ВПЛИВ BSI НА ЄВРОПЕЙСЬКУ СТРАТЕГІЮ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Мельникова О.А., Грасмік С.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток квантових обчислень є загрозою для сучасних криптографічних механізмів, що ґрунтуються на складності факторизації або обчислення дискретного логарифму. Квантові комп'ютери мають потенціал виконувати обчислення, які є практично недосяжними для класичних систем. Наприклад, алгоритм Шора за поліноміальний час факторизує великі числа або знаходить дискретний логарифм [1, 2]. Це потенційна вразливість для багатьох криптографічних алгоритмів — зокрема, для RSA та ECC, які використовуються у цифрових підписах, сертифікатах і протоколах безпеки TLS. Саме через це BSI (Федеральне відомство з безпеки інформаційних технологій Німеччини) визначає одним із пріоритетів розроблення та впровадження стандартів постквантової безпеки [3].

Метою доповіді є узагальнення підходів BSI щодо забезпечення постквантової стійкості інформаційних систем та аналіз впливу BSI на європейську політику стандартизації криптографії. **В доповіді** розглянуто особливості переходу від класичних до постквантових криптографічних рішень, визначені в сучасних технічних настановах і рекомендаціях BSI. Зокрема, в оновлених німецьких вимогах до криптографічних засобів запропоновано поетапне виведення з використання класичних алгоритмів (RSA, DSA, ECC) та впровадження квантово-стійких систем на основі решіткових перетворень, наприклад, FrodoKEM, Classic McEliece, ML-KEM (Kyber) і SPHINCS+ [1, 2]. Ці алгоритми були оцінені за показниками швидкодії, використання пам'яті та сумісності з чинними протоколами, що дає змогу забезпечити безпечний перехід до постквантових рішень без радикальної перебудови IT-інфраструктури. Впровадження цих алгоритмів забезпечує необхідний рівень безпеки для довготривалого збереження конфіденційних даних і сумісність із чинними протоколами безпеки. Основою для вибору цих алгоритмів є результати наукових досліджень, проведених для BSI у рамках проєкту [4], де обґрунтовано доцільність використання решіткових криптосистем як базових постквантових рішень.

Окрім решіткових криптосистем, BSI також розглядає кодові (code-based) та гібридні підходи як потенційно надійні варіанти для окремих сценаріїв застосування. Як зазначено в документі [2] (криптографічні методи: рекомендації та довжини ключів), жоден окремий алгоритм не є універсальним для всіх типів даних чи середовищ, тому рекомендується підтримувати кілька альтернативних постквантових рішень. Такий підхід підвищує стійкість національної інфраструктури до майбутніх технологічних ризиків і забезпечує гнучкість під час переходу до нових стандартів безпеки.

BSI особливо наголошує на принципі криптографічної гнучкості (crypto-agility) — здатності інформаційних систем швидко змінюватися відповідно до

нових криптографічних стандартів. Такий підхід дає змогу поєднувати класичні та постквантові механізми на перехідному етапі, зокрема у формі гібридних криптографічних систем. У них поєднуються класичні та постквантові підписи (наприклад, ECDSA зі SPHINCS+ або XMSS), що забезпечує перевірку достовірності даних двома незалежними алгоритмами та підвищує загальну стійкість системи на час перехідного періоду [1].

У межах європейської співпраці BSI активно бере участь у розробці спільних рішень щодо переходу до постквантової криптографії. Зокрема, німецькі рекомендації лягли в основу спільної позиції органів кібербезпеки ЄС [5], які координують впровадження нових стандартів після завершення процесу стандартизації постквантових алгоритмів, ініційованого NIST. Такий підхід забезпечує узгодженість національних стратегій і сприяє створенню єдиної безпекової інфраструктури в європейському цифровому просторі. BSI також проводить практичні тестування/оцінювання алгоритмів у середовищах із обмеженими ресурсами, зокрема для застосування в IoT-пристроях [2]. Їх результати підтвердили, що алгоритми Kyber і SPHINCS+ можуть ефективно працювати навіть на малопотужних вбудованих системах, що важливо для інтеграції в інфраструктуру “розумних” пристроїв.

Дослідження за підтримки BSI щодо ринку криптографії та квантових обчислень [6] свідчать: більшість німецьких підприємств вже відчувають потребу переходу на квантово-стійкі рішення, але впровадження поступове через високу складність міграції наявних систем.

Таким чином, діяльність BSI визначає як національний, так і європейський напрямок розвитку постквантової криптографії. Поєднання нормативного, технічного та практичного підходів дає можливість створювати цілісну стратегію переходу до нової моделі інформаційної безпеки в умовах квантових технологій.

Список літератури

1. Bundesamt für Sicherheit in der Informationstechnik. *Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI.* — Bonn: BSI, 2020.

2. Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* (BSI TR-02102-1, Version 2025-01). — Bonn: BSI, 2025.

3. Bundesamt für Sicherheit in der Informationstechnik. *Kryptografie quantensicher gestalten.* — Bonn: BSI, 2023.

4. Buchmann J., Dahmen E., Hülsing A. *Gitterbasierte Verfahren.* — Darmstadt: TU Darmstadt, 2017. — (BSI-Studie).

5. European PQC Partnership. *Joint Statement on the Transition to Post-Quantum Cryptography.* — 2025. — URL: https://pqcpartnership.eu/joint-statement (дата звернення: 15.10.2025).

6. KPMG & Bundesamt für Sicherheit in der Informationstechnik. *Marktumfrage Kryptografie und Quantencomputing.* — Berlin: KPMG, 2023.