МНИАП

КИБЕРБЕЗОПАСНОСТЬ: ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

Стремительная эволюция квантовых компьютеров создает новый вызов перед специалистами по кибербезопасности. Особенность квантовых вычислений позволяет реализовать алгоритмы, создающие возможность сравнительно быстрого взлома любых паролей, основанных на наиболее распространенных на сегодняшний день алгоритмах шифрования.

Ожидается, что к 2027 году квантовые компьютеры позволят, с высокой вероятностью, взламывать наиболее стойкий и распространенный алгоритм шифрования RSA– 2048 (назван по числу бит – двоичных разрядов).

Термин RSAобозначает так называемые «полупростые числа» - то есть числа, полученные путем перемножения двух простых чисел. Взлом кода, упрощенно, требует найти эти простые числа. В 1991 году был начат конкурс по разложению RSA – чисел на простые множители. На сегодняшний день исследователям удалось разложить числа от RSA – 330до RSA– 768 (по числу бит). Поэтому стойкость шифров, основанных на RSA– 2048, является абсолютной.

Главная проблема в том, что квантовые компьютеры могут очень эффективно решать подобный класс задач, в том числе по обеспечению «квантового превосходства», то есть создания квантового компьютера, мощность которого превосходит любую теоретически достижимую мощность обычных компьютеров. Согласно расчетам, для этого требовалось создать 50-кубитный (кубит – квантовый бит). Текущий рекорд принадлежит IBM – 72 кубита.

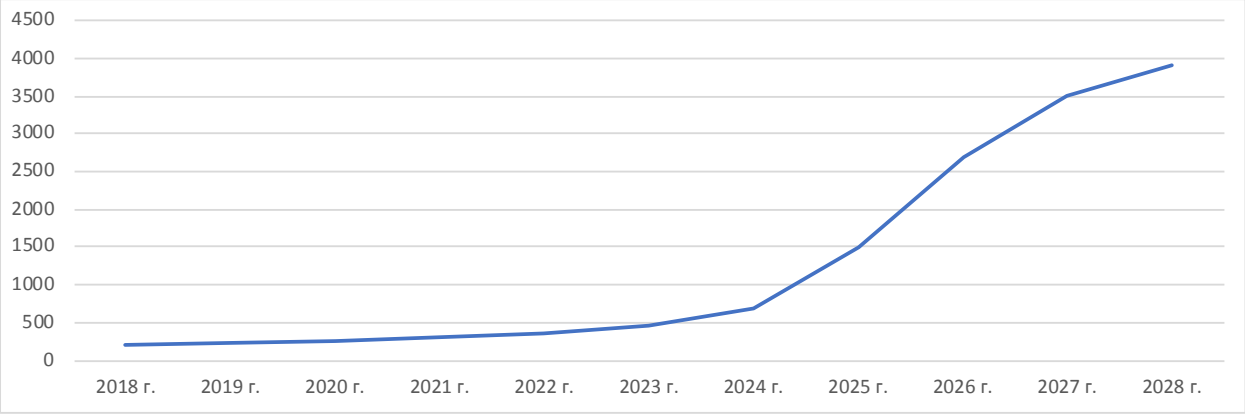
Проблема аппаратной реализации существующих кубитов – в низкой стабильности, высоком «зашумлении» информации. Это пока не позволяет полностью реализовать потенциал существующих квантовых компьютеров, но и здесь наблюдается значительный прогресс.

Решением проблемы риска квантового взлома существующих систем криптографии является переход на другие алгоритмы шифрования. Ряд наиболее перспективных алгоритмических основ для постквантовой криптографии:

- Алгоритмы решетчатой криптографии: в настоящее время разработано около 10 различных алгоритмов. Исследования активно продолжаются и поддерживаются, в том числе на государственном уровне (Европейская комиссия);
- Многомерная криптография: несколько предложенных решений оказались нестойкими к взлому, но ожидается, вариант многомерной цифровой подписи, использующий алгоритм «Радуга», может стать основой для перспективной квантово-стойкой цифровой подписи;
- Кеш-криптография. Изобретена в 1970 году. Интерес к этому решению вернулся после осознания рисков взлома шифров с использованием квантовых компьютеров;
- Другие алгоритмы: код с коррекцией ошибок, изогенная эллиптическая кривая, системы с симметричным ключом и др.

В целом ожидается, что объем рынка постквантовой криптографии вырастет к 2028 году до $3,9 млрд. Текущий размер – около $ 200 млн.

Прогноз динамики мирового рынкапостквантовой криптографии, $ млн.



Источник: Inside Quantum Technology

Важно, что уже сейчас на рынке постквантовой криптографии ведутся «патентные войны»: разрабатываемые алгоритмы патентуются авторами, а крупные компании формируют пулы патентов, закрывающие наиболее перспективные направления от конкурентов.

Для малого бизнеса текущая ситуация на рынке – отличная возможность для разработки и продвижения собственных высокоинтеллектуальных продуктов.