Обчисливши значення початкових залишків, відкритий текст можна відновити за допомогою КТЗ по модулях $p_{1i}$. Якщо змінити більше одного модуля, то при розшифруванні потрібно буде розв'язати систему діофантових рівнянь, в якій залишки $b_i$ визначаються неоднозначно.

Дослідження підтвердило, що запропоновані методи забезпечують можливість ефективного шифрування та коректного відновлення відкритого тексту за рахунок властивостей КТЗ.

1. Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. Journal of Information Security and Applications, 58, 102729.
2. Mohan Ananda P. Residue Number Systems: Theory and Applications. Birkhäuser. 2016. 351 p.

## Вплив квантових обчислень на сучасну криптографію: загрози, виклики та напрямки розвитку постквантових алгоритмів

УДК 004.056.55

Михайло Касянчук[1], Юрій-Богдан Петренчук[2]

*Західноукраїнський національний університет,*
*[1]kasyanchuk@ukr.net, [2]petrenchuk.yuriy@gmail.com*

Сучасний розвиток квантових обчислень суттєво змінює модель загроз для криптографії. Алгоритми, які вважалися практично незламними для класичних комп'ютерів, можуть стати вразливими. Зокрема, алгоритм Шора забезпечує поліноміальний розв'язок задач факторизації великих чисел і обчислення дискретного логарифма, що створює загрозу для криптосистем RSA, DSA та ECC. Алгоритм Ґровера прискорює пошук у неструктурованих просторах, зменшуючи ефективну стійкість симетричних ключів завдяки квадратичному прискоренню. У результаті традиційні криптографічні підходи можуть втратити необхідний рівень безпеки у квантову епоху.

Вплив квантових обчислень на криптографію є одним із ключових викликів інформаційної безпеки XXI століття. Більшість сучасних криптографічних протоколів, що використовуються в Інтернеті, електронному урядуванні, банківських системах і блокчейн-інфраструктурі, базуються на математичних задачах, складність яких визначається обмеженнями класичних обчислень. Поява масштабованих квантових комп'ютерів змінює цю парадигму криптостійкості [1].

Алгоритм Шора, запропонований у 1994 році, дозволяє ефективно виконувати факторизацію великих чисел і обчислення дискретного логарифма на квантовому комп'ютері. Це означає, що криптосистеми на основі RSA та еліптичних кривих (ECDSA, ECDH) можуть стати вразливими після появи достатньо потужних квантових пристроїв. Дослідження показують, що для зламу RSA-2048 знадобляться тисячі логічних кубітів із корекцією помилок, хоча точні оцінки залежать від розвитку квантового обладнання.

Квантові обчислення впливають і на симетричну криптографію. Алгоритм Ґровера прискорює перебір ключів, зменшуючи складність атаки приблизно з

$O(2^n)$ до $O(2^{n/2})$. Таким чином, AES-128 у квантовій моделі забезпечує близько 64 біт ефективної безпеки, що робить AES-256 більш придатним для довготривалого використання. Водночас практична реалізація алгоритму Гровера потребує значних квантових ресурсів, тому збільшення довжини ключів залишається ефективним способом підвищення стійкості.

Особливу небезпеку становить стратегія “store now, decrypt later”, коли зашифровані дані можуть зберігатися для подальшого дешифрування після появи квантових комп’ютерів. Це критично для інформації з тривалим терміном зберігання, зокрема державних архівів, фінансових документів, медичних записів і військових комунікацій. Тому перехід до квантово-стійких алгоритмів розглядається як стратегічна необхідність уже сьогодні.

У відповідь на ці виклики Національний інститут стандартів і технологій США (NIST) у 2016 році розпочав процес стандартизації постквантової криптографії. У 2022–2024 роках було обрано перші алгоритми нового покоління, серед яких CRYSTALS-Kyber для обміну ключами та CRYSTALS-Dilithium для цифрового підпису. Вони базуються на складності задач Module-LWE (MLWE) та Module-SIS (MSIS), для яких наразі не відомо ефективних квантових алгоритмів розв’язання [2]. У процесі стандартизації також проводиться порівняння алгоритмів PQC за рівнями безпеки, розмірами ключів і продуктивністю, оскільки різні схеми можуть мати переваги в окремих сценаріях використання — від високопродуктивних мережевих протоколів до ресурсно-обмежених вбудованих систем.

Алгоритми на основі решіток (CRYSTALS-Kyber, Dilithium) демонструють кращий компроміс між продуктивністю й розмірами даних порівняно з деякими іншими підходами, тому вони й були серед лідерів впровадження. Проте оптимізація під апаратні архітектури (ARM, x86) та захист від побічних каналів залишається критичною. Рекомендована на практиці стратегія — використання гібридних схем, які поєднують класичні та PQC-компоненти в одному протоколі. Це забезпечує сумісність і поступовий перехід, зменшує ризик невдалого вибору нового алгоритму та гарантує захист у разі появи робочого квантового атакуючого апарату [3][4].

Під час оцінювання постквантових криптосистем необхідно враховувати математичну стійкість до класичних і квантових атак, результати криптоаналізу, вибір параметрів, продуктивність алгоритмів і розміри ключів, а також ризики реалізації, зокрема атаки через побічні канали.

Отже, квантові обчислення змінюють підходи до криптографічної безпеки: асиметричні алгоритми на основі факторизації та дискретного логарифму стають вразливими через алгоритм Шора, а симетричні схеми потребують збільшення параметрів через алгоритм Ґровера. У відповідь формується новий напрям — постквантова криптографія, що базується на математичних задачах, стійких до квантових атак, і поступово інтегрується в сучасну цифрову інфраструктуру.

1. Post-Quantum Cryptography PQC. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

2. On the practical cost of Grover for AES key recovery. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/csrc/media /Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.
3. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. [Електронний ресурс]. – Режим доступу: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
4. Post-Quantum Cryptography: Anticipating Threats and Preparing the Future. [Електронний ресурс]. – Режим доступу:https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future.

## Аналіз енергетичної доцільності впровадження малопотужних апаратних вузлів у віртуалізовані навчальні середовища з кібербезпеки

УДК 004.056:004.738

Онищук Гліб[1] , Сергій Бабич[2]

*Національний університет водного господарства та природокористування, [1]onyshchuk_ak23@nuwm.edu.ua, [2]s.v.babych@nuwm.edu.ua*

Навчальні процеси з кібербезпеки вимагають розгортання складних ізольованих середовищ для тестування вразливостей, моделювання кібератак та налаштування засобів захисту. Традиційна модель забезпечення лабораторій передбачає використання повноцінних потужних робочих станцій («товстих» клієнтів), обчислювальні ресурси яких більшу частину часу використовуються неефективно, а їх обслуговування є складним та вкрай енергозатратним процесом [1].

Дане дослідження присвячене аналізу енергетичної та економічної доцільності заміни традиційних персональних комп'ютерів на малопотужні апаратні вузли («тонкі» або «нульові» клієнти) на базі інфраструктури віртуальних робочих столів (VDI). Актуальність переходу зумовлена глобальною необхідністю реалізації парадигми «зелених ІТ», що спрямована на зменшення енергоспоживання, а також критичною потребою в оптимізації витрат на супровід ІТ-інфраструктури в академічному та бізнес-середовищі [2, 3]. Принциповою особливістю цього підходу є дослідження показників малопотужних вузлів саме в умовах високодинамічних ресурсомістких навантажень, де архітектура VDI здатна одночасно знизити енерговитрати та безпрецедентно підвищити безпеку навчального середовища [1, 4].

Традиційна робоча станція разом з монітором споживає в середньому 150-200 Вт електроенергії [1]. Впровадження архітектури VDI передбачає перенесення всіх обчислювальних процесів на централізований сервер, тоді як на робочому місці студента залишається клієнтський пристрій, рівень енергоспоживання якого складає лише від 8 до 50 Вт [1, 2]. Навіть з урахуванням енерговитрат на живлення серверів та масивів зберігання даних,