

Квантовые вычисления и крах современной криптографии: когда RSA перестанет защищать

Современная цифровая безопасность построена на математических задачах, которые считаются вычислительно неразрешимыми для классических компьютеров. Алгоритмы RSA, Diffie-Hellman и эллиптические кривые обеспечивают конфиденциальность переписки, целостность транзакций и подлинность цифровых подписей. Однако появление квантовых вычислений ставит под сомнение саму основу этой защиты: задача факторизации больших чисел и дискретного логарифмирования, на которой держится большая часть современной криптографии, перестаёт быть неразрешимой. Речь идёт не о теоретической угрозе далёкого будущего, а о риске, который требует подготовки уже сегодня.

По данным ENISA, квантовые вычисления рассматриваются как один из ключевых факторов, способных изменить ландшафт кибербезопасности в горизонте ближайших десятилетий. Алгоритм Шора, теоретически позволяющий факторизовать большие числа за полиномиальное время, делает RSA уязвимым. Алгоритм Гровера ускоряет перебор симметричных ключей, что требует увеличения длины ключей в два раза. NIST подчёркивает, что переход на постквантовую криптографию – это не техническая модернизация, а стратегическая необходимость, поскольку инфраструктура, защищённая сегодня, может быть скомпрометирована в будущем.

Наиболее опасный сценарий получил название «сначала собери, потом расшифруй». Злоумышленник перехватывает и сохраняет зашифрованные данные сегодня, не имея возможности их расшифровать, но рассчитывая сделать это после появления достаточно мощного квантового компьютера. Для государственных структур, финансовых организаций и медицинских учреждений это означает, что конфиденциальная информация, передаваемая сейчас, может быть раскрыта через пять, десять или двадцать лет. Срок жизни таких данных превышает срок жизни используемых криптографических алгоритмов.

Особенно уязвимы долгоживущие секреты: государственная тайна, персональные данные, интеллектуальная собственность, медицинские записи. Если информация должна оставаться конфиденциальной дольше, чем потребуется на создание квантового компьютера, она уже находится

под угрозой. При этом злоумышленнику не нужно взламывать систему в момент передачи, так как ему достаточно сохранить трафик и дожидаться подходящего момента. Это принципиально меняет модель оценки риска: защита перестаёт быть задачей «здесь и сейчас» и становится вопросом долгосрочного планирования.

Ответом на угрозу стало развитие постквантовой криптографии, то есть алгоритмов, устойчивых как к классическим, так и к квантовым атакам. NIST в 2024 году завершил первый этап стандартизации и утвердил набор алгоритмов, включая CRYSTALS-Kyber для обмена ключами и CRYSTALS-Dilithium, FALCON и SPHINCS+ для цифровых подписей. Эти алгоритмы основаны на иных математических задачах: решётках, кодах, хеш-функциях. Однако их внедрение требует пересмотра всей инфраструктуры: протоколов TLS, сертификатов, аппаратных модулей безопасности и встроенных систем.

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцент Рожков Р.С. отмечает, что миграция на постквантовую криптографию сталкивается с рядом практических проблем. Во-первых, новые алгоритмы требуют больших вычислительных ресурсов и объёмов памяти, что критично для устройств интернета вещей и встроенных систем. Во-вторых, необходимо обеспечить совместимость с существующими протоколами и оборудованием. В-третьих, возникает проблема гибридных схем, когда требуется одновременная поддержка классических и постквантовых алгоритмов на переходном этапе. В-четвёртых, многие организации не осознают срочности задачи, откладывая миграцию до момента, когда она станет неизбежной.

А со слов доцента кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.в.н., доцента Тюрникова А.П., особое значение приобретает инвентаризация криптографических активов: организация должна знать, где и какие алгоритмы используются, какие данные защищаются, как долго они должны оставаться конфиденциальными. Без этого невозможно спланировать миграцию. Важную роль играют криптографическая гибкость, то есть способность системы заменять алгоритмы без полной перестройки, и централизованное управление ключами. Здесь ИИ может стать инструментом поддержки: алгоритмы машинного обучения помогают

выявлять устаревшие протоколы, анализировать конфигурации и приоритизировать системы по степени риска.

Однако полностью полагаться на автоматизацию опасно, так как ошибка в миграции может привести к отказу критических сервисов или созданию ложного ощущения защищённости. В критических сценариях должен сохраняться контроль специалиста.

Таким образом, квантовая угроза не отменяет существующие принципы информационной безопасности, но требует их пересмотра с учётом нового горизонта планирования. Главное изменение – это не скорость атаки, а её отложенный характер: данные, защищённые сегодня, могут быть раскрыты завтра. Современная система безопасности должна учитывать два направления риска: компрометацию данных в будущем и необходимость миграции инфраструктуры уже сейчас.

Рожков Р.С.,

кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Тюрников А.П.,

кандидат военных наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ