НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА СИСТЕМНОГО АНАЛІЗУ

УДК: 004.056.5

І.Д. ГОРБЕНКО
Харківський національний університет ім. В.Н. Каразіна;
АТ «Інститут інформаційних технологій», Харків, Україна,
e-mail: *i.d.gorbenko@karazin.ua*.

С.О. КАНДІЙ
Харківський національний університет імені В. Н. Каразіна;
АТ «Інститут Інформаційних технологій», Харків, Україна,
e-mail: *sergeykandy@gmail.com.*

НАЦІОНАЛЬНІ ТА МІЖНАРОДНІ ПОСТКВАНТОВІ СТАНДАРТИ АСИМЕТРИЧНИХ ПЕРЕТВОРЕНЬ

Анотація. Проаналізовано сучасний стан та перспективи стандартизації постквантових алгоритмів асиметричних криптографічних перетворень на національному та міжнародному рівнях. Розглянуто основні причини переходу до постквантової криптографії, зокрема потенційні загрози з боку квантових комп'ютерів наявним криптографічним алгоритмам (RSA, ECC тощо). Наведено огляд конкурсу NIST з вибору стандартів для постквантових механізмів інкапсуляції ключів (KEM) та електронного підпису, а також детально описано алгоритми, вибрані для стандартизації (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+ та HQC). Проаналізовано роль організацій ISO/IEC, ETSI, а також групи IETF у формуванні міжнародних стандартів та рекомендацій. Окрему увагу приділено українським національним стандартам та ініціативам, зокрема алгоритмам «Скеля» та «Вершина», їхнім особливостям та перспективам інтеграції у міжнародні стандарти. Стаття дає розуміння важливості та складності процесу переходу до квантово-стійких алгоритмів й окреслює подальші кроки для успішного впровадження постквантової криптографії.

Ключові слова: постквантова криптографія, механізми інкапсуляції ключів, електронні підписи, стандартизація.

ВСТУП

Постквантова (квантово-стійка) криптографія — це напрям криптографії, в межах якого розробляють алгоритми, стійкі до зламу за допомогою квантових комп'ютерів [1]. Сучасні загальновживані алгоритми асиметричної криптографії (RSA, протокол Діффі–Геллмана, алгоритми на основі еліптичних кривих) ґрунтуються на задачах факторизації або дискретного логарифму, які квантовий комп'ютер зможе розв'язувати експоненційно швидше завдяки алгоритмам Гровера, Шора та їхнім узагальненням [2]. Незважаючи на те, що потужних квантових машин поки що немає, швидкість відповідних досліджень підвищується, що свідчить про потребу в терміновому впровадженні квантово-стійких алгоритмів, оскільки дані, зашифровані сьогодні, можуть бути збережені та розшифровані у майбутньому.

Через це відбувається проактивний перехід на квантово-стійкі алгоритми, що супроводжується активною роботою міжнародних і національних організацій зі стандартизації криптографічних засобів. Створення єдиних стандартів для постквантових асиметричних перетворень набуває особливої актуальності, оскільки воно забезпечує узгодженість криптографічних рішень між різними країнами та