УДК 004.056.55:004.94
DOI https://doi.org/10.32782/2521-6643-2025-1-69.14

Прокопович-Ткаченко Д. І., кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-6590-3898

Хрушков Б. С., аспірант кафедри кібербезпеки
та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0009-0002-3978-5012

Деркач Я. О., магістрант кафедри інфокомунікаційної інженерії
імені В.В. Поповського
Харківського національного університету радіоелектроніки
ORCID: 0009-0009-7208-370X

ПОСТКВАНТОВІ ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВИКЛИКИ ГЛОБАЛЬНОГО ТА НАЦІОНАЛЬНОГО РІВНЯ

У статті розглянуто ключові аспекти впливу квантових обчислень на сучасну інформаційну безпеку, а також потенційні наслідки їх впровадження у різних сферах суспільного життя. Зокрема, аналізуються ризики, які виникають через можливість зламу традиційних криптографічних алгоритмів, таких як RSA, DSA, ECC та інші, за допомогою квантових комп'ютерів, які здатні виконувати обчислення з небаченою швидкістю. Це створює загрозу для конфіденційності, цілісності та доступності інформації у фінансових, державних, військових та інших критично важливих системах.

У роботі пропонуються шляхи вирішення проблем, пов'язаних із впровадженням стійкої до квантових атак криптографії. Описано перспективи використання алгоритмів, що базуються на ґратках, кодах корекції помилок, багатоваріантних рівняннях, ізогеній еліптичних кривих та інших підходах, здатних забезпечити довготривалу безпеку даних. Розглянуто міжнародні ініціативи щодо стандартизації постквантових криптографічних технологій, серед яких особливу роль відіграє програма NIST з розробки нових криптографічних стандартів.

Окрему увагу приділено викликам, які постають перед країнами на національному рівні. Серед них – необхідність модернізації існуючих інформаційних систем, розробки нових стандартів кібербезпеки, підготовки спеціалістів у галузі квантових технологій, а також значні фінансові та організаційні витрати. Виокремлено ризики для фінансової, енергетичної, транспортної та державної інфраструктури, які є критично залежними від надійних криптографічних методів захисту.

Стаття акцентує увагу на важливості міжнародної співпраці в умовах глобальних постквантових загроз. Запропоновано механізми міжнародного обміну досвідом, спільні дослідження та створення альянсів для прискорення впровадження стійких до квантових атак технологій. Розглянуто необхідність розробки нових стратегій кіберзахисту, які враховують виклики майбутнього та забезпечують стабільність сучасних інформаційних систем у постквантову еру

Ключові слова: *постквантові загрози, квантові комп'ютери, інформаційна безпека, криптографія, міжнародна співпраця.*

Prokopovych-Tkachenko D. I., Khrushkov B. S., Derkach Y. O. Post-quantum threats to information security: challenges at the global and national levels

The article examines the key aspects of the impact of quantum computing on modern information security, as well as the potential consequences of its implementation in various spheres of public life. In particular, it analyzes the risks arising from the possibility of breaking traditional cryptographic algorithms, such as RSA, DSA, ECC, and others, using quantum computers capable of performing computations at unprecedented speeds. This poses a threat to the confidentiality, integrity, and availability of information in financial, governmental, military, and other critically important systems.

The study proposes solutions to address issues related to the implementation of quantum-resistant cryptography. It outlines the prospects of using algorithms based on lattices, error-correcting codes, multivariate equations, isogenies of elliptic curves, and other approaches capable of ensuring long-term data security. International initiatives for the standardization of post-quantum cryptographic technologies are considered, with particular emphasis on the NIST program for the development of new cryptographic standards.

Special attention is paid to the challenges faced by countries at the national level. These include the need to modernize existing information systems, develop new cybersecurity standards, train specialists in quantum technologies, and address sig-

© Д. І. Прокопович-Ткаченко, Б. С. Хрушков, Я. О. Деркач, 2025

nificant financial and organizational costs. Risks are highlighted for financial, energy, transportation, and governmental infrastructures that are critically dependent on reliable cryptographic protection methods.

The article emphasizes the importance of international cooperation in addressing global post-quantum threats. Mechanisms for international exchange of experience, joint research, and the formation of alliances to accelerate the implementation of quantum-resistant technologies are proposed. The necessity of developing new cybersecurity strategies that account for future challenges and ensure the stability of modern information systems in the post-quantum era is explored.

Key words: *post-quantum threats, quantum computers, information security, cryptography, international cooperation.*

Постановка проблеми. Розвиток квантових обчислень знаменує нову еру у технологічному прогресі, відкриваючи можливості, що суттєво перевищують потенціал класичних комп'ютерів. Проте ці досягнення супроводжуються значними ризиками, особливо в галузі інформаційної безпеки. Сучасні криптографічні алгоритми, такі як RSA, ECC і DSA, стають вразливими до атак на основі квантових обчислень, зокрема алгоритму Шора, що здатний виконувати факторизацію великих чисел у поліноміальний час. Це створює серйозні загрози для фінансових, урядових і критичних інфраструктур, які базуються на традиційній криптографії

Аналіз останніх досліджень та публікацій. Сучасні дослідження детально висвітлюють як можливості, так і ризики, пов'язані з квантовими обчисленнями. Прескілл (Preskill) (2018) описує концепцію NISQ (Noisy Intermediate-Scale Quantum), яка розкриває обмеження сучасних квантових обчислень, але водночас підкреслює їхній потенціал для зламу сучасних криптографічних систем [6]. Шор (Shor) (1997) запропонував алгоритм для факторизації чисел, що підриває безпеку RSA [8]. Грувер (Grover) (1996) продемонстрував, як квантові обчислення прискорюють пошук у базах даних, що впливає на стійкість симетричних шифрів [4]. NIST (2022) ініціював стандартизацію постквантових алгоритмів, таких як криптографія на основі граток, ізогеній еліптичних кривих і кодів виправлення помилок [5]. У роботах Беннет (Bennett) і Брассард (Brassard) (1984) представлена квантова криптографія, яка пропонує стійкість до квантових атак [2]. Водночас Сміт (Smith) (2022) звертає увагу на геополітичні аспекти розвитку квантових технологій, які можуть посилити нерівність між країнами [9]

Мета статті. Дослідити вплив квантових обчислень на інформаційну безпеку, враховуючи як їхній потенціал, так і ризики для сучасних криптографічних систем, а також запропонувати ефективні шляхи впровадження постквантової криптографії для захисту інформації у нових умовах. Мета передбачає глибокий аналіз загроз, пов'язаних із застосуванням алгоритмів Шора та Гровера, які суттєво підривають стійкість криптографічних протоколів на основі факторизації чисел, дискретного логарифму та перебору ключів. Особливий акцент зроблено на міжнародних ініціативах, таких як програма NIST зі стандартизації постквантових алгоритмів, а також на їхньому потенціалі для створення нових стандартів безпеки. У роботі аналізуються перспективи використання таких алгоритмів, як решіткові криптосистеми, кодові схеми, криптографія на основі ізогеній еліптичних кривих та багатоінваріантних рівнянь, які здатні забезпечити довготривалу інформаційну безпеку. Окремо досліджуються стратегічні виклики, що постають перед державами та організаціями у зв'язку із модернізацією існуючих інформаційних систем. Це включає фінансові витрати, необхідність створення нових стандартів кібербезпеки, підготовку фахівців у галузі квантових технологій та ризики, що виникають через нерівномірний доступ до квантових розробок між різними країнами. Стаття також спрямована на визначення практичних рекомендацій щодо адаптації критичних інфраструктур (фінансової, енергетичної, транспортної та державної) до нових загроз та забезпечення безперервного функціонування інформаційних систем у постквантовому середовищі. Важливою складовою дослідження є аналіз можливостей міжнародної співпраці, обміну досвідом та спільних наукових розробок для прискорення впровадження стійких до квантових атак рішень.

Виклад основного матеріалу. Основна частина, методологія.Дослідження виконано на основі систематичного огляду наукових публікацій, присвячених квантовим обчисленням та криптографії, із застосуванням порівняльного аналізу складності класичних та квантових алгоритмів. Для кількісної оцінки часу факторизації (RSA, DSA, ECC) і пошуку (AES тощо) використано асимптотичний аналіз: порівнювались субекспоненційні або експоненційні оцінки класичних методів із поліномійними чи кореневими оцінками квантових алгоритмів (Шора і Гровера). Аналітичне моделювання базувалося на описі квантового перетворення Фур'є та фазових інверсій, які лежать в основі квантових алгоритмів. На фінальному етапі проведено експертну оцінку ризиків для сучасних криптосистем і сформульовано рекомендації щодо переходу на постквантові схеми захисту.

Нижче наведено розширений опис математичного апарату квантових алгоритмів, які становлять загрозу для сучасної криптографії, з акцентом на відповідних формулах та оцінках складності.

Алгоритм Шора для факторизації

Нехай потрібно факторизувати число

$$N = p \cdot q,$$

де p і q – великі прості числа. Алгоритм Шора зводиться до пошуку періоду функції

$$f(x) = a^x \bmod N,$$

де a – довільне ціле число, взаємно просте з N. Якщо вдається знайти найменше додатне ціле r таке, що

$$a^r \equiv 1 \pmod N,$$

то (за певних умов, наприклад, якщо r парне та $\gcd\left(a^{r/2}-1, N\right) \neq 1$) можна відновити нетривіальний дільник N.

Квантова частина алгоритму

Ключовим інструментом є квантове обчислення періоду за допомогою квантового перетворення Фур'є (Quantum Fourier Transform, QFT). Узагальнена схема:

1. Ініціалізуємо два регістри:

$$|0\rangle \otimes |0\rangle$$

2. Застосовуємо оператор Адамара H (або набір операторів $H^{\otimes n}$) до першого регістра, щоб підготувати рівномірну суперпозицію:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle.$$

3. Обчислюємо $a^x \bmod N$ у другому регістрі за допомогою спеціалізованого унітарного перетворення (modular exponentiation):

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \left|a^x \bmod N\right\rangle$$

4. Застосовуємо квантове перетворення Фур'є (QFT) до першого регістра:

$$\left| x\right\rangle \xrightarrow{\mathrm{QFT}_{2^n}} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}} \Bigg| y\rangle.$$

5. Виконуємо вимірювання результату в першому регістрі. З високою ймовірністю значення вимірювання дає змогу відновити період r.

Оцінка складності

Класичний найшвидший (на сьогодні) загальновідомий метод факторизації (решето числового поля, Number Field Sieve) має субекспоненційну складність приблизно

$$\exp\left(\left(c + o(1)\right)(\ln N)^{1/3} (\ln \ln N)^{2/3}\right)$$

Алгоритм Шора натомість виконується за поліномійну кількість елементарних операцій відносно $\log N$. Часто наводять оцінку:

$$O\left((\log N)^k\right)$$

де k – константа (наприклад, $k \approx 3$ для деяких варіантів реалізації). Така швидкодія руйнує основу безпеки RSA, DSA та ECC, які базуються на складності факторизації та дискретного логарифму.

Алгоритм Гровера для пошуку і перебору ключів

Постановка задачі

Задача пошуку у невпорядкованому просторі (наприклад, перебір усіх можливих ключів розміру n біт) класично потребує в середньому

$$O\left(2^n\right)$$

спроб. Алгоритм Гровера дає можливість виконати пошук за

$$O\left(\sqrt{2^n}\right) = O\left(2^{n/2}\right)$$

Тобто час зменшується у корінь від розміру простору.

Алгоритмічні деталі

Алгоритм Гровера можна подати як послідовність «відбиття» (reflection) стану хвильової функції від цільового розв'язку і від середнього стану. Ключові кроки:

1. Ініціалізується регістр з $|0\rangle$ для n кубітів.
2. Застосовується перетворення Адамара $H^{\otimes n}$ для створення суперпозиції

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

3. Застосовується «оракул» O_f, що змінює фазу амплітуди шуканого елемента. Формально,

$$O_f|x\rangle = \begin{cases} -|x\rangle, & \text{якщо } x = x_{\text{розв'язок}}, \\ |x\rangle, & \text{інакше.} \end{cases}$$

4. Застосовується так звана «дифузійна трансформація» (diffusion operator), яка відбиває амплітуди від середнього значення:

$$D = 2|\psi\rangle\langle\psi| - I,$$

де

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

5. Кроки 3 та 4 повторюються приблизно $O\left(\sqrt{2^n}\right)$ разів, після чого стан системи колапсує до шуканого елемента з ймовірністю, близькою до 1.

Вплив на симетричну криптографію

Для шифру AES-128 класичний перебір ключа дає оцінку 2^{128} операцій, тоді як на квантовому комп'ютері це скорочується до 2^{64}. Хоч це і не настільки радикальний злам, як у випадку алгоритму Шора проти RSA, але все одно фактично «вкорочує» довжину ключа вдвічі. Тому для підвищення безпеки за умов квантових загроз рекомендують збільшувати розмір симетричних ключів (AES-256 замість AES-128 тощо).

Пошук у базах даних

Узагальнений пошук

Алгоритм Гровера можна використати не лише для перебору ключів, а й для будь-якої задачі пошуку у невпорядкованому просторі з N елементів, де класичний пошук потребує $O(N)$. У квантовому варіанті складність стає $O\left(\sqrt{N}\right)$. Формула лишається аналогічною:

$$\text{Час на пошук} \sim O\left(\sqrt{N}\right).$$

Похідні алгоритми

Існують узагальнення і покращення, що дають змогу ефективніше обробляти певні структури даних, але базова ідея лишається: фазова інверсія шуканих розв'язків та дифузійне перетворення приводять до квадратичного прискорення пошуку порівняно з класичними методами.

Висновки та наслідки

1. Алгоритм Шора надає поліноміну складність факторизації і розв'язання задачі дискретного логарифму (необхідних для RSA, DSA, ECC), руйнуючи криптосистеми на основі складності цих задач.

2. Алгоритм Гровера призводить до квадратичного прискорення при пошуку у невпорядкованому просторі, зменшуючи час перебору ключів (наприклад, для AES) з 2^n до $2^{n/2}$.

3. Пошук у базах даних загалом також пришвидшується за тією самою формулою $O\left(\sqrt{N}\right)$, що підтверджує універсальність квантової загрози для задач, де можливий «грубий перебір».

4. Постквантова криптографія. Через перспективу появи квантових комп'ютерів із достатньою кількістю стабільних кубітів активно розвиваються «постквантові» (квантостійкі) алгоритми, що не базуються виключно на факторизації чи дискретному логарифмі. Прикладами є:

– кодові криптосистеми (Code-based),

– решіткові криптосистеми (Lattice-based),

– криптографія на мультиваріантних многочленах та ін.

Практичні рекомендації:

Збільшувати ключі для симетричних алгоритмів (перехід від AES-128 до AES256).

Поступово переходити на постквантові схеми шифрування та цифрового підпису, що витримують атаки алгоритмом Шора.

Таким чином, математичний апарат квантових алгоритмів демонструє суттєве прискорення для широкого класу криптографічних задач, що зумовлює необхідність заздалегідь планувати перехід до квантостійких рішень.

Реалізація:

Результати дослідження підтвердили високу ефективність квантових алгоритмів Шора та Гровера у зламі традиційних криптографічних систем, таких як RSA, ECC, DSA та AES. Це створює суттєві загрози для сучасних методів шифрування, що базуються на факторизації, дискретному логарифмі та переборі

ключів. Було виявлено, що критична інфраструктура, зокрема фінансові системи, енергомережі, транспортні мережі та державні установи, є вразливою до квантових атак, що може призвести до значних економічних і безпекових наслідків. Дослідження підкреслює необхідність термінового впровадження постквантових алгоритмів, таких як ґраткові, кодові, ізогенії еліптичних кривих та багатоваріантні рівняння, які здатні забезпечити довготривалу інформаційну безпеку. Також виявлено суттєву глобальну нерівність у доступі до квантових технологій, що посилює геополітичну і технологічну асиметрію між країнами. Наголошується на важливості міжнародної співпраці, зокрема в межах ініціатив зі стандартизації постквантової криптографії, таких як програма NIST, для мінімізації ризиків та впровадження нових стандартів інформаційної безпеки у постквантовому середовищі.

Висновки. Постквантове середовище створює суттєві загрози як на глобальному, так і на національному рівнях. Згідно з представленими матеріалами, нерівність доступу до квантових технологій посилює стратегічну асиметрію: держави з достатніми ресурсами й науковим потенціалом (США, Китай, ЄС) випереджають інші країни у розробці квантових систем (Прескіл (Preskill), 2018). Це може призвести до виникнення нових форм “цифрової залежності” та загрожує світовому балансу сил, оскільки квантові обчислення надають перевагу в галузі кібербезпеки та військових технологій.

Злам шифрованих даних за допомогою алгоритму Гровера (Grover), (1996) становить критичну загрозу для хмарних сервісів і глобальної інфраструктури обробки персональної, фінансової чи урядової інформації. Особливу небезпеку становить сценарій “збирай зараз, розшифруй пізніше”, коли зловмисники накопичують зашифровані дані, розраховуючи на подальше дешифрування після появи достатньо потужних квантових машин (NIST, 2022). Крім того, компрометація AES або інших симетричних алгоритмів може викликати масові фінансові втрати та загрожувати стабільності світових ринків.

На національному рівні квантові обчислення здатні підривати роботу критичної інфраструктури, зокрема фінансових і енергетичних мереж, транспорту та державних установ. Здатність алгоритму Шора (Shor, 2021) швидко факторизувати великі числа та обчислювати дискретні логарифми робить вразливими такі поширені схеми цифрового підпису, як DSA та ECDSA. Наслідком може бути втрата контролю над банківськими транзакціями, перебої в енергопостачанні чи компрометація оборонної інформації. Це загрожує економічній і безпековій стабільності як окремих держав, так і всього міжнародного середовища.

З огляду на викладене, висновки зводяться до необхідності негайного впровадження постквантових алгоритмів, зокрема криптографії на основі ґраток, ізогеній над еліптичними кривими та кодових схем. Міжнародна співпраця, ініційована такими організаціями, як NIST (2022), є важливим чинником у визначенні стандартів, які забезпечать захист інформації після настання епохи квантових обчислень. Для держав і приватного сектора першочерговим стає модернізація наявної інфраструктури, перехід до нових протоколів шифрування та формування експертного середовища, здатного забезпечити надійну реалізацію постквантових рішень. Лише так можна зменшити негативні наслідки можливих квантових атак і гарантувати безпеку даних у майбутньому.

Список використаних джерел:

1. Аароносн С. Quantum Computing Since Democritus. Cambridge: Cambridge University Press, 2013. URL: https://www.cambridge.org

2. Беннетт С. Г., Брассар Г. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. 1984. С. 175–179. URL: https://ieeexplore.ieee.org

3. Чайлдс А. М., ван Дам В. Quantum Algorithms for Algebraic Problems. Reviews of Modern Physics. 2010. Т. 82, № 1. С. 1–52. URL: https://journals.aps.org

4. Гровер Л. К. A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing. 1996. С. 212–219. URL: https://dl.acm.org

5. Національний інститут стандартів і технологій (NIST). Post-Quantum Cryptography Standardization: Round 3 Submissions. 2022. URL: https://csrc.nist.gov/publications

6. Прескілл Д. Quantum Computing in the NISQ Era and Beyond. Quantum. 2018. Т. 2, № 79. С. 79. DOI: 10.22331/q-2018-08-06-79. URL: https://quantum-journal.org

7. Ріффель Е. Г., Полак В. Х. Quantum Computing: A Gentle Introduction. Cambridge: MIT Press, 2011. URL: https://mitpress.mit.edu

8. Шор П. В. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997. Т. 26, № 5. С. 1484–1509. DOI: 10.1137/S0097539795293172. URL: https://epubs.siam.org

9. Сміт Дж. Quantum Computing: Global Implications. Oxford: Academic Press, 2022. URL: https://www.elsevier.com

10. Нільсен М. А., Чуанг І. Л. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667. URL: https://www.cambridge.org

11. Ладд Т. Д., Єлезко Ф., Лафламм Р., Накамура Ю., Монро С., О'Брайен Дж. Л. Quantum Computers. Nature. 2010. Т. 464, № 7285. С. 45–53. DOI: 10.1038/nature08812. URL: https://www.nature.com

12. Екерт А. К. Quantum Cryptography Based on Bell's Theorem. Physical Review Letters. 1991. Т. 67, № 6. С. 661–663. DOI: 10.1103/PhysRevLett.67.661. URL: https://journals.aps.org

13. Монтанаро А. Quantum Algorithms: An Overview. npj Quantum Information. 2016. Т. 2. С. 15023. DOI: 10.1038/npjqi.2015.23. URL: https://www.nature.com

14. Ван Метер Р. Quantum Networking. Hoboken: Wiley, 2014. URL: https://www.wiley.com

References:

1. Aaronson, S. (2013). *Quantum computing since Democritus.* Cambridge University Press. https://www.cambridge.org

2. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179. https://ieeexplore.ieee.org

3. Childs, A. M., & van Dam, W. (2010). Quantum algorithms for algebraic problems. *Reviews of Modern Physics, 82*(1), 1–52. https://journals.aps.org

4. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219. https://dl.acm.org

5. National Institute of Standards and Technology (NIST). (2022). *Post-quantum cryptography standardization: Round 3 submissions.* https://csrc.nist.gov/publications

6. Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum, 2*(79), 79. https://quantum-journal.org

7. Rieffel, E. G., & Polak, W. H. (2011). *Quantum computing: A gentle introduction.* MIT Press. https://mitpress.mit.edu

8. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509. https://epubs.siam.org

9. Smith, J. (2022). *Quantum computing: Global implications.* Academic Press. https://www.elsevier.com

10. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information.* Cambridge University Press. https://www.cambridge.org

11. Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. *Nature, 464*(7285), 45–53. https://www.nature.com

12. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*(6), 661–663. https://journals.aps.org

13. Montanaro, A. (2016). Quantum algorithms: An overview. *npj Quantum Information, 2*, 15023. https://www.nature.com

14. Van Meter, R. (2014). *Quantum networking.* Wiley. https://www.wiley.com