# ЗАЩИТА ДАННЫХ В ЭПОХУ КВАНТОВЫХ КОМПЬЮТЕРОВ: ВАЖНОСТЬ ПЕРЕХОДА НА ПОСТКВАНТОВУЮ КРИПТОГРАФИЮ

М.А. Наумов

*Государственное предприятие «НИИ ТЗИ», г. Минск, Республика Беларусь*

В настоящее время сложно представить передачу конфиденциальной информации между информационными системами без применения средств криптографической защиты информации. Совместное использование симметричных и асимметричных криптографических алгоритмов позволяет обеспечивать защиту передаваемых данных с заданным уровнем стойкости. Однако не все принимают во внимание возрастающую угрозу применения квантовых компьютеров для атак на уязвимые криптографические алгоритмы асимметричного шифрования, выработки и проверки электронной цифровой подписи.

Современная криптография подразумевает использование «дорогих» асимметричных алгоритмов только для проверки подлинности сертификата и выработки общего сеансового ключа, который используется при шифровании основного объема данных с помощью симметричной криптосистемы.

Несмотря на то, что симметричные алгоритмы не являются уязвимыми для атак с применением квантовых компьютеров сами по себе, существует возможность раскрытия сеансовых ключей, с помощью атак на уязвимые асимметричные алгоритмы. Поэтому целесообразно инициировать постепенный переход на использование постквантовых алгоритмов.

Наиболее важно начинать внедрение постквантовых алгоритмов в тех областях, где информация сохраняет актуальность долгое время. Это любые пользователи и операторы конфиденциальной информации с длительным жизненным циклом:

– государственная и иная охраняемая законом тайна;
– коммерческая тайна;
– персональные данные;
– медицинские данные;

– промышленные ноу-хау.

Для других областей этот класс атак менее критичен, так как через условные десять лет информация потеряет свою актуальность. Но, скорее всего, в течение ближайших пяти–восьми лет мы увидим переход на квантово-устойчивые решения по всему миру для защиты от новых угроз. Множество систем, использующих классические асимметричные алгоритмы, могут стать уязвимыми уже в ближайшие несколько лет.

В настоящее время в США с июля 2022 года по итогам NIST (National institute of standards and tecnology) были отобраны несколько постквантовых алгоритмов с открытым ключом, а с ноября 2022 года был инициирован переход на постквантовую криптографию для всех внутренних агенств в течении 2023 года.

**Список литературы**

1. NIST [Электронный ресурс]. – 2023. – Режим доступа: https://csrs.nist.gov/projects/post-quantum-cryptography – Дата доступа: 05.04.2023.

2. Migrating to Post-Quantum Cryptography [Электронный ресурс]. – November 18, 2022. – Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf – Дата доступа: 8.04.2023