ВЭФ бьёт тревогу, призывая центральные банки уже сейчас подготовиться к кибервызовам будущего.

Всемирный экономический форум (ВЭФ) недавно выступил с предупреждением о возможной уязвимости цифровых валют центральных банков (Цифровые валюты центральных банков (CBDC) – это цифровые формы национальных валют, выпущенные и контролируемые центральными банками. Они представляют собой официальное платежное средство, которое функционирует как цифровой аналог традиционных бумажных денег и монет. CBDC могут использоваться для проведения платежей и переводов, обеспечивая высокую степень безопасности и эффективности транзакций." data-html="true" data-original-title="CBDC" >CBDC) перед атаками квантовых компьютеров.

На сегодняшний день квантовые компьютеры остаются в основном экспериментальными. Хотя существуют различные доказательства концепции, и несколько лабораторий ранее заявляли о решении с их помощью специфических задач, которые традиционные компьютеры не могут решить в разумные сроки, до наступления гипотетического «Q-Day», момента, когда злоумышленники смогут взломать стандартное шифрование с помощью квантовых компьютеров, ещё есть время.

Тем не менее, потенциальные угрозы для традиционных методов шифрования могут затронуть все отрасли и особенно плачевно сказаться на сфере цифровых активов. Согласно предположениям ВЭФ, эта угроза может буквально уничтожить цифровые валюты CBDC.

В своём блоге представители ВЭФ написали 21 мая, что «центральные банки должны встроить криптографическую гибкость в системы CBDC для защиты от квантовых кибератак, нацеленных на платёжную инфраструктуру».

В посте также упоминается, что «более 98% центральных банков мировой экономики исследуют возможности CBDC. В то же время частный сектор разрабатывает масштабируемые квантовые компьютеры, которые смогут создать $1,3 трлн стоимости к 2025 году».

Среди учёных нет единого мнения о том, когда квантовые компьютеры достигнут уровня, на котором их мощность и доступность станут угрозой для текущих методов шифрования. Прогнозы варьируются от нескольких лет до десятилетий.

ВЭФ выделил три конкретные угрозы, которые квантовые компьютеры могут представлять для CBDC:

Чтобы смягчить или устранить все эти угрозы, ВЭФ рекомендует центральным банкам уже сейчас создавать CBDC со встроенной защитой от квантовых атак, используя методологии «криптографической гибкости».

Согласно ВЭФ, «криптографическая гибкость» — это способность легко координировать и менять криптографические алгоритмы в зависимости от актуальных угроз в реальном времени, чтобы эффективно противостоять развивающимся атакам.

Таким образом, центральные банки должны уже сейчас адаптировать свои системы к новым угрозам и активно развивать защитные меры, чтобы обеспечить безопасность цифровых валют в будущем.