Квантовая угроза безопасности технологии блокчейн

105 стр. | PDF | 2022 г.

Сегодня мы наблюдаем рост внимания к технологии блокчейн и распределенного реестра (*Distributed Ledger Technology*, DLT), которая является одной из ключевых сквозных технологий Цифровой экономики Российской Федерации. Однако большинство криптопримитивов, применяемых в блокчейне, в том числе хеш-функции (ГОСТ Р 34.11-2018, SHA-2, SHA-3, SHA256, Ethash, SCrypt, X11, Equihash, RIPEMD160 и др.), электронные подписи (ГОСТ 34.10-2018, ECDSA, EdDSA, Ring, One-Time, Borromean, Multi-signature и др.), асимметричные криптографические алгоритмы (RSA, Диффи-Хеллмана и др.) и соответствующие протоколы уже не являются квантово-устойчивыми, то есть устойчивыми к атакам с использованием так называемого релевантного или значимого квантового компьютера (англ. Cryptographically Relevant Quantum Computer, CRQC). Сегодня уже известны эффективные квантовые алгоритмы, в частности, алгоритм Шора для факторизации и дискретного логарифмирования, которые могут быть успешно применены для взлома перечисленных криптопримитивов.

Предложена новая постановка задачи обеспечения киберустойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации в условиях квантовых кибератак злоумышленников на основе авторских моделей и методов. Настоящий материал является первой работой по упомянутой проблеме и содержит результаты не только качественного, но и количественного изучения квантовой устойчивости блокчейн-экосистем и платформ государства и бизнеса. По этой причине пособие представляет несомненный теоретический и практический интерес для специалистов в области компьютерных наук и информационных технологий.