнеса к будущим квантовым кибератакам **Источник**

В декабре 2022 года администрация Джо Байдена поручила NIST, АНБ и Агентству по кибербезопасности и защите инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA) в срок от 90 дней до 1 года выполнить все необходимые мероприятия по защите критической инфраструктуры США и их союзников по НАТО от квантовых атак **Источник**

Актуальность проблемы

Department of Homeland Security (seit 9/11)

US Government

Department of Justice

Foreign Intelligence Surveillance Court FISC (FISA)

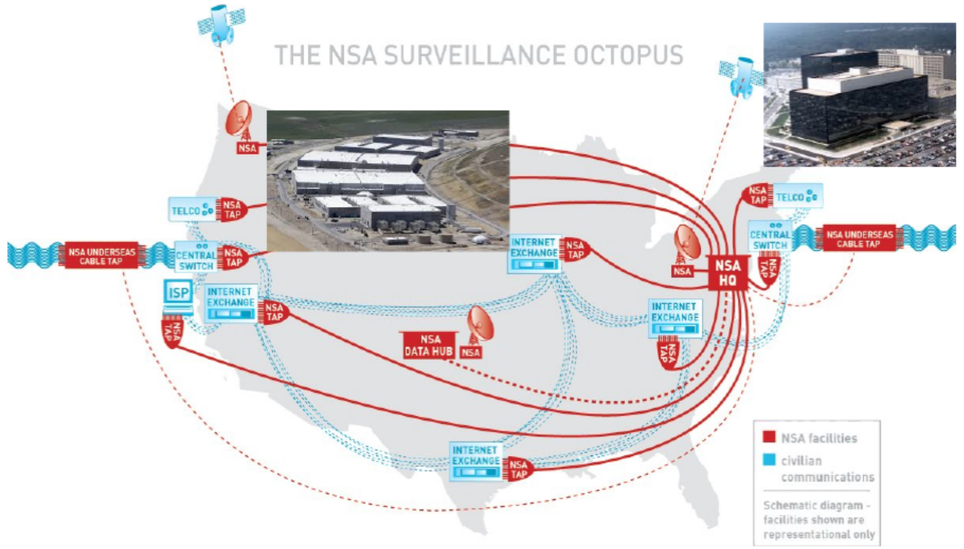
Cyber Command

Drug Enforcement Administration

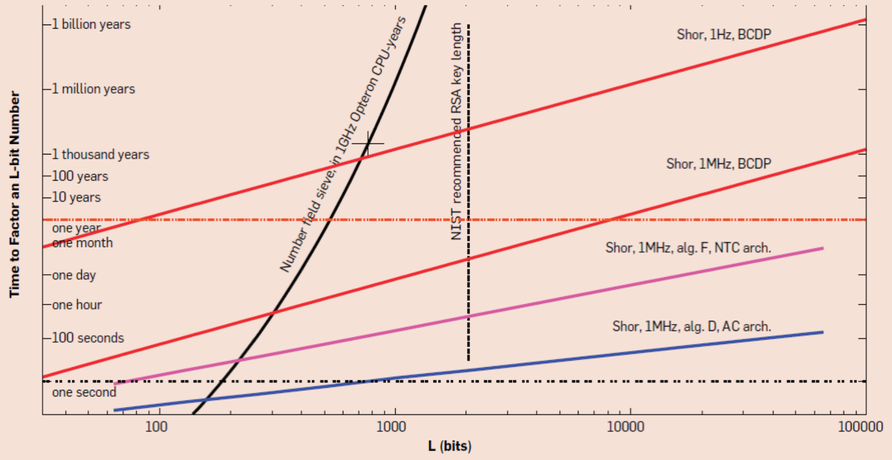
Central Intelligence Agency

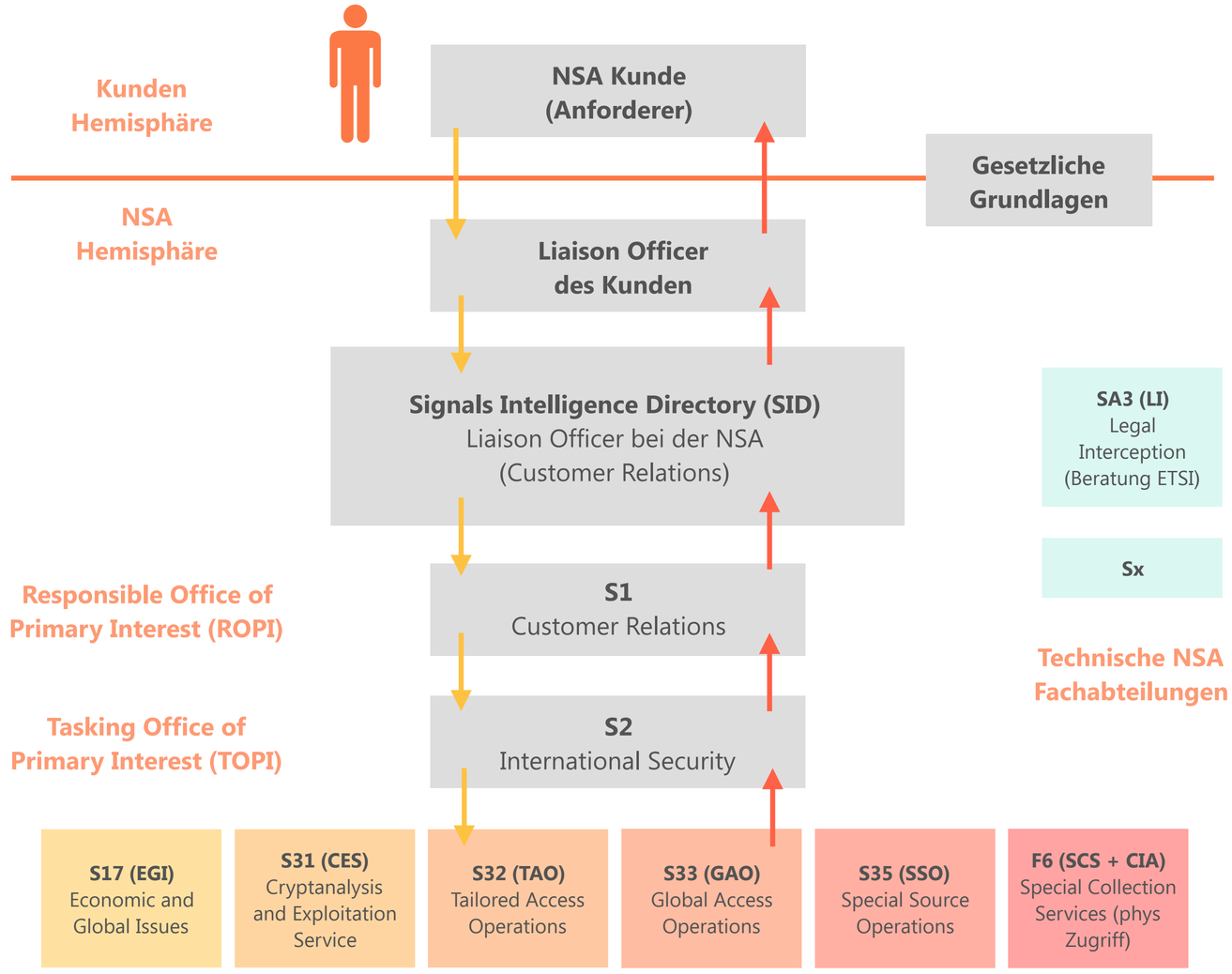
National Security Agency

Federal Bureau of Investigation

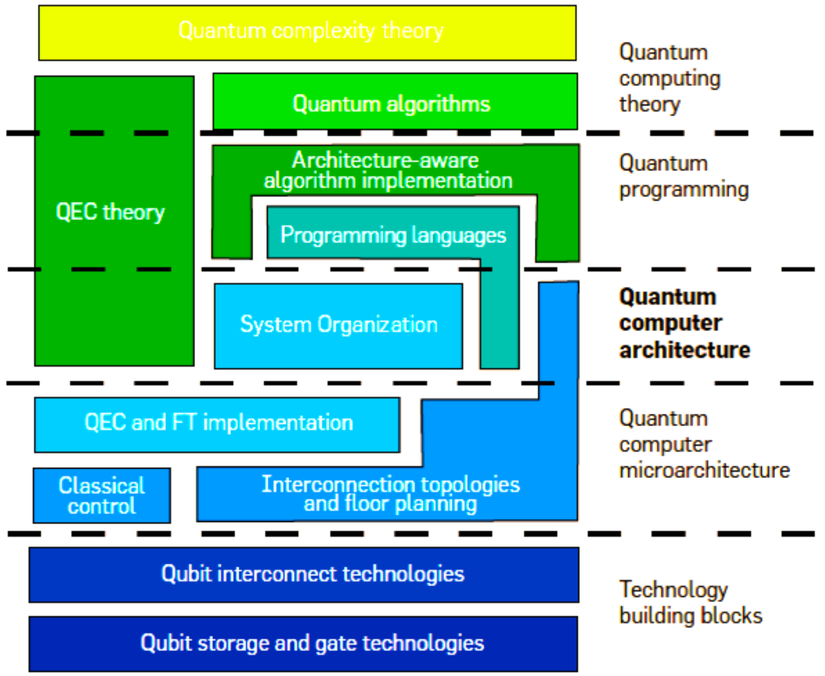


Актуальность проблемы





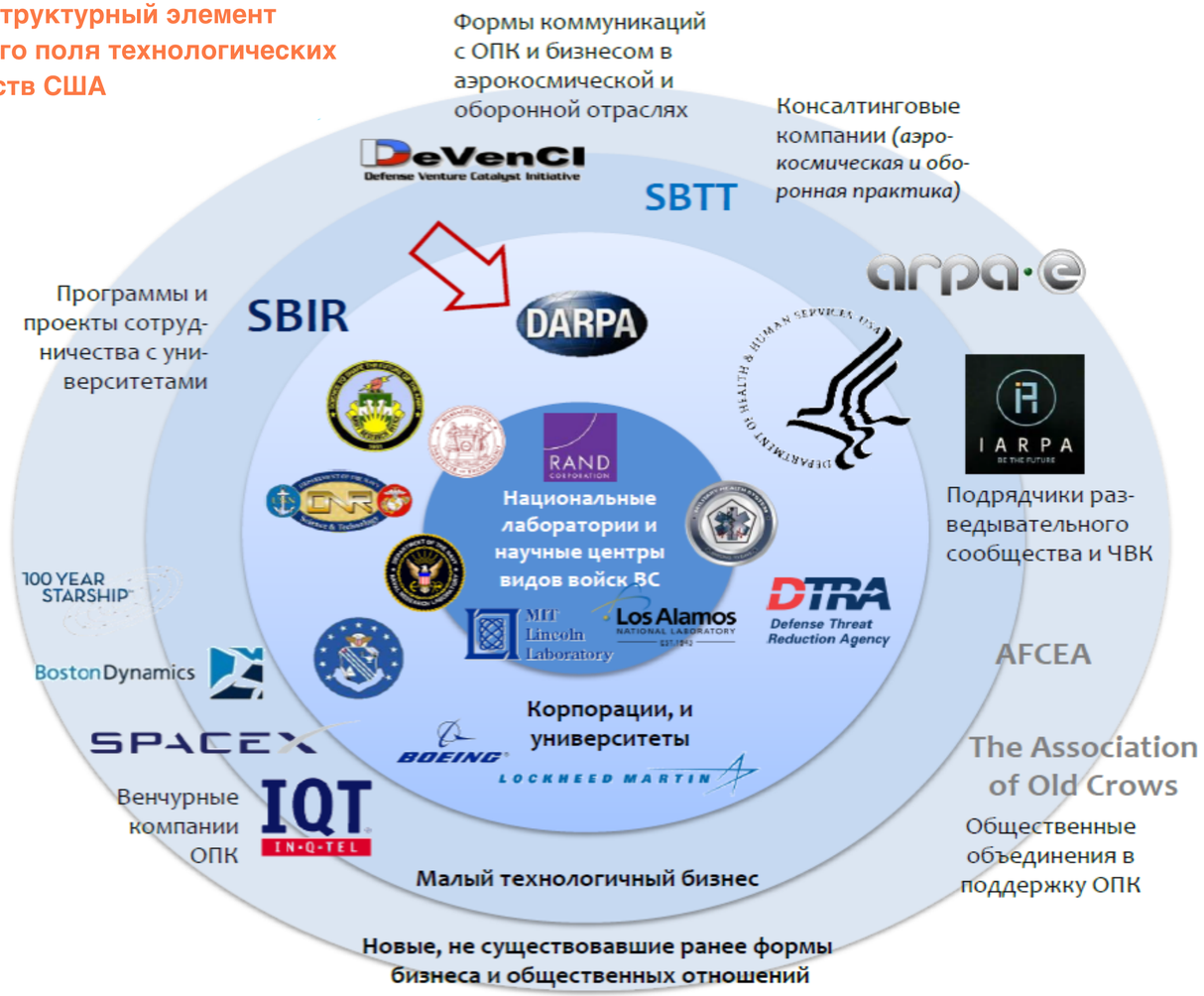
Национальные квантовые программы и инициативы

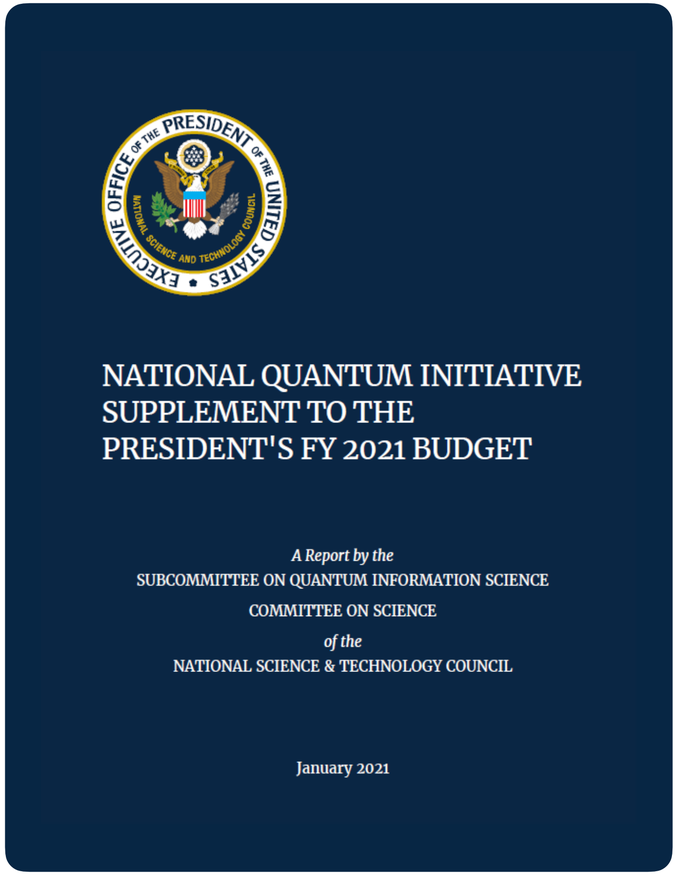


Национальные квантовые программы и инициативы

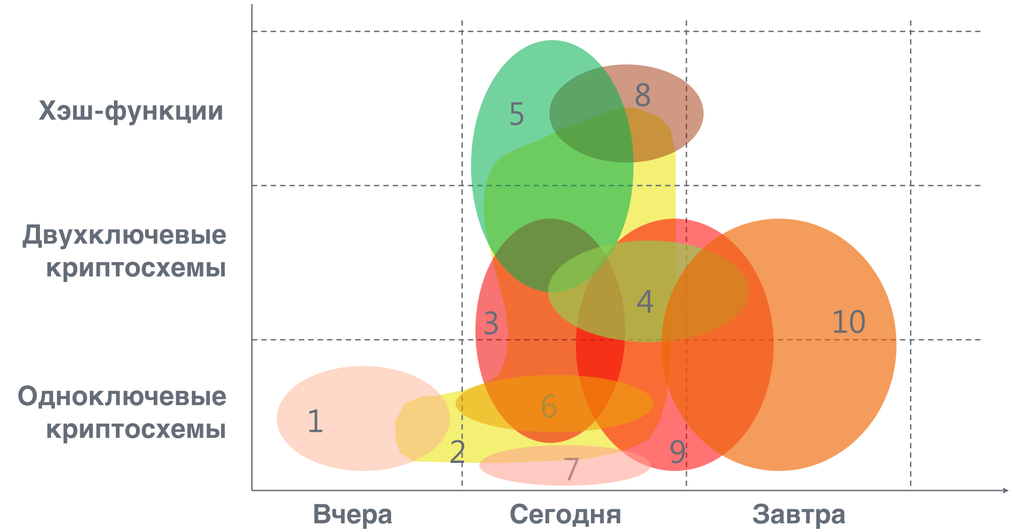
Эффект масштаба

DARPA - это яркий, но всего лишь структурный элемент игрового поля технологических новшеств США





Классификация основных алгоритмов и инструментов криптоанализа



1 - Частотный анализ

2 - Полный перебор ключей

3 - Анализ ключевого генератора

4 - Решение задач факторизации и дискретного логарифмирования

5 - Метод “Встречи посередине”

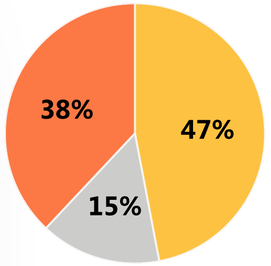
6 - Разностный анализ

7 - Линейный анализ

8 - Метод коллизий

9 - Анализ по побочным каналам

10 - Квантовый анализ

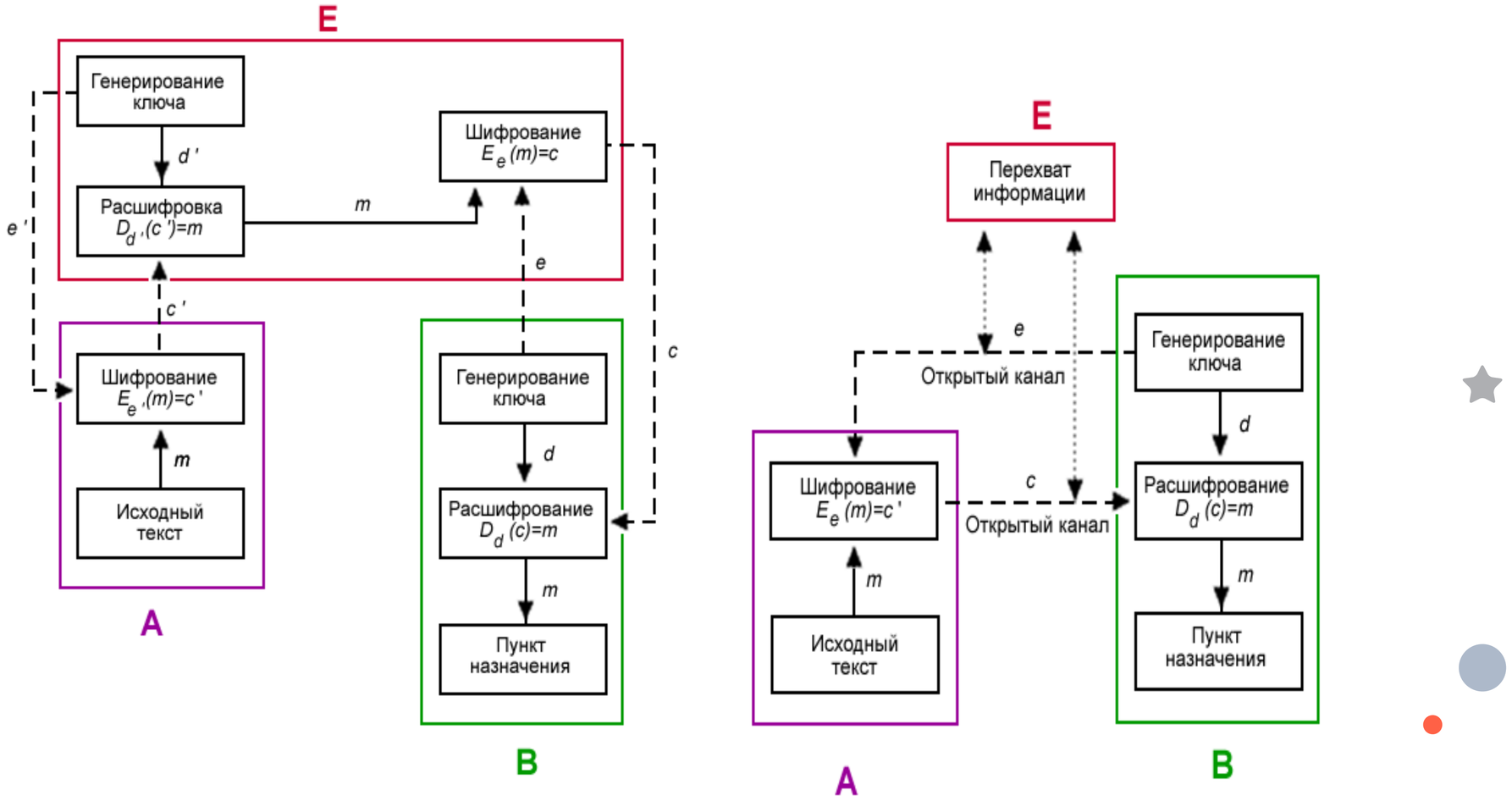


Современные О КИИ РФ по состоянию на февраль 2023 года:

- Используют двухключевые схемы
- Используют одноключевые схемы
- Не используют шифрование

Решение проблемы факторизации	
Название	Сложность
Метод Ферма	$T(N) = O(N^{\frac{1}{3}})$
Метод Ленстры	$T = O(e^{\sqrt{2 \ln p \ \ln \ln p}})$
Метод Диксона	$T = O(L(n)^2)$
Метод квадратичного решета	$T = O(\exp\left((1+o(1))\sqrt{\log n \log \log n}\right))$
Метод решета числового поля	$T(N) = O(n \log n \log N)$
Метод Шора	$T = O(\log_3 M)$
Решение проблемы дискретного логарифмирования	
Название	Сложность
Метод Адлемана	$T = O(c^{\ln p^{\frac{1}{2}}})$
Метод COS	$T = O(\exp((\log p \log \log p)^{\frac{1}{2}}))$
Метод решета числового поля	$T(N) = O(n \log n \log N)$
Метод Шора	$T = O(\log_3 M)$

Пример вскрытия схем ассиметричного шифрования (RSA, ЭЛЬ-ГАМАЛЯ) и цифровой подписи (DSA, ECDSA или RSA-PSS)



Основные гипотезы предлагаемого способа решения задачи

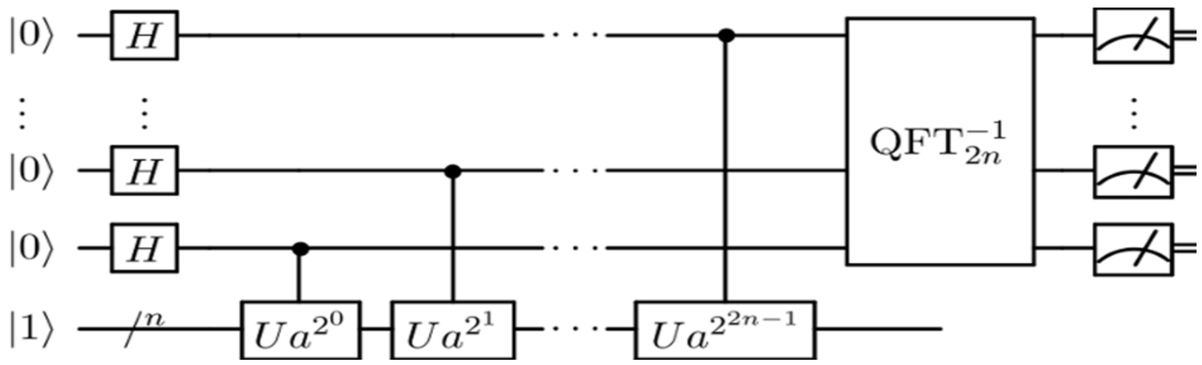


Рисунок. Представление алгоритма Шора в виде последовательности гейтов

1. Алгоритм Шора способен выполнить факторизацию числа за полиномиальное время, на что не способен ни один другой существующий на данный момент алгоритм факторизации.

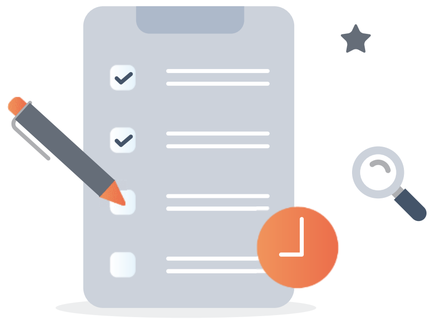
2. Проблема дискретного программирования в квантовом представлении является частным случаем проблемы факторизации, а значит тоже может быть решена за полиномиальное время.

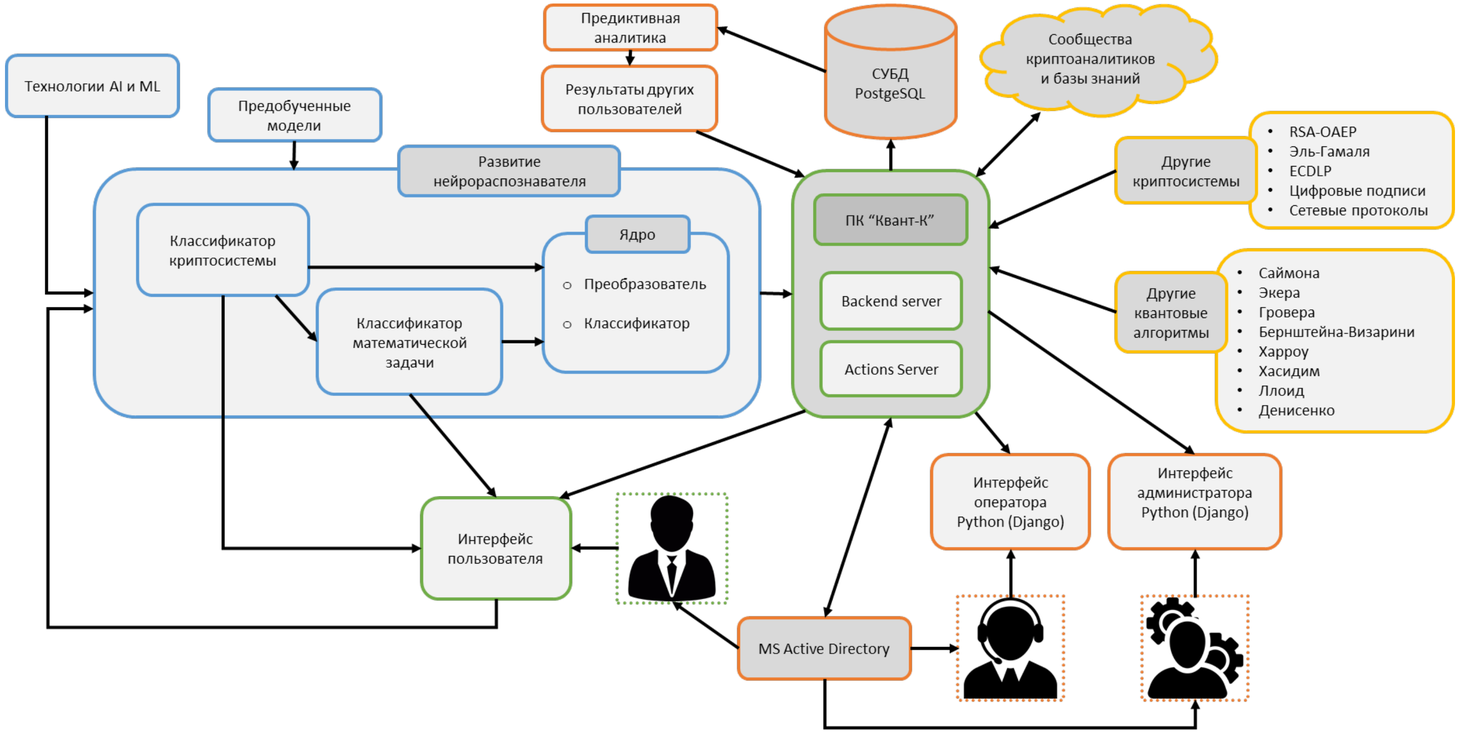
3. Любые алгоритмы устройств с традиционной архитектурой могут быть реализованы на квантовом компьютере, но как правило используют алгоритмы имеющие выигрыш в временной сложности, или иными словами обладающие квантовым превосходством.

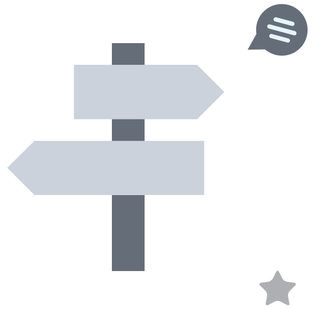
4. Квантовых мощностей современных универсальных квантовых компьютеров может не хватать для решения задач, поэтому целесообразно использовать симуляции квантового компьютера на суперЭВМ.

5. Такого рода рода реализации обладают псевдополиномиальной сложностью, однако сохраняют большое количество преимуществ по сравнению с использованием других известных алгоритмов факторизации.

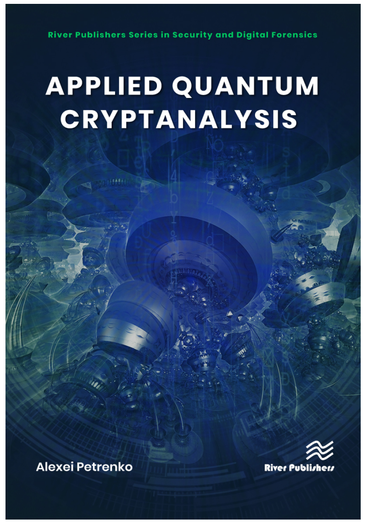
Возможные направления развития программного комплекса Квант-К







1. Подключение нейросетевых распознавателей, отвечающих за распознавание криптосистем и математических задач, связанных между собой
2. Дальнейшая модернизация квантовой части алгоритма Шора, подключение модулей исправления ошибок вычислений
3. Подключение других квантовых алгоритмов, возможность анализа большего количества криптосистем, подключение облачной платформы
4. Подключение службы каталогов, интерфейсов оператора, администратора, СУБД и модуля предиктивной аналитики



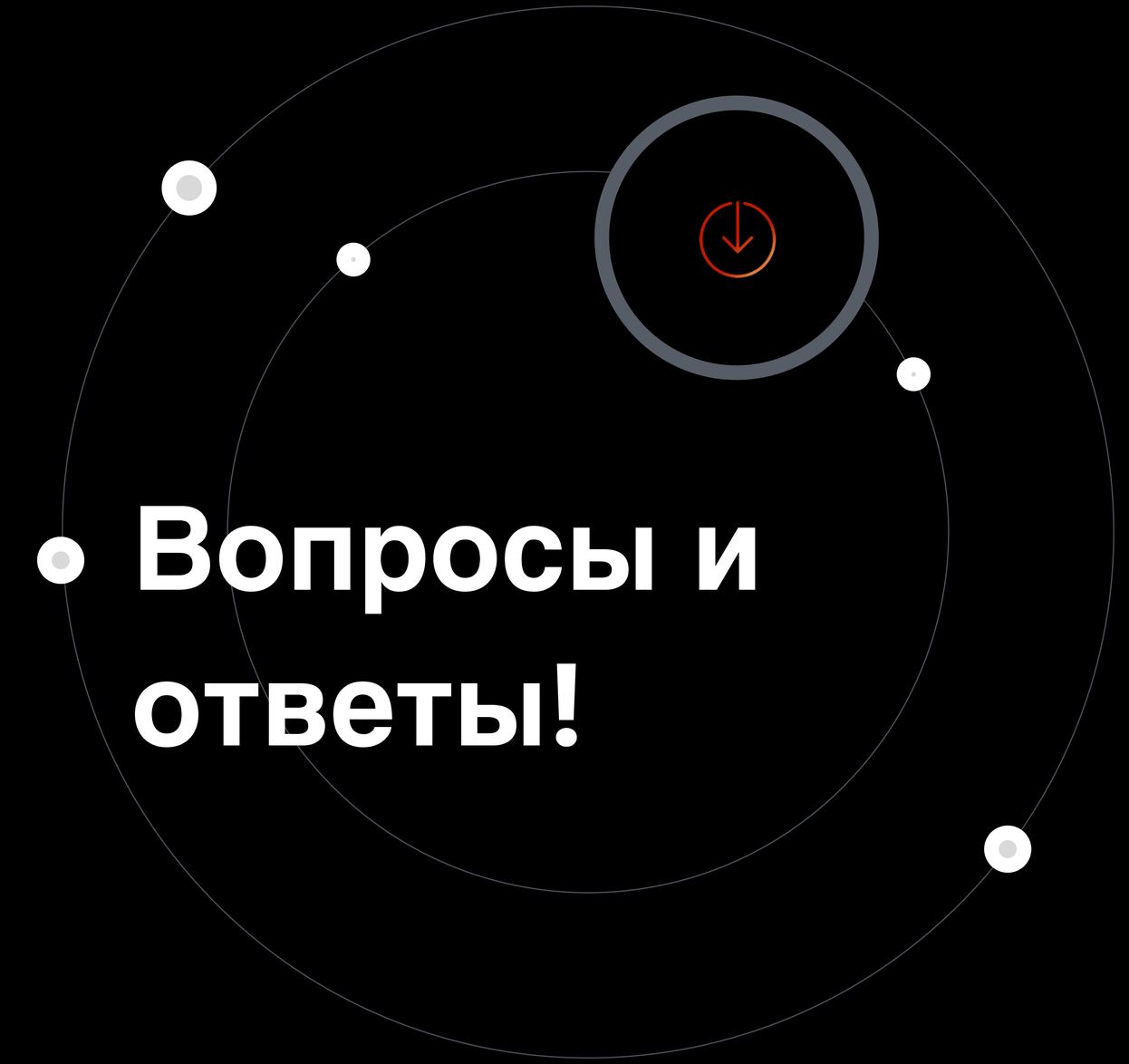
River Publishers Series in Information Science and Technology

Applied Quantum Cryptanalysis

Author: Alexei Petrenko, Editor: Sergei Petrenko, Innopolis University, Russia. — 222 p.:
ISBN: 9788770227933(Hardback) and e-ISBN: 9788770227926(Ebook) © 2022, 1st ed., 222 p. 59 illus. (Scopus).

Квантово-устойчивый блокчейн

Алексей Петренко (научно-популярная монография), ISBN 978-5-4461-2357-5, «Издательский Дом «Питер», 2023. – 320 с.



Вопросы и ответы!