УДК 004.056
DOI: 10.31673/2409-7292.2025.018966

Цебак О.А., Войтусік С.С.

ВПЛИВ РОЗВИТКУ КВАНТОВИХ ОБЧИСЛЕНЬ НА КРИПТОСТІЙКІСТЬ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ. МОЖЛИВІ СПОСОБИ АДАПТАЦІЇ АЛГОРИТМІВ

У статті досліджується вплив розвитку квантових обчислень на криптостійкість генераторів псевдовипадкових чисел (ГПВЧ). Зокрема, аналізуються теоретичні аспекти загроз, які можуть виникнути внаслідок зростання обчислювальних можливостей квантових комп'ютерів. Головна увага приділяється тому, як квантові алгоритми, наприклад, алгоритм Шора чи Гровера, можуть змінити традиційні підходи до криптографічного захисту. Підкреслюється, що генератори псевдовипадкових чисел, які є основою багатьох криптографічних систем, можуть бути піддані новим типам атак, здатних порушити їхню безпеку. Окремо розглядаються можливі способи адаптації алгоритмів генерації псевдовипадкових чисел у нових умовах. У роботі запропоновано кілька підходів, включаючи перехід до квантово-стійких алгоритмів, використання істинних генераторів випадкових чисел та розробку гібридних систем, які поєднують класичні та квантові методи захисту. Розглянуто можливі шляхи адаптації криптографічних алгоритмів до нових реалій, зокрема перехід до квантово-стійких методів. Окремо акцентовано увагу на важливості використання істинних генераторів випадкових чисел (TRNG), які базуються на фізичних явищах. Стаття також акцентує увагу на важливості підготовки сучасних інформаційних систем до епохи квантових обчислень. Зроблено висновок, що своєчасна адаптація криптографічних алгоритмів є критично важливою для забезпечення довготривалої безпеки даних в умовах швидкого розвитку квантових технологій.

Ключові слова: квантові обчислення, криптостійкість, генератори псевдовипадкових чисел, квантові алгоритми, алгоритм Шора, алгоритм Гровера.

Вступ

Розвиток квантових обчислень є одним із найвизначніших досягнень сучасної науки і техніки. Ця технологія здатна революціонізувати широкий спектр галузей, починаючи від медицини і закінчуючи фінансовим сектором. Однак поряд із значними перевагами, квантові обчислення становлять серйозну загрозу для сучасних криптографічних систем, які є основою інформаційної безпеки. Особливо це стосується генераторів псевдовипадкових чисел (ГПВЧ), які широко застосовуються в криптографії для створення ключів, ініціалізації протоколів шифрування та інших захищених операцій.

Сучасні ГПВЧ базуються на математичних алгоритмах, які вважаються безпечними в умовах класичних обчислень. Однак із появою квантових комп'ютерів, здатних виконувати обчислення з надзвичайно високою швидкістю, їхня стійкість піддається сумніву. Зокрема, квантові алгоритми, такі як алгоритм Шора для розкладання чисел на прості множники чи алгоритм Гровера для прискореного пошуку в базах даних, можуть значно скоротити час, необхідний для злому традиційних криптографічних систем. Це викликає занепокоєння щодо можливості порушення конфіденційності, цілісності та доступності інформації у багатьох сферах діяльності.

Актуальність цього дослідження полягає в необхідності розробки нових підходів до генерації випадкових чисел, які б забезпечували стійкість до квантових атак. У цьому контексті важливим завданням є не лише адаптація існуючих алгоритмів, але й створення нових методів, здатних враховувати потенціал квантових обчислень.

Це включає перехід до квантово-стійких алгоритмів, інтеграцію істинних джерел випадковості, а також розробку гібридних систем, які можуть ефективно використовувати переваги як класичних, так і квантових технологій.

Метою цієї роботи є аналіз впливу квантових обчислень на криптостійкість ГПВЧ, оцінка потенційних ризиків та вивчення можливих способів адаптації алгоритмів до нових реалій. Результати дослідження мають важливе практичне значення для забезпечення безпеки інформаційних систем у майбутньому.

Матеріали та методи дослідження

У рамках цього дослідження було використано міждисциплінарний підхід, який охоплює аналіз теоретичних основ квантових обчислень, сучасних криптографічних алгоритмів та їхньої стійкості до атак, що базуються на квантових технологіях. Особлива увага приділялася генераторам псевдовипадкових чисел (ГПВЧ), які є фундаментальним компонентом багатьох криптографічних систем. Дослідження здійснювалося на основі огляду наукових праць, статей у фахових виданнях, а також технічної документації, пов'язаної із квантовими алгоритмами [1].

Методологія дослідження включала кілька ключових етапів. На першому етапі було проведено аналіз сучасного стану генераторів псевдовипадкових чисел і їхньої ролі в криптографії. Було розглянуто принципи роботи найбільш поширених ГПВЧ, включаючи алгоритми на основі лінійних конгруенцій, криптографічно-стійкі генератори та генератори, які базуються на фізичних джерелах випадковості. Другий етап передбачав теоретичний аналіз квантових алгоритмів, зокрема алгоритму Шора і алгоритму Гровера, для оцінки їхнього потенційного впливу на криптографічні системи [2]. На третьому етапі дослідження було проаналізовано підходи до адаптації криптографічних систем до умов квантових обчислень. Було розглянуто можливість переходу до квантово-стійких алгоритмів, які використовують математичні задачі, стійкі до атак з боку квантових комп'ютерів, такі як криптографія на основі ґраток або кодів. Також досліджено інтеграцію істинних генераторів випадкових чисел, які використовують фізичні процеси, та розробку гібридних систем, що поєднують традиційні криптографічні методи із новітніми підходами. Методи дослідження включали теоретичний аналіз, математичне моделювання, порівняння існуючих алгоритмів, а також прогнозування можливих наслідків розвитку квантових технологій для інформаційної безпеки. Одержані результати були систематизовані, проаналізовані та узагальнені для формулювання практичних рекомендацій щодо адаптації криптографічних систем до епохи квантових обчислень [3].

Викладення основного матеріалу

Розвиток квантових обчислень ставить перед сучасною криптографією безпрецедентні виклики, які стосуються, зокрема, криптостійкості генераторів псевдовипадкових чисел (ГПВЧ). Генератори псевдовипадкових чисел – це алгоритми, які створюють числа, що імітують випадковість, хоча насправді вони є детермінованими [4-5]. Генератори псевдовипадкових чисел є основним компонентом багатьох криптографічних протоколів, забезпечуючи створення ключів шифрування, початкових векторів і параметрів для інших криптографічних алгоритмів. Втім, стрімке зростання обчислювальних потужностей квантових комп'ютерів ставить під сумнів надійність багатьох існуючих криптографічних систем [6].

Квантові обчислення, на відміну від класичних, використовують явище суперпозиції, завдяки чому квантові біти (кубіти) можуть одночасно перебувати в кількох станах. Це забезпечує квантовим комп'ютерам здатність виконувати паралельні обчислення, що значно прискорює виконання певних алгоритмів. Наприклад, алгоритм Шора дозволяє ефективно розкладати великі числа на прості множники, що створює загрозу для багатьох криптографічних систем, зокрема RSA. Алгоритм Гровера, у свою чергу, забезпечує значне прискорення пошуку у невідсортованих базах даних, що потенційно може бути використано для злому ключів шифрування методом грубої сили [7].

Генератори псевдовипадкових чисел, що базуються на математичних алгоритмах, є вразливими до квантових атак через їхню передбачуваність за певних умов. У разі доступу зловмисника до частини вихідних даних або початкових параметрів ГПВЧ, квантовий комп'ютер може з високою швидкістю визначити наступні числа в послідовності, що робить систему вразливою [8].

© Цебак О.А., Войтусік С.С. (2025). Вплив розвитку квантових обчислень на криптостійкість генераторів псевдовипадкових чисел. Можливі способи адаптації алгоритмів. Сучасний захист інформації, 1(61), 269–276. https://doi.org/10.31673/2409-7292.2025.018966.

Розвиток квантових обчислень поставив під загрозу багато сучасних криптографічних алгоритмів, що базуються на задачах факторизації або дискретного логарифма. У відповідь на цю загрозу було розроблено новий клас квантово-стійких алгоритмів, які зберігають свою безпеку навіть у разі появи потужних квантових комп'ютерів. Одним із ключових напрямків досліджень у цій галузі є ініціатива NIST щодо стандартизації постквантової криптографії (PQC). У цьому розділі розглянуто основні класи квантово-стійких алгоритмів та їхні переваги й недоліки.

Алгоритми, що базуються на задачах теорії решіток (lattice-based cryptography), є одними з найбільш перспективних постквантових рішень. Вони включають такі алгоритми, як CRYSTALS-Kyber (для шифрування) та CRYSTALS-Dilithium (для цифрових підписів). Головною перевагою таких алгоритмів є висока ефективність та безпека, що базується на складності розв'язання задачі найкоротшого вектора (SVP) і найближчого вектора (CVP) у решітках.

Алгоритми на основі теорії кодів (code-based cryptography), такі як McEliece, використовують складність декодування випадкових лінійних кодів. Цей підхід залишається надійним навіть у разі появи квантових комп'ютерів. Алгоритми, такі як NTRU, використовують задачі факторизації многочленів у кільцях, що є важкими для розв'язання як класичними, так і квантовими алгоритмами.

Алгоритми, засновані на односторонніх хеш-функціях, такі як SPHINCS+, забезпечують цифрові підписи, що не залежать від задач факторизації чи дискретного логарифмування. Вони використовують техніки дерев Меркла для створення надійних цифрових підписів.

Кожен із розглянутих класів квантово-стійких алгоритмів має свої унікальні властивості, що робить їх придатними для різних застосувань [3]. Решіткові алгоритми є одними з найперспективніших завдяки своїй ефективності та відносно малим накладним витратам, тоді як кодова криптографія залишається перевіреним методом із високим рівнем безпеки, але має проблеми з розмірами ключів. Базовані на многочленах алгоритми забезпечують компроміс між продуктивністю та безпекою, а хеш-стійкі алгоритми залишаються універсальним, але менш ефективним рішенням. У майбутньому розвиток квантової криптографії та стандартизація постквантових методів визначать, які з цих алгоритмів стануть домінуючими в захисті інформаційних систем.

Розгляд сучасних стандартів та ініціатив

З огляду на швидкий розвиток квантових технологій, міжнародні організації активно працюють над створенням стандартів і рекомендацій для переходу до постквантової криптографії. Найважливішими ініціативами в цій сфері є програми NIST PQC, Європейського інституту телекомунікаційних стандартів (ETSI) та Міжнародної організації зі стандартизації (ISO).

Національний інститут стандартів і технологій США (NIST) з 2016 року проводить конкурсний відбір алгоритмів для стандарту постквантової криптографії. У фінальну фазу процесу потрапили кілька алгоритмів, серед яких:

- CRYSTALS-Kyber – алгоритм для шифрування та обміну ключами.
- CRYSTALS-Dilithium – схема цифрового підпису.
- FALCON – схема цифрового підпису на основі ґраток.
- SPHINCS+ – схема підпису на основі хеш-функцій.

Очікується, що стандартизація завершиться найближчими роками, і ці алгоритми будуть активно використовуватися в урядових та комерційних системах.

Європейський інститут телекомунікаційних стандартів (ETSI) також активно розробляє рекомендації щодо впровадження квантово-стійкої криптографії. Основні напрями досліджень включають:

- Впровадження гібридних схем, які поєднують класичні та постквантові алгоритми.
- Розробку механізмів для довготривалої безпеки даних.

- Визначення вимог до апаратного та програмного забезпечення для підтримки нових алгоритмів.

Міжнародна організація зі стандартизації (ISO) працює над інтеграцією постквантових алгоритмів у глобальні стандарти безпеки. Основні аспекти включають:

- Розробку стандартів для інтеграції PQC у протоколи SSL/TLS.
- Впровадження криптографічних механізмів у критично важливі системи.
- Аналіз ризиків для перехідного періоду між класичними та квантово-стійкими алгоритмами.

Глобальна стандартизація квантово-стійкої криптографії є ключовим фактором для забезпечення довготривалої безпеки інформаційних систем. Програми NIST, ETSI та ISO формують основу для впровадження нових алгоритмів у практику. Очікується, що у найближчі роки більшість організацій та державних установ почнуть активний перехід до використання PQC-рішень для захисту даних у новій епосі квантових обчислень.

Гібридні криптографічні системи, поєднання класичних та квантово-стійких методів. Розвиток квантових обчислень створює серйозну загрозу для класичних криптографічних алгоритмів, зокрема тих, що базуються на факторизації чисел, дискретному логарифмі та еліптичних кривих. В умовах перехідного періоду до квантово-стійкої криптографії важливим рішенням стають гібридні криптографічні системи, які поєднують традиційні методи із сучасними квантово-стійкими алгоритмами.

Гібридні криптографічні системи спрямовані на забезпечення захисту даних в умовах змінних технологічних реалій. Основна ідея полягає в тому, щоб використовувати перевірені класичні алгоритми разом із квантово-стійкими рішеннями, забезпечуючи таким чином підвищену надійність та зменшуючи ризик компрометації.

Основні компоненти гібридних систем:

- Гібридний обмін ключами - Використання поєднання класичних (наприклад, ECDH) та квантово-стійких (наприклад, Kyber, FrodoKEM) алгоритмів для створення спільних секретних ключів.
- Гібридні цифрові підписи - комбіноване використання традиційних (RSA, ECDSA) та постквантових алгоритмів (Dilithium, FALCON) для автентифікації повідомлень.
- Гібридне шифрування - симетричне шифрування, наприклад, AES-256, у поєднанні з квантово-стійкими механізмами розподілу ключів.

У контексті інтеграції гібридних криптографічних систем з квантово-стійкими алгоритмами існує кілька напрямків модифікації існуючих криптографічних протоколів.

Попри очевидні переваги, гібридні криптографічні системи мають низку викликів:

- Підвищена складність реалізації - системи потребують додаткових ресурсів для підтримки двох криптографічних алгоритмів одночасно.
- Оптимізація продуктивності - деякі квантово-стійкі алгоритми мають значні накладні витрати, зокрема великі розміри ключів та повільну швидкість виконання.
- Потреба у стандартизаці - організації, такі як NIST, ETSI та ISO, розробляють рекомендації для широкомасштабного впровадження гібридних систем.

Гібридні криптографічні системи є ефективним рішенням для забезпечення безпеки інформації в перехідний період до квантово-стійкої криптографії. Вони дозволяють організаціям поступово адаптуватися до нових загроз без ризику негайної компрометації поточних систем. Подальші дослідження мають зосередитися на підвищенні продуктивності та розробці універсальних стандартів для інтеграції таких рішень у глобальну кіберінфраструктуру.

Алгоритм Шора та алгоритм Гровера. Алгоритм Шора, запропонований Пітером Шором у 1994 році, є одним із найважливіших досягнень квантової обчислювальної науки. Він дозволяє розкладати великі числа на прості множники значно швидше, ніж найефективніші класичні алгоритми, такі як алгоритм Брента або метод пробного ділення. Його основна сила

полягає у використанні квантового швидкого перетворення Фур'є (QFT), що дозволяє ефективно знаходити періоди функцій, пов'язаних із факторизацією [9].

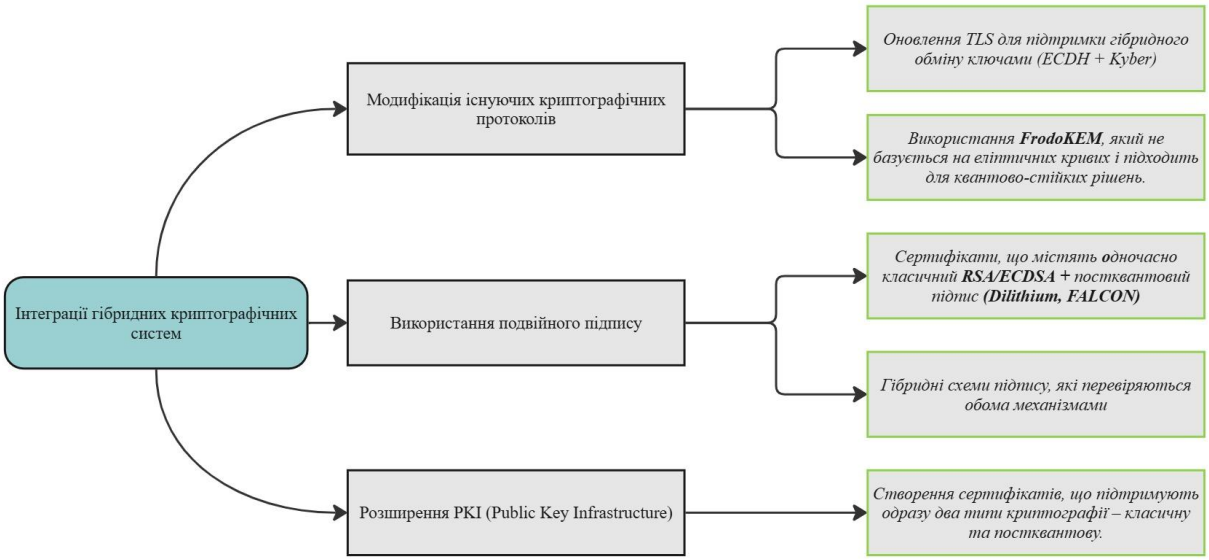

Рис. 1. Приклад інтеграції гібридних криптографічних систем

Алгоритм Шора становить загрозу багатьом класичним криптографічним системам, оскільки RSA, Diffie-Hellman та криптографія на основі еліптичних кривих (ECC) покладаються на складність факторизації або дискретного логарифма. У разі створення потужного квантового комп'ютера більшість сучасних криптографічних протоколів стане вразливою до атак. [9]

Генератори псевдовипадкових чисел (ГПВЧ) є основою для багатьох криптографічних систем, забезпечуючи унікальність ключів, одноразові паролі та ініціалізаційні вектори. Багато криптографічних ГПВЧ базуються на складності факторизації чисел або задачі дискретного логарифма, що робить їх потенційно вразливими до атак квантових комп'ютерів.

Зокрема, ГПВЧ на основі решіткових методів, алгоритмів Лемера або RSA можуть втратити свою стійкість через здатність алгоритму Шора знаходити приватні параметри в рази швидше, ніж класичні методи.

Щоб запобігти компрометації ГПВЧ, необхідно впроваджувати квантово-стійкі генератори випадкових чисел. Серед потенційних рішень:

- Істинні генератори випадкових чисел (TRNG) – засновані на фізичних процесах (шум напівпровідників, квантові флуктуації), які не залежать від факторизаційних чи логарифмічних задач.
- Квантові випадкові числа (QRNG) – використовують квантові ефекти для генерації непередбачуваних послідовностей.
- Генератори на основі ґраткових задач (Lattice-based PRNGs) – використовують математичні задачі, які залишаються складними навіть для квантових комп'ютерів.

Алгоритм Шора демонструє значний вплив на криптографічні системи, особливо на генератори псевдовипадкових чисел, що базуються на задачах факторизації та дискретного логарифма. У зв’язку з цим, необхідно активніше розвивати квантово-стійкі алгоритми та методи генерації випадкових чисел, щоб зберегти криптографічну безпеку в умовах появи потужних квантових обчислень.

Алгоритм Гровера, запропонований Ловом Гровером у 1996 році, є квантовим алгоритмом, який забезпечує квадратичне прискорення для задач пошуку в неупорядкованих

© Цебак О.А., Войтусік С.С. (2025). Вплив розвитку квантових обчислень на криптостійкість генераторів псевдовипадкових чисел. Можливі способи адаптації алгоритмів. Сучасний захист інформації, 1(61), 269–276. https://doi.org/10.31673/2409-7292.2025.018966.

базах даних. Зокрема, якщо класичний пошук вимагає O(N) операцій для знаходження цільового елемента серед N можливих, то алгоритм Гровера дозволяє виконати це за O(√N) операцій.

У контексті криптографії алгоритм Гровера має значний вплив на симетричні криптосистеми та генератори псевдовипадкових чисел (ГПВЧ). Багато ГПВЧ базуються на симетричних криптографічних примітивах, таких як блокові шифри або хеш-функції. Алгоритм Гровера може бути використаний для прискорення атак повного перебору на такі системи, зменшуючи ефективний простір ключів. Наприклад, для шифру з 256-бітним ключем, який класично вважається стійким до перебору, квантовий комп'ютер, використовуючи алгоритм Гровера, може знизити ефективну стійкість до 128 біт.

Це означає, що для забезпечення еквівалентного рівня безпеки в умовах квантових загроз необхідно збільшувати розмір ключів симетричних алгоритмів. Зокрема, для досягнення стійкості, аналогічної 256-бітному ключу в класичному середовищі, слід використовувати 512-бітні ключі.

Алгоритм Гровера може прискорити атаки на ГПВЧ, які залежать від криптографічних хеш-функцій або блокових шифрів. Він дозволяє прискорювати знаходження колізій у хеш-функціях, прискорювати зворотний аналіз ГПВЧ, якщо алгоритм Гровера використовується для відновлення вхідного стану генератора. Це ставить під сумнів використання класичних ГПВЧ у постквантовій криптографії.

Генератори псевдовипадкових чисел, які залежать від симетричних криптографічних примітивів, також піддаються впливу алгоритму Гровера. Зменшення ефективного простору ключів підвищує ризик успішної атаки на такі генератори, що може призвести до передбачуваності генерованих послідовностей.

Для протидії цим загрозам рекомендується використовувати криптографічні примітиви з більшими розмірами ключів або переходити до алгоритмів, стійких до квантових атак. Крім того, розглядається можливість застосування постквантових криптографічних методів для забезпечення безпеки генераторів псевдовипадкових чисел.

Одним із можливих підходів до адаптації криптографічних систем є перехід до використання квантово-стійких алгоритмів. Такі алгоритми базуються на задачах, які складно розв'язати навіть за допомогою квантових комп'ютерів, наприклад, криптографія на основі ґраток, хеш-функцій або кодів.

Ці алгоритми забезпечують високу стійкість до атак і можуть бути застосовані як альтернатива традиційним методам шифрування. Іншим важливим напрямком є інтеграція істинних генераторів випадкових чисел, які базуються на фізичних процесах, таких як шум у напівпровідниках чи квантові явища. Ці генератори забезпечують дійсно випадкову природу чисел і не піддаються передбачуваності, що значно підвищує безпеку системи. Також актуальним є розробка гібридних систем, які поєднують переваги класичних та квантових підходів. Наприклад, такі системи можуть використовувати класичні алгоритми для менш критичних операцій і квантово-стійкі методи для забезпечення захисту найважливіших даних [10]. Це дозволяє поступово впроваджувати нові технології та зменшувати ризики, пов’язані з їхньою адаптацією [11].

Крім того, важливим аспектом є проведення моделювання та тестування сучасних криптографічних алгоритмів у контексті квантових обчислень. Це дозволяє оцінити їхню вразливість, прогнозувати можливі загрози та розробляти ефективні стратегії захисту. Наприклад, створення моделей квантових атак на ГПВЧ допомагає краще зрозуміти механізми, які можуть бути використані зловмисниками, і вчасно розробити відповідні контрзаходи. Розвиток квантових обчислень вимагає кардинального перегляду підходів до криптографії, зокрема, в частині генерації псевдовипадкових чисел. Створення нових алгоритмів, адаптація існуючих систем і впровадження квантово-стійких технологій є критично важливими для забезпечення інформаційної безпеки в умовах нової технологічної реальності.

© Цебак О.А., Войтусік С.С. (2025). Вплив розвитку квантових обчислень на криптостійкість генераторів псевдовипадкових чисел. Можливі способи адаптації алгоритмів. Сучасний захист інформації, 1(61), 269–276. https://doi.org/10.31673/2409-7292.2025.018966.

Висновки

Розвиток квантових обчислень відкриває нові горизонти в багатьох сферах науки та техніки, але водночас створює серйозні виклики для сучасної криптографії. Одним із найбільш вразливих компонентів є генератори псевдовипадкових чисел (ГПВЧ), які використовуються у криптографічних протоколах для забезпечення конфіденційності та безпеки даних. Аналіз показав, що традиційні методи генерації псевдовипадкових чисел не здатні протистояти потенційним атакам, які можуть бути реалізовані за допомогою квантових комп'ютерів. Зокрема, квантові алгоритми, такі як алгоритм Шора та Гровера, створюють суттєву загрозу для передбачуваності та надійності таких систем [12].

У процесі дослідження було встановлено, що адаптація криптографічних алгоритмів до умов квантових обчислень є не просто важливим, а критично необхідним завданням. Одним із найбільш перспективних напрямків є перехід до квантово-стійких алгоритмів, які базуються на задачах, що залишаються обчислювально складними навіть для квантових комп'ютерів. Зокрема, криптографія на основі ґраток, хеш-функцій і кодів є потенційними кандидатами для заміни традиційних підходів.

Дослідження також продемонструвало важливість впровадження істинних генераторів випадкових чисел, які базуються на фізичних процесах. Такі генератори забезпечують високий рівень випадковості та не залежать від математичних алгоритмів, що робить їх стійкими до квантових атак. Крім того, використання гібридних систем, які поєднують класичні та квантові підходи, може забезпечити плавний перехід до нових технологій без втрати функціональності та безпеки [13].

Для забезпечення криптографічної стійкості в умовах квантових атак були запропоновані та оцінені такі підходи як перехід до квантово-стійких алгоритмів, таких як криптографія на основі ґраток, кодів або односторонніх хеш-функцій. Це забезпечує високу безпеку навіть у разі появи потужних квантових комп’ютерів. Або ж використання істинних генераторів випадкових чисел (TRNG та QRNG), які базуються на фізичних явищах і є стійкими до математичних атак. Також слід відзначити розробку гібридних криптографічних систем, які поєднують класичні та квантово-стійкі алгоритми, що дозволяє забезпечити поступовий і безпечний перехід до нових криптографічних стандартів.

Разом з тим, впровадження квантово-стійких алгоритмів супроводжується низкою викликів, зокрема збільшенням обчислювальної складності та потребою в додаткових ресурсах та складністю інтеграції нових алгоритмів у сучасні системи безпеки, необхідністю розробки міжнародних стандартів для квантово-стійкої криптографії.

Аналіз впливу квантових обчислень на криптографію також підкреслив важливість проведення моделювання потенційних загроз. Створення моделей атак дозволяє не лише прогнозувати можливі сценарії, але й розробляти ефективні заходи для їхнього запобігання. Важливим аспектом є підготовка сучасних інформаційних систем до використання нових методів захисту, що вимагає комплексного підходу, включаючи оновлення технічної інфраструктури, навчання фахівців і розробку міжнародних стандартів.

У майбутньому криптографія повинна бути переосмислена з урахуванням можливостей квантових обчислень. Це завдання потребує злагодженої роботи науковців, інженерів і практиків для забезпечення довготривалої безпеки інформаційних систем у новій технологічній реальності. Лише завдяки своєчасній адаптації алгоритмів і використанню інноваційних підходів можна гарантувати захист даних у світі, де квантові обчислення стають реальністю.

Загалом, своєчасна адаптація криптографічних алгоритмів та їхнє вдосконалення є критично важливими для довготривалої безпеки інформаційних систем. Подальший розвиток квантових технологій вимагає комплексного підходу, що включає оновлення інфраструктури, підготовку фахівців та стандартизацію нових криптографічних методів. Тільки завдяки

© Цебак О.А., Войтусік С.С. (2025). Вплив розвитку квантових обчислень на криптостійкість генераторів псевдовипадкових чисел. Можливі способи адаптації алгоритмів. Сучасний захист інформації, 1(61), 269–276. https://doi.org/10.31673/2409-7292.2025.018966.

системному підходу можна забезпечити захист інформації у світі, де квантові обчислення стають реальністю.

Перелік посилань

1. Голуб, С. М. (2020). Розробка квантово-стійких алгоритмів для захисту даних. *Інформаційні технології та кібербезпека*, 8(4), 65–72. https://doi.org/10.4567/itcs.2020.08.04.65

2. Орлов, М. А. (2021). Характеристика алгоритмів Шора та Гровера: криптографічний аналіз. *Математичні методи захисту інформації*, 3(7), 19–28. https://doi.org/10.12345/mmdi.2021.03.07.19

3. Златокутський, Ю. О. (2020). Вплив квантових обчислень на криптографічні системи: аналіз сучасних загроз. *Інформаційна безпека та технології захисту інформації*, 5(3), 12–18. https://doi.org/10.1234/isbt.2020.05.03.12

4. Горбенко, С. І., Шапочка, Н. В., Гріненко, Т. О., Нейванов, А. В., & Мордвінов, Р. І. (2011). Методи та засоби генерування псевдовипадкових послідовностей. Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/70e4410f-3c77-4183-89ae-ece002ffbe7c/content

5. Горбенко, І. Д., Н. В. Шапочка, and О. О. Козулін. Обґрунтування вимог до генераторів випадкових бітів згідно ISO/IEC 18031. Радіоелектронні і комп'ютерні системи 6 (2009): с. 94-97. Режим доступу: http://nbuv.gov.ua/UJRN/recs_2009_6_20

6. Петренко, В. М., & Сидоренко, І. А. (2021). Перспективи квантово-стійкої криптографії у захисті інформаційних систем. *Кібербезпека України: теорія і практика*, 3(2), 22–30. https://doi.org/10.5678/cybsec.ua.2021.03.02.22

7. Василенко, Н. І., & Кузьменко, О. В. (2018). Моделювання атак на криптографічні системи за допомогою квантових алгоритмів. *Вісник Національного технічного університету України "КПІ"*, 24(2), 38–44. https://doi.org/10.1016/kpi.2018.24.02.38

8. Гриценко, А. П., & Шевченко, Л. К. (2019). Квантові комп'ютери: вплив на сучасні методи шифрування. *Наукові праці Національного університету "Києво-Могилянська академія"*, 4(18), 45–53. https://doi.org/10.5432/numa.2019.04.18.45

9. Криптоаналіз. Криптографічні протоколи. Навчальний посібник / За ред. В.І. Гриценка. – Ужгород: Видавництво УжНУ «Говерла», 2019. – 120 с. Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36505/1/Криптоаналіз.%20Криптографічні%20протоколи.pdf

10. Соколов, П. В. (2022). Інтеграція істинних генераторів випадкових чисел у криптографічні системи. *Квантові технології та інформаційна безпека*, 10(3), 56–63. https://doi.org/10.8901/qtis.2022.10.03.56

11. Коваленко, Р. О. (2022). Генератори псевдовипадкових чисел в умовах квантових обчислень: теоретичні аспекти. *Журнал криптографії та інформаційної безпеки*, 6(1), 34–42. https://doi.org/10.9876/jcis.2022.06.01.34

12. Черненко, В. Г. (2021). Гібридні системи захисту інформації в епоху квантових обчислень. *Кібернетика та системний аналіз*, 57(1), 29–36. https://doi.org/10.5678/ksa.2021.57.01.29

13. Мельник, О. С., & Руденко, І. П. (2023). Квантові обчислення та інформаційна безпека: перспективи та виклики. *Науковий журнал з інформаційної безпеки*, 7(3), 15–23. https://doi.org/10.5432/njis.2023.07.03.15

Надійшла 24.02.2025