Готовність IT-інфраструктури до епохи квантових обчислень

УДК 621.395.7 (043.2)

Павло Воробець[1]

Національний університет "Львівська політехніка", [1]pavlo.a.vorobets@lpnu.ua

Стрімкий розвиток квантових обчислень формує новий клас загроз для сучасної IT-інфраструктури. Ключовою проблемою є потенційна здатність квантових алгоритмів, зокрема алгоритму Шора, ефективно розв'язувати задачі факторизації великих чисел та обчислення дискретного логарифму, що лежать в основі більшості сучасних криптографічних систем. У результаті під загрозою опиняються базові механізми захисту інформації, які використовуються в IT-інфраструктурі, включаючи протоколи TLS, VPN-з'єднання, інфраструктуру відкритих ключів (PKI), а також системи управління ідентифікацією та доступом. Компрометація цих механізмів може призвести до порушення конфіденційності, цілісності та автентичності даних.

Додаткову небезпеку становить сценарій "harvest now, decrypt later", за якого зашифровані дані можуть накопичуватися зловмисниками з метою їх подальшого розшифрування після досягнення достатнього рівня розвитку квантових технологій. Це особливо критично для даних із тривалим життєвим циклом, таких як фінансова, медична або державна інформація [1]. Незважаючи на усвідомлення потенційних ризиків, рівень готовності сучасної IT-інфраструктури до квантових загроз залишається низьким. Більшість організацій продовжує використовувати криптографічні алгоритми, стійкість яких базується на обчислювальній складності задач, вразливих до квантових алгоритмів.

Однією з ключових проблем є відсутність повної інвентаризації криптографічних залежностей в інфраструктурі. У багатьох випадках організації не мають чіткого розуміння, де саме і яким чином використовуються криптографічні механізми — у протоколах передачі даних, внутрішніх сервісах, API, системах зберігання або сторонніх рішеннях. Додатковим ускладненням є висока ступінь інтегрованості криптографії в IT-системи. Криптографічні механізми часто жорстко вбудовані в архітектуру застосунків, мережевих сервісів і платформ, що суттєво ускладнює їх заміну або оновлення без впливу на працездатність систем. Також значним обмеженням є відсутність практичного досвіду впровадження постквантових алгоритмів у продуктивних середовищах. Хоча відповідні стандарти вже розробляються, їх інтеграція в існуючі IT-ландшафти потребує часу, ресурсів і зміни підходів до проектування безпеки. У сукупності ці фактори свідчать про те, що більшість сучасних IT-інфраструктур не готова до швидкої адаптації в умовах появи квантових загроз, що підвищує ризики для довгострокового захисту даних [2].

Квантові обчислення по-різному впливають на криптографічні алгоритми залежно від їх типу. Найбільш критичний вплив спостерігається для асиметричних алгоритмів, таких як RSA, ECC та Diffie–Hellman. Їх безпека базується на складності задач факторизації великих чисел та обчислення дискретного логарифму, які можуть бути ефективно розв'язані за допомогою

квантових алгоритмів. Це означає, що у разі появи масштабованих квантових комп'ютерів такі алгоритми можуть бути повністю скомпрометовані.

Натомість симетричні алгоритми шифрування, зокрема AES, є менш вразливими до квантових атак. Використання алгоритму Гровера дозволяє лише квадратично прискорити перебір ключів, що фактично зменшує ефективну довжину ключа вдвічі. У практичному вимірі це означає необхідність переходу на довші ключі (наприклад, використання AES-256 замість AES-128) для збереження належного рівня безпеки [3]. Подібний підхід застосовується і до криптографічних хеш-функцій. Квантові алгоритми знижують їх стійкість до пошуку колізій, однак не призводять до повної компрометації. Відповідно, підвищення рівня безпеки досягається шляхом використання хеш-функцій із більшою довжиною вихідного значення.

З огляду на зазначені ризики, ключовим завданням є підготовка IT-інфраструктури до поступового переходу на квантово-стійкі механізми захисту. Одним із базових принципів такої підготовки є впровадження підходу crypto-agility — здатності систем гнучко змінювати криптографічні алгоритми без суттєвих змін архітектури. Першочерговим кроком є інвентаризація криптографічних залежностей, включаючи TLS, VPN, PKI, API та системи управління секретами. Це дозволяє визначити критичні компоненти інфраструктури та пріоритети їх модернізації. Важливим аспектом є централізоване управління ключами та сертифікатами, що спрощує їх ротацію та подальший перехід на нові алгоритми. Додатково доцільним є впровадження гнучких конфігурацій безпеки, зокрема підтримки змінюваних криптографічних наборів і гібридних рішень.

У висновку слід зазначити, що підготовка до квантової епохи не є одноразовим заходом, а тривалим процесом трансформації IT-інфраструктури. Впровадження принципів гнучкості, централізації управління криптографією та поступової міграції дозволить знизити ризики та забезпечити стійкість систем у майбутньому.

1. Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. – 2022. – Vol. 15. – Article 100242.
2. Воробець П. А., Горпенюк А. Я., Опірський І. Р. Перехід до постквантових криптографічних систем: виклики, стандартизація та перспективи // Безпека інформації. – 2024. – Т. 30, № 2. – С. 306–315
3. Alagic G., et al. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545. – 2025. – 54 p.

З історії становлення національної системи захисту інформації. 1992–1999 рр.

УДК 94:35.083.8(045)

Валерій Ворожко

СБ України, wp06vv@gmail.com