и компанией QRate мы провели демонстрацию квантово-защищенного беспилотного автомобиля. Это важный результат, так как временные горизонты массового появления беспилотников на дорогах совпадают с темпами развития квантовых компьютеров. Поэтому необходимо уже сегодня учитывать квантовую криптографию в тех технических решениях, которые через 5–7 лет будут применяться масштабно. Уже сегодня доступны следующие категории решений:

1. QRate QKD312 – высокоскоростное квантовое распределение ключей. Оборудование использует метод передачи ключей шифрования, основанный на принципах квантовой физики. Установка передает секретный ключ на расстояние до 120 км в заданный период времени, с исключением риска перехвата. Оборудование квантового распределения ключей устанавливается поверх существующей инфраструктуры и работает совместно с предустановленными средствами криптографической защиты информации.

2. QRate Chaos – квантовый генератор случайных чисел. Главное назначение квантового генератора случайных чисел – выдача последовательности числовых данных, в которых текущее число не имеет никакой корреляции с предыдущими значениями. Случайные числа играют важную роль в жизни современного общества. Прежде всего случайность является неотъемлемой составляющей современных криптографических систем, включающих мобильную связь, безналичные платежи, электронную почту, интернет-банкинг и другие. Огромное значение случайность также играет в различных областях науки и техники, которым внедрение стохастических методов дало мощный импульс развития.

3. QRate Lab – учебная квантовая лаборатория. QRate Lab – это комплексный подход к организации учебной квантовой лаборатории.

С ее помощью организации и университеты могут самостоятельно заниматься подготовкой специалистов в области квантовых коммуникаций. Лаборатория оснащена передовым оборудованием, созданным специально для этих задач. Она включает в себя аппаратный научно-образовательный комплекс, программное обеспечение и методические материалы.

4. Другое электронное оборудование. Компания QRate осуществляет поставку различного электронного оборудования для систем фотоники, квантовых систем, систем распределения квантового ключа, научно-образовательных комплексов и других решений[3].

Постквантовая криптография

На российском и международном рынке доступны и решения с постквантовой криптографией, например решения квантово-устойчивой кибербезопасности для блокчейн-экономики, от QApp.

Объем данных стремительно растет, а их ценность увеличивается; более 40% данных блокчейн-проектов нуждаются в усиленной защите; криптографическая защита требует наибольшего внимания; квантовые компьютеры представляют реальную угрозу безопасности блокчейн-проектов.

Новые поколения вычислительных устройств – квантовые компьютеры – за счет принципиально другой схемотехники и логики работы смогут взломать существующие методы защиты информации. В горизонте нескольких лет полностью небезопасными становятся многие традиционные алгоритмы криптографии:

- распределение ключей (ECDH, DH);
- асимметричное шифрование (RSA);
- электронная подпись (ECDSA, DSA, ГОСТ Р 34.10–2012).

Весь мир уже вовлечен в "квантовую гонку". ИТ-гиганты инвестируют сотни миллионов долларов в разработку квантовых компьютеров. Уже сейчас некоторые решения доступны для продажи или через облачный доступ. Международный институт сертификации NIST активно проводит глобальную программу оценки качества квантово-безопасных алгоритмов.

Данные с горизонтом хранения в пять и более лет защищать нужно уже сейчас: злоумышленник может сохранить их и расшифровать с появлением у него доступа к квантовому компьютеру.

Компания QApp уже сегодня предоставляет комплексные решения квантово-устойчивой кибербезопасности для проектов блокчейн-экономики. Их программные продукты реализованы на основе алгоритмов постквантовой криптографии.

Каждое из решений позволяет защитить данные пользователей от атак с использованием квантовых компьютеров. Криптография внутри решений основана на математических алгоритмах, непосильных и для классических, и для квантовых компьютеров. Они предлагают решения как для распределения ключей, так и для электронно-цифровой подписи, а также для инфраструктурных проектов и конечных продуктов блокчейн-экономики. Постквантовые решения не требуют покупки нового дорогостоящего оборудования, как в случае использования квантовой криптографии.

Взлом любого из компонентов блокчейн-инфраструктуры неминуемо ведет к компрометации информации, поэтому все компоненты на различных уровнях должны быть защищены:

- блокчейн-инфраструктура (VPN для нод, квантово-устойчивая аутентификация для нод);
- блокчейн, кошельки (квантово-устойчивый блокчейн, реализация постквантовой подписи для транзакций);
- смарт-контракты (квантово-устойчивые подписи для смарт-контрактов);
- интерфейсы доступа к данным, онлайн-кошельки (квантово-безопасный доступ к данным, защита мобильного доступа, расширение для браузеров, защита десктоп-приложений).

Внутри решений QApp – PQLR SDK (уникальная библиотека квантово-устойчивых алгоритмов компании QApp). Реализована также поддержка различных платформ и портируемость: интеграция в OpenSSL (TLS 1.3, KEM, ЭЦП), поддержка российской хеш-функции ГОСТ Р34.11–2012, регулярные обновления и простота интеграции.

Внутри библиотеки собраны актуальные квантово-устойчивые алгоритмы. Осуществляется регулярное тестирование самых перспективных алгоритмов и добавление их в библиотеку, параллельно ведутся работы над упрощением процесса интеграции. Оптимизируется каждый добавляемый квантово-устойчивый алгоритм без потери надежности.

На сегодня доступны следующие продукты:

1. Qtunnel – передовая защита от квантовой угрозы. Программное решение для создания с клиентами квантово-устойчивого канала передачи данных или в рамках инфраструктуры бизнеса.

2. PQStor – решение для квантово-устойчивого шифрования end-to-end файлов и папок. Пользователь сам выбирает место хранения файлов: локальный компьютер, внешние устройства хранения данных или публичные облака.

3. TAF v2.1 – фреймворк для детектирования атак по времени в криптографических продуктах. Повышение защищенности программно-аппаратных решений.

Компания QApp оказывает полный спектр консультационных услуг по квантово-устойчивым решениям кибербезопасности для компаний блокчейн-экономики:

- комплексный аудит кибербезопасности;
- бенчмаркинг решений квантово-устойчивой кибербезопасности;
- подготовка аналитических заключений и разработка стратегии внедрения квантово-устойчивой кибербезопасности;
- проведение образовательных воркшопов по квантовым технологиям[4].

3 https://goqrate.com/articles/nauchnyy-vzglyad/kak-kvant-menyaet-sovremennyy-mir-k-luchshemu/ – Как квант меняет современный мир к лучшему.

4 https://qapp.tech/pqlr/cases/blockchain – Квантовые блокчейны – решения QAPP для блокчейн-экономики.