

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Квантовая угроза слева

Вероятно, появление квантовых компьютеров, ожидаемое к 2030 году, может произойти раньше. Первыми об этом узнают криптографы, ведь не зря наблюдается шквал интереса к квантовой и постквантовой криптографии

Серия материалов издания Politico «А может ли ЕС хранить секреты?», освещавших кризис доверия в ЕС, связанный с утечками секретной информации и обсуждением ужесточения мер безопасности, уже несколько месяцев приковывает к себе внимание ИБ-экспертов во всем мире.

Главная причина — одна из наиболее закрытых тем, материалы по которой в открытом доступе появляются крайне редко, самым неожиданным образом оказалась предметом многочисленных обсуждений. Эти дискуссии позволяют косвенно ответить на вопрос: «А что у нас?» в контексте другого вопроса: «А что у них в области криптографии?»

Как будет по-английски «импортозамещение»?

По данным Politico в прочтении журналистами «Известий», ситуация выглядит следующим образом: «Послы стран Евросоюза после целого ряда утечек в США документов, представляющих гостайну, теперь регулярно встречаются в специальном "бункере", защищенном от прослушки, чтобы обсудить самые острые вопросы, предварительно ознакомившись с бумажными документами». В частных беседах специалисты объясняют причины.

Во-первых, наличие глобальной системы радиоэлектронной разведки «Эшелон» (ECHELON) в рамках «альянса пяти глаз» (Five Eyes). Она предназначена для перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру, но прежде всего — с территории бывшего СССР. Естественно, что информация, о которой пишет Politico, была зашифрована, но тем не менее, попав в штаб-квартиру Агентства национальной безопасности (АНБ) США, была расшифрована и уже оттуда утекла в руки журналистов.

Во-вторых, несмотря на наличие во Франции (как и в России, и в США) всемирно признанных школ криптографии и не менее признанного вендора средств криптографической защиты информации (СКЗИ), компании Thales, очень много конфиденциальной информации в ЕС шло посредством американского ПО, например Microsoft, Apple, Google и других, с обычным для них шифрованием. Поэтому в ЕС стали активно изучать опыт России в области импортозамещения IT в целом и СКЗИ в частности. Однако проблема состоит в том, что самодостаточной в рассматриваемом сегменте является лишь Франция, а в ЕС, как известно, 27 государств.

В-третьих, поскольку документы были расшифрованы, это означает, что в АНБ помимо

классических суперкомпьютерных мощностей уже работают квантовые компьютеры, иначе трудно объяснить, чем были заняты специалисты Thales.

Ответов на множество вопросов пока нет, зато есть намеки, а также те, кто сами проявили себя как потенциальные жертвы «квантов». А главное, была названа примерная цена вопроса.

Цена вопроса — 5,6 млн BTC

Утро 13 апреля 2026 года положило начало бурному обсуждению в криптосообществе BIP-361, предложения, которое может изменить фундаментальные правила владения биткоином. Поводом для обсуждения стала публикация в марте «технической белой книги» Google Quantum AI, которая радикально сдвинула оценку сроков появления квантовой угрозы влево. Согласно анализу исследователей, под угрозой атаки со стороны квантовых вычислений сегодня находятся около трети циркулирующего предложения биткоина.

BIP-361 (Bitcoin Improvement Proposal) предполагает поэтапный отказ от использования биткоин-адресов, уязвимых для квантовых атак. Основная идея — заморозить средства на таких адресах и предоставить владельцам механизм миграции на новые, квантово-устойчивые адреса с помощью доказательств с нулевым разглашением (Zero-Knowledge Recovery).

BitMEX Research, исследовательское подразделение криптобиржи BitMEX, 15 апреля 2026 года предложила мировому криптосообществу альтернативный механизм для смягчения последствий возможной заморозки биткоинов. Механизм с «канареечным фондом» добавляет сложности, но может снизить негативные последствия для пользователей и экосистемы биткоина. Механизм рассматривается как альтернатива или дополнение к BIP-361.

Уже на следующий день, 16 апреля 2026 года, основатель блокчейн-платформы Cardano **Чарльз Хоскинсон** заявил, что BIP-361 ошибочно обозначен как софт-форк и что его план восстановления с нулевым разглашением не может спасти примерно 1,7 млн BTC, созданных до 2013 года.

Из-за чего, собственно, разгорелся этот сыр-бор? Известно, что **Джеймсон Лопп,** по данным портала coindesk, ведущий разработчик и соавтор BIP-361, утверждал, что заморозка неактивных монет, количество которых он оценивает в 5,6 млн BTC, «предпочтительнее, чем позволять будущему квантовому атакующему получить к ним доступ и сбросить их на рынок».

Помимо финансового вопроса виден спор о будущей архитектуре самих крупнейших открытых блокчейн-сетей. Обсуждение BIP-361 вновь подняло вопрос о допустимости вмешательства в протокол биткоина. Многие эксперты проводят здесь аналогии с хардфорком Ethereum после взлома DAO в 2016 году, который разделил сеть и вызвал споры о принципах децентрализации. То есть вопрос не только в «квантах».

Криптосуверенитет

Пока эксперты спорят о сумме потерь и юридической чистоте, вполне уместно отметить: «А ведь их предупреждали!» И не кто-нибудь, а представители Ассоциации ФинТех (АФТ), которая в сентябре 2025 года представила шестой выпуск аналитического фреймворка «Финтех-Радар», посвященный постквантовой криптографии и квантово-устойчивой защите данных финансовой отрасли России. В документе было отмечено: «Примерно к 2030 году квантовые компьютеры могут стать достаточно мощными для взлома текущих криптоалгоритмов». Похоже, и эти цифры придется сдвигать влево…

Однако при этом установлено, что оптимальным методом защиты данных от квантовой угрозы являются постквантовые алгоритмы. Это новый класс асимметричных алгоритмов шифрования, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров. Постквантовая криптография может быть легко интегрирована с серверной инфраструктурой, системами аутентификациии, мобильными и веб-сервисами.

Об этом говорили и на научно-практической конференции «РусКрипто'2026», прошедшей в конце марта в Подмосковье. В частности, **Андрей Елистратов,** советник Управления методологии и стандартизации ИБ и киберустойчивости департамента информационной безопасности Банка России, заявил: «Обеспечение ИБ кредитно-финансовой сферы невозможно без устойчивых криптографических механизмов. Переход финансовых организаций на отечественные криптографические стандарты — важнейший этап обеспечения технологического суверенитета отрасли».

Если перейти от слов к делу, то на фоне возможных потерь владельцев сети Биткоин масштабный проект отечественного платежного гиганта НСПК во исполнение требований Банка России, зафиксированных в его Положении № 821-П от 17.08.2023, в частности в п. 5.6, касающемся операторов значимых платежных систем, вовсе не выглядит дорогостоящим и бесполезным.

В ходе XIII Технологической конференции НСПК, прошедшей 23 июня 2025 года в Москве, **Игорь Голдовский,** главный архитектор и директор департамента инноваций НСПК, заявил: «К 1 января 2031 года необходимо, чтобы на нашем рынке появились терминалы и карты, работающие на базе в том числе и отечественной криптографии».

В ходе «РусКрипто'2026» НСПК еще раз подняла этот вопрос. А вот представителю финансового регулятора досталась куда более сложная и актуальная тема: «Задачи, решаемые Банком России в рамках использования СКЗИ в проекте цифровой рубль».

Понятно, что затрагиваемые вопросы довольно чувствительны, но широкой общественности в Банке России дали четко понять: «Криптография становится основой цифрового суверенитета». Б.О