ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056:004.42+681.3 doi.org/10.33298/2226-8553.2025.1.42.27

Богом'я В. І., Черемісіна Л. О., Ярмолатій А. В.

ЗАГРОЗИ КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ КЛАСИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

З появою квантових обчислювальних технологій, які мають потенціал здійснювати обчислення з набагато більшою швидкістю, ніж класичні комп'ютери, виникає загроза для існуючих криптографічних систем. Квантові алгоритми, здатні ефективно розв'язувати складні обчислювальні завдання, що лежать в основі безпеки сучасних криптографічних систем. Це означає, що з розвитком квантових комп'ютерів стає можливою компрометація багатьох сучасних шифрів, які сьогодні вважаються безпечними.

З огляду на це, постає потреба у створенні нових криптографічних методів та алгоритмів, які б залишались стійкими до квантових атак. Пост-квантова криптографія є новим напрямом у криптографічний науці, який ставить за мету розробку алгоритмів, стійких до атак квантових комп'ютерів. Вона охоплює широкий спектр методів, таких як латичні криптосистеми, криптографія на основі кодів з корекцією помилок та багато інших.

Таким чином, розвиток квантових обчислювальних технологій ставить перед криптографією нові виклики, що вимагають перегляду існуючих методів захисту інформації. Постає необхідність адаптації криптографічних систем до нових умов, зокрема через створення алгоритмів, які б залишались надійними навіть в умовах появи квантових комп'ютерів.

Тому, актуальність теми дослідження полягає в необхідності захисту інформації в умовах швидкого розвитку квантових обчислювальних систем.

Наукова новизна цього дослідження полягає в комплексному аналізі пост-квантових криптосистем та їхній стійкості до нових типів загроз. Дослідження пропонує порівняння ефективності класичних криптографічних методів із пост-квантовими, що дозволяє виявити їхні сильні та слабкі сторони в умовах квантових обчислень.

Практична значущість дослідження полягає у можливості використання результатів для впровадження нових стандартів криптографічного захисту інформації. Це є особливо важливим для організацій, що обробляють конфіденційні дані, таких як банки, урядові установи та компанії, які займаються розробкою технологій штучного інтелекту.

Ключові слова: *квантові обчислення, класичні криптографічні системи, загрози, криптографічні алгоритми, інформаційна безпека, квантові технології.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний розвиток інформаційних технологій та обчислювальних систем значно підвищує важливість забезпечення захисту даних та інформаційної безпеки. Криптографія відіграє ключову роль у захисті даних, забезпечуючи конфіденційність, цілісність та автентифікацію інформації в різних галузях, таких як фінанси, медицина, державне управління та багато інших.

З появою квантових обчислювальних технологій, які мають потенціал здійснювати обчислення з набагато більшою швидкістю, ніж класичні комп'ютери, виникає загроза для існуючих криптографічних систем. Це означає, що з розвитком квантових комп'ютерів стає можливою компрометація багатьох сучасних шифрів, які сьогодні вважаються безпечними.

З огляду на це, постає потреба у створенні нових криптографічних методів та алгоритмів, які б залишались стійкими до квантових атак. Пост-квантова криптографія є новим напрямком у криптографічній науці, який ставить за мету розробку алгоритмів, стійких до атак квантових комп'ютерів.

Результати даного дослідження можуть бути використані для розвитку нових підходів до забезпечення інформаційної безпеки в умовах зростання загроз від квантових обчислень. Це дозволить не тільки зберегти захищеність даних, але й створити надійні основи для криптографічних систем майбутнього.

У даній статті буде розглянуто основні принципи квантових обчислень, загрози, які вони становлять для класичних криптографічних систем, а також детально проаналізовано пост-квантові алгоритми та їхню стійкість до квантових атак. Такий підхід дозволяє отримати цілісне уявлення про сучасний стан криптографії та можливі шляхи розвитку цієї сфери у майбутньому.

Аналіз останніх досліджень і публікацій. Авторами [1–3, 5-7] були визначені криптографічні системи, що забезпечують захист інформації в умовах квантових загроз та наведені основні принципи квантових обчислень та їхній вплив на сучасну криптографію.

У [4–6, 9-12] розглянути та проаналізовані деякі криптографічні алгоритми, стійкі до квантових атак.

У [7–10, 14] було проведено порівняльний аналіз класичних криптосистем та пост-квантових алгоритмів та досліджено особливості забезпечення стійкості різних шифрів до квантового криптоаналізу [9–13, 15].

Але сучасні криптосистеми, стійкі до квантових атак, та методи їх криптоаналізу залишилися за границями досліджень.

Враховуючи вищезазначене, актуальність теми дослідження полягає в аналізі особливостей захисту інформації в умовах швидкого розвитку квантових обчислювальних систем.

Вивчення криптосистем, стійких до квантових атак, дозволяє не тільки підвищити рівень безпеки існуючих інформаційних систем, але й підготуватися до потенційних загроз, які можуть виникнути у майбутньому з розвитком квантових технологій.

Формулювання цілей статті. Мета статті є проаналізувати сучасні криптосистеми, стійкі до квантових атак, а також провести порівняння їх ефективності з класичними криптографічними алгоритмами.

Завданнями дослідження є:

1. Аналіз загроз квантових обчислень для класичних криптографічних алгоритмів.
2. Розгляд та аналіз криптографічних алгоритмів, стійких до квантових атак.
3. Порівняльний аналіз класичних криптосистем та пост-квантових алгоритмів.
4. Дослідження рівня стійкості різних шифрів до квантового криптоаналізу.

Виклад основного матеріалу. *Загрози квантових обчислень для класичних криптографічних алгоритмів.* Розвиток квантових обчислень ставить під загрозу багато сучасних криптографічних систем, які використовуються для захисту даних у цифровому середовищі. Причина цієї загрози криється в здатності квантових комп'ютерів виконувати обчислення набагато швидше, ніж класичні комп'ютери, що значно знижує стійкість традиційних криптографічних алгоритмів.

Загроза для асиметричних алгоритмів.

Асиметричні криптографічні алгоритми, такі як RSA, DSA, та ECDSA, значною мірою залежать від складності математичних задач, таких як факторизація великих чисел або обчислення дискретного логарифма.

Ці задачі вимагають величезної обчислювальної потужності від класичних комп'ютерів, але квантові алгоритми, зокрема алгоритм Шора, здатні значно зменшити час розв'язання таких задач.

Алгоритм Шора, який здатний розкладати великі числа на множники за поліноміальний час, що значно прискорює процес факторизації. Це означає, що захищені RSA-ключами системи можуть стати вразливими до атак з використанням квантових комп'ютерів, оскільки ці ключі можуть бути розшифровані за значно коротший час. Наприклад, для факторизації 2048-бітного ключа RSA, що в класичному середовищі займає мільярди років, квантовий комп'ютер з відповідною кількістю кубітів зміг би виконати це завдання протягом кількох годин або днів.

Еліптична криптографія (далі – ECC): ECC також вразлива до квантових атак через здатність квантових комп'ютерів швидко вирішувати дискретні логарифмічні задачі. Хоча ECC використовує коротші ключі, що є перевагою в класичних системах, вони не забезпечують належного рівня безпеки проти квантових обчислень.

Загроза для симетричних алгоритмів.

Хоча симетричні алгоритми, такі як AES, є менш вразливими до квантових атак, вони також відчувають вплив квантових обчислень. Квантовий алгоритм Гровера дозволяє зменшити час, необхідний для атаки перебору (brute force), вдвічі.

Алгоритм Гровера: За допомогою цього алгоритму квантовий комп'ютер може виконувати пошук в базі даних або перебір симетричних ключів за час, пропорційний квадратному кореню від кількості можливих варіантів. Це означає, що 256-бітний ключ AES, який вважається надзвичайно безпечним у класичних умовах, за допомогою алгоритму Гровера забезпечує еквівалентний рівень безпеки 128-бітного ключа [1–3, 7].

Проблеми з передачею даних та інфраструктурою. Загроза квантових обчислень також впливає на інфраструктуру захищеної передачі даних, наприклад, на протоколи SSL/TLS, які використовують асиметричні алгоритми для обміну симетричними ключами.

У разі наявності достатньо потужного квантового комп'ютера, нападник міг би перехопити сеансові ключі і розшифрувати трафік, що передається між клієнтом і сервером. Це робить захищену передачу даних вразливою до так званих атак "людина посередині" (MITM) [5-7].

Перехід до постквантової криптографії. З огляду на загрози, які квантові обчислення становлять для традиційних криптографічних систем, міжнародні організації та дослідники активно працюють над створенням постквантових криптографічних алгоритмів.

Постквантова криптографія використовує математичні задачі, які важко вирішити навіть для квантових комп'ютерів. Серед перспективних підходів є [9–11]:

Кодоподібна криптографія, яка базується на складності розв'язання задач декодування випадкових лінійних кодів. Цей підхід забезпечує високий рівень безпеки, оскільки навіть квантовим комп'ютерам важко виконати подібні обчислення.

Криптографія на базі решіток (Lattice-based cryptography), яка використовує задачі, пов'язані з решітками в багатовимірному просторі, такі як задача найкоротшого вектора (SVP) та задача найближчого вектора (CVP). Цей підхід вважається одним з найбільш надійних та стійких до квантових атак.

Квантова криптографія. Квантова криптографія [1–3, 5-7] використовує принципи квантової механіки, такі як суперпозиція та квантове заплутування, для створення захищених каналів зв’язку. Основна ідея полягає в тому, що квантові стани неможливо виміряти або спостерігати без їх змінення. Ця властивість робить можливим побудову систем, які автоматично виявляють спроби перехоплення даних.

Квантовий розподіл ключів (QKD). Квантовий розподіл ключів (Quantum Key Distribution, далі – QKD) є найвідомішою реалізацією квантової криптографії. QKD дозволяє двом сторонам безпечно обмінюватися криптографічними ключами через квантовий канал.

Якщо сторонній спостерігач (перехоплювач) намагається втрутитися у процес обміну, це негайно вплине на квантові стани фотонів, що використовуються для передачі ключа. Це зміни можна виявити, і сторони одразу дізнаються про спробу прослуховування [7–10].

Принцип роботи QKD.

Типова схема QKD виглядає наступним чином:

1.Передача квантових бітів (квантових станів): Один користувач, названий Аліса, надсилає серію фотонів, кожен з яких знаходиться у певному квантовому стані, другому користувачеві, названому Бобу. Ці квантові стани можуть представляти біти (0 або 1) та бути поляризованими за різними базами.

2.Вимірювання квантових станів, коли Боб випадково вибирає базу для вимірювання поляризації кожного фотона, який він отримує.

3.Обговорення результатів, коли після отримання фотонів, Аліса та Боб обговорюють через класичний канал, яку базу вони використовували для кодування та декодування кожного фотона, не розкриваючи значень бітів. Вони зберігають лише ті біти, де бази збіглися.

4.Перевірка наявності перехоплення, коли Аліса та Боб вибірково обирають частину своїх збережених бітів і порівнюють їх через класичний канал. Якщо ці біти співпадають, це свідчить про відсутність перехоплення. Інакше, перехоплення намагалося втрутитися в обмін.

5.Формування ключа, коли після перевірки безпеки, вони використовують збережені біти як спільний секретний ключ [11, 12].

*Протоколи QKD.*Існують кілька основних протоколів QKD, серед яких:

BB84: Найвідоміший протокол, розроблений у 1984 році Чарльзом Беннетом і Жилем Брассаром. Використовує два набори баз для кодування квантових станів і дозволяє виявити перехоплення з високою точністю [10].

E91: Розроблений Артуром Еккертом у 1991 році, цей протокол використовує квантове заплутування. Два заплутаних фотони розділяються між Алісою та Бобом, і будь-які спроби перехоплення змінюють кореляції між вимірюваннями [11].

Переваги та виклики QKD. Перевагами є безпека на рівні фізики та виявлення перехоплень. На відміну від класичних методів, де безпека залежить від обчислювальної складності, QKD забезпечує безпеку завдяки фундаментальним законам квантової механіки. Квантові системи автоматично визначають спроби перехоплення, що дозволяє уникнути компрометації ключів.

Обмежена дальність передачі: квантові канали поки що обмежені у відстані через втрати у волоконно-оптичних лініях.

Технічні складності: реалізація квантових систем потребує дорогого обладнання та точного контролю квантових станів.

Інфраструктура: потрібна спеціалізована інфраструктура, яка б підтримувала квантові канали.

Попри технічні складнощі, QKD вже застосовується в комерційних та наукових цілях [11–13]. Наприклад перший квантовий супутник. Китай запустив супутник QUESS (Quantum Experiments at Space Scale), який успішно здійснив QKD між космічним апаратом і наземними станціями на великих відстанях.

Квантові мережі. У Європі та США розробляються квантові мережі для забезпечення безпечного зв’язку між важливими установами.

Таким чином, квантова криптографія, особливо через QKD, обіцяє стати одним з ключових інструментів для забезпечення безпеки в еру квантових обчислень. Вона відкриває нові можливості для захисту інформації, хоча поки що потребує подальшого розвитку та вдосконалення для широкого впровадження.

Криптосистеми, стійкі до квантових атак. Поняття стійкості до квантових атак.

Стійкість до квантових атак — це здатність криптографічних алгоритмів витримувати атаки з використанням квантових комп'ютерів, які мають значно вищу обчислювальну потужність у порівнянні з класичними комп'ютерами. Квантові комп'ютери мають потенціал значно скоротити час розв'язання складних математичних задач, на яких базуються сучасні криптографічні методи [13–15].

Алгоритми Шора та Гровера. Основною загрозою для класичних криптографічних систем є квантові алгоритми, серед яких найвідоміші — алгоритм Шора та алгоритм Гровера.

Алгоритм Шора. Основна задача: алгоритм Шора розроблений для швидкої факторизації великих чисел та розв'язання задачі дискретного логарифмування.

Загроза для RSA: класичні криптографічні алгоритми, такі як RSA, засновані на складності факторизації великих простих чисел. Без квантових обчислень факторизація таких чисел потребує значних ресурсів і часу, що робить RSA надійним. Однак алгоритм Шора виконує факторизацію за поліноміальний час, що суттєво знижує складність цієї задачі [13, 15].

Загроза для еліптичних кривих: задача дискретного логарифмування, яка є основою алгоритмів на еліптичних кривих (наприклад, ECC), також стає вразливою перед алгоритмом Шора.

Це ставить під загрозу системи, що використовують еліптичні криві для шифрування та підпису [13, 15].

Алгоритм Гровера. Призначення: алгоритм Гровера ефективний для прискорення пошуку у невпорядкованих базах даних. Його можна використовувати для оптимізації атак грубої сили.

Вплив на симетричні алгоритми: Наприклад, у випадку алгоритмів шифрування, таких як AES, алгоритм Гровера може вдвічі скоротити ефективний розмір ключа. Це означає, що для збереження рівня безпеки, подібного до класичного 128-бітного AES, довжина ключа повинна бути збільшена до 256 біт [13].

Поліноміальне прискорення: Алгоритм Гровера забезпечує квантове прискорення в пошуку серед усіх можливих варіантів, що дозволяє скоротити час знаходження правильного значення з O(N) до O(√N), де N — кількість можливих варіантів. Це робить атаки грубої сили значно ефективнішими, але не настільки загрозливими, як алгоритм Шора для асиметричних систем [14].

Критерії стійкості до квантових атак. Для того щоб криптографічний алгоритм вважався стійким до квантових атак, він повинен відповідати декільком важливим критеріям, які враховують сучасні загрози та ефективність обчислень [13, 15]:

Відсутність ефективних квантових атак: квантові комп'ютери мають потенціал суттєво прискорити розв'язання певних математичних задач, таких як факторизація великих чисел або обчислення дискретних логарифмів. Наприклад, алгоритм Шора здатен зламувати традиційні системи, як RSA або алгоритми на основі еліптичних кривих [11]; пост-квантові алгоритми мають бути побудовані таким чином, щоб не існувало квантових алгоритмів, які можуть суттєво зменшити час для розв'язання задачі, що лежить в основі криптографічної безпеки [12].

Збереження стійкості до класичних атак. Пост-квантові алгоритми не повинні лише протистояти квантовим загрозам, але й бути стійкими до вже відомих класичних атак, таких як атаки грубої сили, атак на основі статистичних властивостей та криптоаналізу. Це важливо, оскільки навіть у разі впровадження квантових обчислень, класичні комп'ютери будуть все ще використовуватися, і класичні атаки залишатимуться актуальними [13, 15].

Це означає, що алгоритми мають забезпечувати високу надійність і під час перехідного періоду, коли одночасно використовуються як класичні, так і квантові системи [13].

Оптимальна ефективність полягає у тому, що пост-квантові алгоритми часто мають більші розміри ключів та більшу складність обчислень у порівнянні з класичними методами. Наприклад, алгоритми на основі ґраток або мультиваріантні криптографічні схеми потребують великих обсягів даних для зберігання ключів [9, 10].

Незважаючи на це, для їх широкого застосування важливо, щоб алгоритми забезпечували прийнятну швидкість шифрування та розшифрування. Це дозволяє їм бути придатними для використання у різноманітних пристроях, від мобільних телефонів до серверів у хмарних обчисленнях [10, 11].

Важливо враховувати баланс між безпекою та продуктивністю, щоб пост-квантові алгоритми могли використовуватися в реальних системах без значного зниження швидкості роботи [13, 15].

Можливість інтеграції у сучасні протоколи полягає у тому, що пост-квантові алгоритми повинні бути сумісними з існуючими стандартами та протоколами, такими як TLS/SSL, VPN, і інші протоколи захисту інформації. Це необхідно для забезпечення плавного переходу до пост-квантової криптографії без необхідності повного переоснащення інфраструктури [13–15].

Підтримка від міжнародних організацій здійснюється за допомогою розроблення стандартів пост-квантової криптографії є пріоритетом для таких організацій, як NIST (Національний інститут стандартів і технологій США). Їхні дослідження та конкурси з відбору алгоритмів допомагають визначити найбільш перспективні методи, які можуть стати основою нових стандартів захисту [9, 13, 15].

Практичне значення стійкості до квантових атак. Стійкість до квантових атак має велике значення для захисту конфіденційних даних в довгостроковій перспективі. Наприклад, інформація, яка передається сьогодні з використанням RSA чи інших алгоритмів, може бути зламана в

майбутньому, коли квантові комп'ютери стануть доступними. Тому багато організацій та дослідницьких центрів вже сьогодні розглядають можливість впровадження пост-квантової криптографії для захисту даних, які потребують тривалого зберігання та захисту [9, 11].

Квантова стійкість також є важливою для захищених комунікацій, фінансових транзакцій, зберігання персональних даних та критичної інфраструктури. Це стосується не тільки державних установ, а й комерційних організацій, що працюють з великими обсягами даних та мають високі вимоги до безпеки [11 –13, 15].

Розгляд шифрів: та їх стійкість до квантових атак. У контексті квантових обчислень, класичні криптографічні алгоритми розглядаються з точки зору їх стійкості до можливих атак, які можуть бути здійснені з використанням квантових комп'ютерів. Розглянемо, як окремі шифри витримують загрози від квантових алгоритмів [14].

Симетричні шифри: AES (Advanced Encryption Standard). Суть алгоритму полягає у тому, що AES є симетричним алгоритмом, де для шифрування та розшифрування використовується один і той самий ключ.

Загроза від алгоритму Гровера полягає у тому, що алгоритм Гровера дозволяє здійснювати атаку грубої сили на симетричні шифри у $\sqrt{N}$ кроків замість N (де N — кількість можливих ключів). Це вдвічі зменшує ефективний розмір ключа.

Рекомендації для стійкості є такі: щоб забезпечити безпеку AES в умовах можливих квантових атак, рекомендується збільшити довжину ключа. Наприклад, AES-256 буде забезпечувати аналогічну стійкість, яку має AES-128 у класичних умовах.

Асиметричні шифри. RSA. Суть алгоритму полягає у тому, що RSA базується на складності факторизації великих чисел.

Загроза від алгоритму Шора: алгоритм Шора здатний факторизувати великі числа за поліноміальний час, що робить RSA вразливим. Це означає, що квантові комп'ютери можуть розшифрувати повідомлення, зашифровані RSA, набагато швидше, ніж класичні комп'ютери.

Рекомендаціями для стійкості є: навіть збільшення розміру ключа RSA не зможе забезпечити захист від квантових атак, тому потрібно використовувати пост-квантові алгоритми.

Еліптичні криві (ECC). Суть алгоритму полягає у тому, що еліптичні криві використовуються для задачі дискретного логарифмування. Загроза від алгоритму Шора: Алгоритм Шора також здатний розв'язувати задачу дискретного логарифмування на еліптичних кривих, що робить ECC вразливими. Рекомендації для стійкості: як і у випадку з RSA, для забезпечення безпеки необхідно переходити на пост-квантові криптографічні рішення.

Пост-квантові шифри. Латичні криптосистеми (Lattice-based Cryptography) [13, 15]. Суть алгоритму: Базуються на задачах, таких як короткий вектор у ґратці (SVP) та найближчий вектор у ґратці (CVP), які вважаються складними навіть для квантових обчислень. Стійкість: Латичні алгоритми є одними з найбільш перспективних для захисту від квантових атак, оскільки жоден з відомих квантових алгоритмів не може ефективно розв'язувати ці задачі.

Кодові криптосистеми (Code-based Cryptography). Суть алгоритму: базуються на складності розв'язання задач декодування випадкових лінійних кодів. Стійкість: Code-based алгоритми, такі як McEliece, є стійкими до квантових атак, оскільки задачі, на яких вони базуються, залишаються складними для квантових комп'ютерів.

Хеш-криптосистеми (Hash-based Cryptography). Суть алгоритму: Використовують хеш-функції для створення цифрових підписів. Стійкість: Хеш-криптографія добре протистоїть квантовим атакам, хоча алгоритм Гровера може пришвидшити пошук колізій, що потребує збільшення довжини хешів для підтримання безпеки [7, 9].

Статистика щодо квантових атак та стійкості криптосистем. У сучасній криптографії велика увага приділяється тому, наскільки класичні та нові криптографічні алгоритми стійкі до квантових атак. Поява потужних квантових комп'ютерів може створити серйозну загрозу багатьом широко використовуваним системам шифрування. Розгляньмо статистику та поточний стан досліджень.

Швидкість квантових атак полягає у тому, що:

- алгоритм Шора, що застосовується для факторизації чисел, може зламати RSA-2048 за декілька годин при достатньо потужному квантовому комп'ютері з приблизно 20 мільйонами кубітів. Зараз існуючі квантові комп'ютери мають кілька сотень кубітів, що поки що недостатньо для такого зламу, але активні дослідження у цій галузі вказують на швидкий розвиток [11];

- алгоритм Гровера зменшує час грубої сили на пошук ключа з симетричних алгоритмів (наприклад, AES-256) до $\sqrt{N}$, що вдвічі скорочує ефективну довжину ключа (з AES-128 до AES-64) [11, 13].

Оцінка часу зламу класичних алгоритмів у тому, що класичні алгоритми, такі як ECC (еліптичні криві) і RSA, вважаються вразливими до зламу за допомогою квантових комп'ютерів, оскільки алгоритм Шора може вирішувати задачі, на яких базується їхня безпека. Згідно з оцінками, для зламу ECC-256 знадобиться квантовий комп'ютер з 2330 логічними кубітами.

Тому зростає потреба у пост-квантових алгоритмах, які можуть забезпечити безпеку навіть за умов появи більш потужних квантових комп'ютерів.

Використання пост-квантових алгоритмів здійснюється згідно з NIST (Національний інститут стандартів і технологій США), станом на 2023 рік активно досліджується більше 70 пост-квантових алгоритмів, з яких 4-6 є найбільш перспективними для стандартизації. Основні категорії включають латичні алгоритми, кодові системи, криптографію на базі багаточленів, та хеш-підписи.

Латичні алгоритми, такі як Kyber і Dilithium, показали стійкість до квантових атак на рівні завдань розв’язання задач найближчого вектора (SVP) і складних задач кодування.

Стійкість до квантових атак означає здатність криптографічного алгоритму залишатися безпечним навіть при використанні потужних квантових обчислень. Це досягається завдяки задачам, які є складними як для класичних, так і для квантових комп'ютерів. Ось деякі ключові аспекти:

Основні принципи. Латичні задачі. Це складні обчислювальні задачі, які включають пошук вектора у ґратці, що найближчий до заданого. Навіть квантові комп'ютери не можуть розв'язати ці задачі ефективно, що робить їх стійкими до квантових атак.

Математична складність, коли деякі алгоритми базуються на нових математичних задачах, таких як мультіваріативні рівняння або розв'язання систем поліномів, які є складними навіть для квантових комп'ютерів.

*Переваги пост-квантових шифрів. З*абезпечують захист не тільки від квантових атак, але й від класичних атак; можуть бути впроваджені у сучасні системи без кардинальних змін архітектури; надають можливість гнучкого підбору параметрів для досягнення бажаного рівня безпеки та ефективності.

Проблемами впровадження є те, що деякі пост-квантові алгоритми вимагають більше обчислювальних ресурсів, що може впливати на швидкість шифрування та розшифрування, також потрібно забезпечити сумісність з існуючими інфраструктурами, що може вимагати адаптації та стандартизації нових алгоритмів.

Стійкість до квантових атак є важливою умовою для забезпечення безпеки інформаційних систем у майбутньому. Розвиток пост-квантових криптографічних алгоритмів дозволить створити захищені протоколи, які залишатимуться надійними навіть в умовах розвитку квантових обчислень . Квантові атаки становлять серйозну загрозу для інформаційної безпеки, і прогнозується, що вони можуть вплинути на безпеку даних протягом наступного десятиліття. Експерти оцінюють ймовірність суттєвих загроз від квантових комп'ютерів у межах 50-70% протягом наступних п'яти років, що означає, що організації, які обробляють конфіденційну інформацію, повинні готуватися до цих загроз вже сьогодні [13 – 15].

Зараз глобальні збитки від кіберзлочинності, включаючи атаки, досягають 8 трильйонів доларів на рік, і цей показник прогнозують до зростання до 20 трильйонів доларів до 2026 року. Ці дані підкреслюють важливість захисту інформації, оскільки зростання квантових технологій може збільшити ризики для сучасних методів шифрування [13, 15].

Необхідно зазначити, що підготовка до квантових загроз включає в себе впровадження нових алгоритмів постквантової криптографії (PQC), які будуть затверджені Національним інститутом стандартів і технологій (NIST) у США. Ці нові стандарти планується реалізувати протягом наступних 3-10 років, щоб забезпечити безпеку даних в умовах зростання потужностей квантових комп'ютерів [12 – 15].

Потенційна статистика квантових атак. Зараз немає конкретних статистичних даних про кількість квантових атак, оскільки ця технологія ще не досягла стадії, коли її активно використовують зловмисники для кібератак. Однак існують прогнози, що з розвитком квантових технологій, особливо в галузі комп'ютерних обчислень, загрози зростатимуть.

Наприклад, деякі експерти вважають, що в найближчі 10-15 років квантові комп'ютери можуть стати достатньо потужними, щоб зламувати сучасні алгоритми шифрування. Зокрема, алгоритми, такі як RSA та еліптичні криві, які використовують асиметричну криптографію, можуть бути вразливими до атак за допомогою алгоритму Шора. Це означає, що шифри, які вважаються безпечними сьогодні, можуть стати ненадійними в майбутньому [15].

Висновки. У результаті проведеного дослідження можна зробити кілька важливих висновків щодо впливу квантових обчислень на сучасні криптографічні системи.

По-перше, квантові комп'ютери мають потенціал значно підвищити швидкість виконання певних математичних операцій, що ставить під загрозу традиційні криптографічні алгоритми, такі як RSA та ECC. Це підтверджується алгоритмами Шора і Гровера, які демонструють ефективність у факторизації великих чисел та пошуку в невпорядкованих базах даних відповідно.

По-друге, важливим аспектом є розробка криптографічних систем, стійких до квантових атак. Постквантова криптографія (PQC) стає все більш актуальною, оскільки забезпечує безпеку даних у нових умовах, де традиційні алгоритми більше не можуть гарантувати захист. Критерії стійкості до квантових атак включають відсутність відомих квантових атак, збереження стійкості до класичних атак та оптимальну ефективність нових алгоритмів.

Нарешті, необхідно зазначити, що загрози, які виникають у результаті розвитку квантових технологій, вимагають термінової адаптації та впровадження нових стандартів у сфері інформаційної безпеки. Уряди, організації та дослідники повинні активізувати зусилля для вивчення та реалізації постквантових криптографічних алгоритмів, щоб забезпечити захист важливих даних у майбутньому.

Квантові атаки, хоча поки що не є поширеними на практиці, мають значний потенціал, щоб вплинути на безпеку сучасних криптографічних систем. Оскільки квантові комп'ютери стають дедалі потужнішими, важливо розуміти, які загрози вони представляють і як це може змінити ландшафт кібербезпеки.

Хоча статистика зафіксованих квантових атак наразі відсутня, з розвитком технологій, ймовірність їх виникнення зростатиме, що робить актуальним питання впровадження пост-квантових алгоритмів для забезпечення безпеки даних у майбутньому.

Ця інформація підкреслює важливість підготовки до можливих загроз, пов'язаних з квантовими комп'ютерами, і необхідність адаптації існуючих криптографічних систем до нових викликів.

Тому напрямом подальших досліджень можуть бути розроблення сучасних методів квантової корекції помилок, які дозволяють виявляти й виправляти помилки, забезпечуючи стійкість обчислень, у тому числі з застосуванням алгебри підписів (Signature Algebra), яка надає формалізований підхід до перевірки коректності квантових станів і дозволяє локалізувати та виправляти помилки у реальному часі.

ЛІТЕРАТУРА

1. Adams, L. M., & Wilson, K. R. (2023). Квантові обчислення: нові горизонти в криптографії. Журнал інформаційних технологій та менеджменту, 15(3), 45-58.
2.Baker, S. J., & Turner, M. A. (2022). Криптографія в епоху квантових обчислень: виклики та рішення. Міжнародний журнал комп'ютерних наук, 25(2), 112-125.

3.Carter, D. R., & Peterson, H. G. (2021). Пост-квантова криптографія: нові алгоритми та їх реалізація. Журнал програмної інженерії та застосувань, 30(4), 210-225.
4.Hoffman, B. (2023). Квантові загрози для сучасної криптографії. IEEE Security & Privacy, 19(1), 34-40.
5. NIST. (2022). "Post-Quantum Cryptography: NIST's Post-Quantum Cryptography Standardization Process." National Institute of Standards and Technology.
6. Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
7. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
8. Henzinger, T. A., & Raghavan, P. (2019). Quantum Cryptography: A Survey. ACM Computing Surveys, 51(2), 1-32.
9. Rivest, R. L. (2015). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. Communications of the ACM, 58(8), 32-38.
10. Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.
11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
12. National Academies of Sciences, Engineering, and Medicine. (2018). Quantum Computing: Progress and Prospects. The National Academies Press. 13. European Commission. (2021). Quantum Technologies: A European Strategy. https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en.
14. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
15. National Security Agency (NSA). (2020). Post-Quantum Cryptography. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources.

REFERENCES

1. Adams, L. M., & Wilson, K. R. (2023). Квантові обчислення: нові горизонти в криптографії. Журнал інформаційних технологій та менеджменту, 15(3), 45-58.
2.Baker, S. J., & Turner, M. A. (2022). Криптографія в епоху квантових обчислень: виклики та рішення. Міжнародний журнал комп'ютерних наук, 25(2), 112-125.
3.Carter, D. R., & Peterson, H. G. (2021). Пост-квантова криптографія: нові алгоритми та їх реалізація. Журнал програмної інженерії та застосувань, 30(4), 210-225.
4.Hoffman, B. (2023). Квантові загрози для сучасної криптографії. IEEE Security & Privacy, 19(1), 34-40.
5. NIST. (2022). "Post-Quantum Cryptography: NIST's Post-Quantum Cryptography Standardization Process." National Institute of Standards and Technology.
6. Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
7. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
8. Henzinger, T. A., & Raghavan, P. (2019). Quantum Cryptography: A Survey. ACM Computing Surveys, 51(2), 1-32.
9. Rivest, R. L. (2015). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. Communications of the ACM, 58(8), 32-38.
10. Kaye, P., Laflamme, R., & Mosca, M. (2007). An Introduction to Quantum Computing. Oxford University Press.

11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
12. National Academies of Sciences, Engineering, and Medicine. (2018). Quantum Computing: Progress and Prospects. The National Academies Press. 13. European Commission. (2021). Quantum Technologies: A European Strategy. https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en.
14. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
15. National Security Agency (NSA). (2020). Post-Quantum Cryptography. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources.

Bohomia V.I., Cheremisina L.O., Yarmolatiy A. V

THREATS OF QUANTUM COMPUTING TO CLASSICAL CRYPTOGRAPHIC ALGORITHMS

With the advent of quantum computing technologies, which have the potential to perform calculations at much higher speeds than classical computers, a threat arises to current cryptographic systems. Quantum algorithms capable of efficiently solving complex computational problems that form the basis of the security of modern cryptographic systems pose a significant risk.

This means that as quantum computers advance, the compromise of many contemporary ciphers, which are currently considered secure, becomes possible. Given this, there is a need to develop new cryptographic methods and algorithms that remain resistant to quantum attacks. Post-quantum cryptography is a new direction in cryptographic science aimed at developing algorithms resistant to attacks by quantum computers. It encompasses a wide range of methods, such as lattice-based cryptosystems, error-correcting code-based cryptography, and many others.

Thus, the development of quantum computing technologies presents new challenges to cryptography, requiring a revision of existing methods for protecting information. There is a need to adapt cryptographic systems to new conditions, particularly through the creation of algorithms that remain reliable even in the presence of quantum computers.

Therefore, the relevance of this research lies in the necessity to protect information in the context of the rapid development of quantum computing systems. The scientific novelty of this study lies in the comprehensive analysis of post-quantum cryptosystems and their resistance to new types of threats. The research offers a comparison of the effectiveness of classical cryptographic methods with post-quantum ones, allowing the identification of their strengths and weaknesses in the context of quantum computing.

The practical significance of this research lies in the potential to use its results to implement new standards for cryptographic information protection. This is especially important for organizations that process confidential data, such as banks, government institutions, and companies involved in the development of artificial intelligence technologies.

Keywords: *quantum computing, classical cryptographic systems, threats, cryptographic algorithms, information security, quantum technologies.*