**Создание квантовых компьютеров откроет принципиально новые возможности для человечества, но при этом существующие методы защиты информации утратят свою эффективность. Несмотря на то что пока квантовые компьютеры только выходят за пределы лабораторий, потребность в использовании квантово-безопасной, или, как ее еще называют, постквантовой криптографии есть уже сегодня.**

Классическая криптография

Криптография изучает методы защиты конфиденциальности и целостности информации, а также процедуры проверки подлинности (аутентификации). Классическая криптография опирается на математические алгоритмы. Данные, которые пользователи передают по электронной почте, через облачные сервисы или мессенджеры, защищены тем или иным криптографическим протоколом. Каждый из этих протоколов включает в себя набор алгоритмов шифрования, то есть свод правил, определяющих, как именно будет преобразована информация.

Алгоритмы шифрования для данных в цифровом виде можно разделить на два основных типа: симметричные (например, AES) и асимметричные (самый распространенный — RSA). При симметричном шифровании стороны, обменивающиеся данными, используют один и тот же секретный ключ для шифрования и расшифровки данных. Этот ключ не известен третьей стороне, соответственно, она не имеет доступа к данным. Симметричные алгоритмы обычно используются для таких задач, как шифрование больших баз данных, файловых систем и хранилищ.

Асимметричные алгоритмы предполагают использование двух ключей — открытого и закрытого. Эти ключи связаны между собой математическими зависимостями. Для шифрования данных используется открытый ключ, а для их дешифровки — закрытый ключ из той же пары. Такая разновидность асимметричных алгоритмов называется алгоритмами с открытым ключом.

При симметричном шифровании стороны должны иметь общий закрытый ключ еще до начала обмена данными, а при асимметричном — начинают обмен без общей секретной информации: здесь одна сторона (получатель) знает оба ключа и передает второй (отправителю) только открытый ключ.

Многие криптографические протоколы являются гибридными. Начиная обмен информацией, стороны используют алгоритмы с открытым ключом для передачи одной строки, а затем переходят на гораздо более быстрые симметричные алгоритмы, где эта общая строка выступает в качестве секретного ключа.

Уже сегодня компании и пользователи накапливают и хранят данные, которые будут представлять ценность и через пять, десять и даже тридцать лет. Если не позаботиться об их защите сегодня, грядущие успехи в квантовых вычислениях сделают подобную информацию легкодоступной для третьих лиц. Нельзя исключать, что заинтересованные лица могут перехватить информацию сейчас, а расшифровать позднее, когда появится техническая возможность.

Кроме того, нужно учитывать и тот факт, что быстро обновить имеющуюся инфраструктуру будет затруднительно. Инвестируя в создание сетей и хранилищ критически значимых данных, разумно уже сейчас предусмотреть вероятное появление квантовых компьютеров в перспективе. Ведь инфраструктура, которую организация создает сегодня, вероятнее всего будет использоваться еще не одно десятилетие.

представит между 2022 и 2024 годами.

Страховка на случай квантового прорыва

Учитывая текущие успехи исследовательских групп в области квантовых вычислений, коммерческие компании и правительства стран должны задуматься о ценности своих данных. Для защиты информации, которая должна остаться конфиденциальной через 10–30 лет, внедрять квантово-безопасную криптографию рекомендуется уже сегодня, не дожидаясь стандартизации.

Важно понимать, что перейти на постквантовые алгоритмы немедленно после принятия стандартов не удастся. Понадобится большая подготовительная работа. Новые ключи могут иметь несколько большие размеры, и инфраструктура должна быть рассчитана для их передачи без потери привычной скорости коммуникации.

В то же время многие предложения, поданные в NIST,— это лишь незначительные изменения хорошо изученных задач. Можно выбрать одно или несколько из них и использовать в тандеме с текущей криптографией. Такой модульный переход к квантово-безопасной криптографии выглядит наилучшим решением, так как он гарантирует текущую безопасность данных, даже в том случае, если в постквантовых алгоритмах обнаружатся «болезни молодости», связанные с их внедрением в отсутствие универсальных квантовых компьютеров. При этом, внедрив элементы квантово-безопасной криптографии сейчас, собственники данных застрахуют себя на случай грядущего прорыва в квантовых вычислениях.

Сроки хранения конфиденциальных данных

* Записи налогового учета, согласно требованиям закона Сарбейнза—Оксли,— 7–10 лет в большинстве стран
* Срок засекречивания сведений, составляющих гостайну в России,— до 30 лет
* Документы по личному составу в Российской Федерации – не менее 50 лет
* Хранение неактивных банковских счетов, списков всех уничтоженных записей в США — бессрочно
* Чтобы обезопасить интернет-коммуникации, специалисты в области криптографии работают над созданием методов шифрования, которые не смогут обойти квантовые компьютеры будущего. Это значит, что к моменту распространения квантовых компьютеров у человечества в руках будут надежные способы защиты целостности и конфиденциальности данных, а также новые средства и процедуры аутентификации пользователей.