УДК 004.056

***Щур Н. О., ст. викладач***
*Державний університет «Житомирська політехніка»*

## КРИПТОГРАФІЧНА ГНУЧКІСТЬ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи працюють в умовах постійної зміни криптографічних вимог. Розвиток криптоаналізу, зростання обчислювальних можливостей і підготовка до постквантового переходу роблять недостатнім підхід, за якого криптографічні алгоритми жорстко вбудовані в прикладну логіку, протоколи або апаратні компоненти. Показово, що NIST уже затвердив три перші стандарти постквантової криптографії – FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) і FIPS 205 (SLH-DSA), а в березні 2025 року додатково обрав HQC як резервний алгоритм для майбутнього стандарту шифрування. Це свідчить, що проблема заміни криптографічних примітивів уже є практичним завданням для розробників, адміністраторів і власників цифрової інфраструктури.

У документах NIST криптографічна гнучкість (crypto agility) визначається як здатність замінювати й адаптувати криптографічні алгоритми в протоколах, застосунках, програмному забезпеченні, апаратурі, мікропрограмному забезпеченні та інфраструктурі без втрати безпеки й без порушення безперервності роботи системи [1]. Такий підхід варто розглядати не як окрему технічну функцію, а як архітектурну властивість інформаційної системи. Вона передбачає, що криптографія має бути винесена на рівень керованих сервісів, політик і стандартних інтерфейсів, а не залишатися набором ізольованих рішень у різних компонентах.

Основою криптографічної гнучкості є належне управління криптографічними ризиками. NIST рекомендує інтегрувати криптографічну гнучкість у систему управління інформаційною безпекою, проводити інвентаризацію криптографічних активів, застосовувати автоматизовані засоби виявлення алгоритмів і довжин ключів, визначати пріоритети переходу та централізовано впроваджувати криптографічні політики. Водночас слід враховувати залежності від постачальників, програмних бібліотек, апаратних засобів захисту ключів, хмарної інфраструктури та мережевих протоколів, оскільки недостатня гнучкість навіть одного елемента ланцюга постачання може унеможливити перехід усієї системи.

Для сучасних інформаційних систем особливе значення мають кілька практичних вимог. Передусім необхідно забезпечити взаємосумісність під час переходу між алгоритмами, адже певний час нові й застарілі механізми співіснуватимуть. Крім того, механізми узгодження алгоритмів у протоколах мають бути захищені від атак примусового зниження рівня захисту, інакше зловмисник може нав’язати слабший криптографічний набір. Архітектура системи також повинна враховувати, що постквантові ключі, підписи та шифротексти часто мають більший розмір, ніж традиційні, що впливає на сертифікати, мережеві протоколи, сховища даних і продуктивність. У перехідний період можливе застосування гібридних схем, які поєднують класичні та постквантові механізми, однак це ускладнює систему і потребує чіткого плану подальшої повної міграції.

Актуальність криптографічної гнучкості підтверджується також практичними дорожніми картами міграції [2]. Зокрема, NCSC у 2025 році запропонував етапний підхід до переходу на постквантову криптографію – до 2028 року провести повне виявлення залежностей і підготувати первинний план, до 2031 року виконати ранні пріоритетні міграції, а до 2035 року завершити перехід основних систем, сервісів і продуктів. Хоча ці строки не є універсальними для всіх країн і секторів, сама логіка такого підходу є показовою: спочатку інвентаризація, далі пріоритезація, після цього керована технічна заміна.

Отже, криптогнучкість у сучасних інформаційних системах є не додатковою перевагою, а необхідною умовою довгострокової кіберстійкості. Система, що не підтримує швидку й контрольовану заміну криптографічних механізмів, накопичує технічний борг і стає вразливою до нових типів атак, регуляторних змін та технологічних зсувів. Тому під час проєктування нових інформаційних систем доцільно закладати модульність криптографічних сервісів, централізоване керування політиками, інвентаризацію криптографічних залежностей і готовність до багатоетапних міграцій.

**Список використаних джерел**

1. Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W. and Kent, K. (2025), Considerations for Achieving Crypto Agility: Strategies and Practices, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, URL: https://doi.org/10.6028/NIST.CSWP.39.

2. Timelines for migration to post-quantum cryptography – NCSC.GOV.UK, URL: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.