УДК 004.02
DOI https://doi.org/10.32782/IT/2025-1-3

Володимир БОГОМ'Я
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0000-0003-4403-3130*
***Scopus Author ID:** 51863292100*

Любов ЧЕРЕМІСІНА
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0009-0005-0719-0745*

Андрій ЯРМОЛАТІЙ
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0009-0004-8655-9928*

Бібліографічний опис статті: Богом'я, В., Черемісіна, Л., Ярмолатій, А. (2025). Дослідження впливу квантових обчислень на стеганографію. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 18–25, doi: https://doi.org/10.32782/IT/2025-1-3

ДОСЛІДЖЕННЯ ВПЛИВУ КВАНТОВИХ ОБЧИСЛЕНЬ НА СТЕГАНОГРАФІЮ

З появою квантових обчислювальних технологій, що мають потенціал обчислювати з набагато більшою швидкістю, ніж класичні комп'ютери класична стеганографія стикається з новими загрозами, які ускладнюють приховування інформації. Водночас це стимулює розвиток нових підходів, таких як постквантова стеганографія, яка враховує потенціал квантових обчислень.

Але, виявляється, що квантові обчислення мають потенціал радикально змінити багато аспектів криптографії, а стеганографія, яка використовується для приховування інформації, також може зазнати впливу.

***Мета роботи.** Аналіз особливостей впливу найвідомішої реалізації квантової криптографії, як квантовий розподіл ключів (Quantum Key Distribution для розробки рекомендацій щодо підвищення ефективності стеганографічних методів.*

***Методологія дослідження.** Для дослідження впливу квантових обчислень на стеганографію розглянуто застосування різноманітних методів, залежно від конкретних цілей дослідження та доступних ресурсів, а саме: математичне моделювання стеганографічних алгоритмів, аналіз вразливостей перед квантовими алгоритмами, розробка квантових атак на стеганографічні методи та інші.*

***Наукова новизна.** Авторами у цієї проблематиці були визначені основні криптографічні системи, що забезпечують захист інформації в умовах квантових загроз, у тому числі особливості квантової криптографії. Також наведені основні особливості квантових обчислень, такі як суперпозиція, заплутаність та зв'язаність.*

Як результати дослідження можуть бути такі. Нарешті, необхідно зазначити, що загрози, які виникають у результаті розвитку квантових технологій, вимагають термінової адаптації та впровадження нових стандартів у сфері інформаційної безпеки.

Інтеграція QKD і стеганографії є багатообіцяючим напрямком, що може знайти застосування в захищених комунікаціях, зокрема в дипломатії, оборонній сфері та приватних зв'язках.

***Висновки.** Квантова механіка пропонує високий рівень випадковості, який може бути використаний для підвищення надійності приховування інформації за рахунок переваг квантового випадкового шуму. Це дозволяє створювати більш стійкі до виявлення стеганографічні системи.*

Потенційні напрямами подальших досліджень можуть бути: вивчення інтеграції квантових методів з класичною стеганографією; аналіз безпеки стеганографічних методів у постквантовий період; розробка квантових протоколів стеганографії; оцінка впливу квантового шуму на приховування та виявлення інформації для захисту систем електронної комерції

***Ключові слова:** квантові обчислення, квантові технології, стеганографія, стеганографічні методи, криптографічні алгоритми, інформаційна безпека, захист електронної комерції.*

Volodymyr BOHOMYA
Doctor of Technical Sciences, Professor, Professor at the Department of Cyber Security, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, bog260341@gmail.com
***ORCID:** 0000-0003-4403-3130*
***Scopus Author ID:** 51863292100*

Liubov CHEREMISINA
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, cheremisina1112@gmail.com
***ORCID:** 0009-0005-0719-0745*

Andrii YARMOLATII
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, ayarmolatii@gmail.com
***ORCID:** 0009-0004-8655-9928*

To cite this article: Bohomya, V., Cheremisina, L., Yarmolatii, A. (2025). Doslidzhennya vplyvu kvantovykh obchyslen' na stehanohrafiyu [Study of the impact of quantum computing on steganography]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 18–25, doi: https://doi.org/10.32782/IT/2025-1-3

STUDY OF THE IMPACT OF QUANTUM COMPUTING ON STEGANOGRAPHY

With the advent of quantum computing technologies, which have the potential to compute at a much higher speed than classical computers, classical steganography faces new threats that make it difficult to hide information. At the same time, it stimulates the development of new approaches, such as post-quantum steganography, which takes into account the potential of quantum computing.

But, it turns out that quantum computing has the potential to radically change many aspects of cryptography, and steganography, which is used to hide information, could also be affected.

***Purpose of the work.** Analysis of the features of the impact of the most famous implementation of quantum cryptography, such as Quantum Key Distribution (Quantum Key Distribution for the development of recommendations for increasing the efficiency of steganographic methods.*

***Research methodology.** To study the impact of quantum computing on steganography, the application of various methods is considered, depending on the specific goals of the study and available resources, namely: mathematical modeling of steganographic algorithms, analysis of vulnerabilities to quantum algorithms, development of quantum attacks on steganographic methods, and others.*

***Scientific novelty.** The authors of this issue identified the main cryptographic systems that provide information protection in the face of quantum threats, including the features of quantum cryptography. The main features of quantum computing are also given, such as superposition, entanglement, and coherence.*

As the results of the study may be as follows. Finally, it should be noted that the threats that arise as a result of the development of quantum technologies require urgent adaptation and implementation of new standards in the field of information security. The integration of QKD and steganography is a promising area that could find applications in secure communications, particularly in diplomacy, defense and private relations.

***Conclusions.** Quantum mechanics offers a high level of randomness that can be used to improve the reliability of hiding information at the expense of the advantages of quantum random noise. This allows for more detection-resistant steganographic systems.*

Potential areas for further research may be: the study of the integration of quantum methods with classical steganography; analysis of the safety of steganographic methods in the post-quantum period; development of quantum steganography protocols; Assessing the impact of quantum noise on information concealment and detection to protect e-commerce systems

***Key words:** quantum computing, quantum technologies, steganography, steganographic methods, cryptographic algorithms, information security, protection of e-commerce systems.*

Постановка проблеми. 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, електронна комерція,

медицина, державне управління, безпеки та оборони тощо (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996; Bennett, Brassard, 1984; Gottesman, 2009; Raussendorf, Harrington, 2007).

З появою квантових обчислювальних технологій, що мають потенціал обчислювати з набагато більшою швидкістю, ніж класичні комп'ютери класична стеганографія стикається з новими загрозами, які ускладнюють приховування інформації. Водночас це стимулює розвиток нових підходів, таких як постквантова стеганографія, яка враховує потенціал квантових обчислень (Shor, 1995).

Аналіз останніх досліджень і публікацій. Авторами (Nielsen, Chuang, 2010; Shor, 1995) були визначені криптографічні системи, що забезпечують захист інформації в умовах квантових загроз, у тому числі квантова криптографія. Також наведені основні особливості квантових обчислень, такі як суперпозиція, заплутаність та зв'язаність (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996; Bennett, Brassard, 1984; Ekert, 1991).

Крім того, визначено можливості подальшого розвитку сучасної стеганографії (Gottesman, 2009; Raussendorf, Harrington, 2007; Preskill, 2018).

Проаналізовано типи квантових помилок і наведено особливості способів їхнього виявлення, наведено методи реалізації квантової корекції на практичних платформах, таких як IBM Qiskit, проаналізовано сумісність алгебри підписів із найновішими квантовими протоколами, такими як BB84, E91, DI-QKD, QSS і BQC (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996; Bennett, Brassard, 1984; Gottesman, 2009; Raussendorf, Harrington, 2007, Preskill, 2018).

Квантові обчислення мають потенціал радикально змінити багато аспектів криптографії, а стеганографія, яка використовується для приховування інформації, також може зазнати впливу.

Враховуючи вищезазначене, актуальність теми дослідження зводиться до аналізу особливостей приховування інформації в умовах швидкого розвитку квантових обчислювальних систем.

Мета статті – проаналізувати особливості впливу найвідомішої реалізації квантової криптографії, як квантовий розподіл ключів (Quantum Key Distribution для розробки рекомендацій щодо підвищення ефективності стеганографічних методів.

Виклад основного матеріалу дослідження. Розвиток квантових обчислень ставить під загрози багато сучасних криптографічних систем, що використовуються для захисту даних у цифровому середовищі. Причиною загроз є здатність квантових комп'ютерів виконувати обчислення набагато швидше, ніж класичні комп'ютери, що значно знижує стійкість традиційних криптографічних алгоритмів (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996; Bennett, Brassard, 1984; Gottesman, 2009; Raussendorf, Harrington, 2007, Preskill, 2018).

Квантова криптографія (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996) використовує такі принципи квантової механіки, як суперпозиція та квантове заплутування, для створення захищених каналів зв'язку. Основна ідея зводиться до того, що квантові стани неможливо вимірювати або спостерігати за ними без їх зміни. Така властивість робить можливим

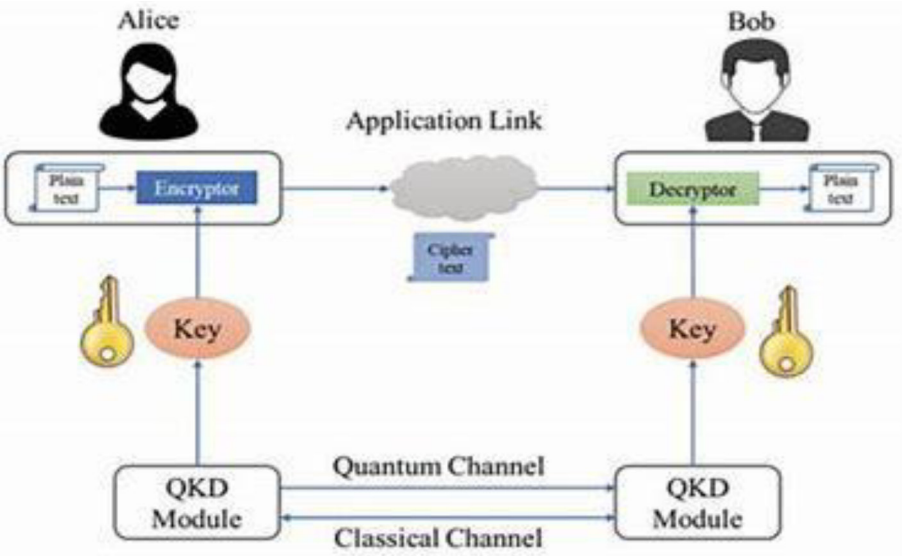

Рис. 1. Квантовий розподіл ключів. Принцип роботи

побудову систем, які автоматично виявляють спроби перехоплення даних.

Квантовий розподіл ключів (Quantum Key Distribution (далі – QKD)) є найвідомішою реалізацією квантової криптографії. QKD дає змогу двом сторонам безпечно обмінюватися криптографічними ключами через квантовий канал (див. рис. 1). Якщо сторонній спостерігач (перехоплювач) намагається втрутитися у процес обміну, це негайно вплине на квантові стани фотонів, що використовуються для передачі ключа. Ці зміни можна виявити і сторони одразу дізнаються про спробу прослуховування (Preskill, 2018; Broadbent, Fitzsimons, Kashefi 2019; Ekert, 1991).

Розглянемо принцип роботи типової схеми QKD (рис. 1). Передача квантових бітів (квантових станів) здійснюється так: один користувач, названий Алісою, надсилає серію фотонів, кожен з яких знаходиться в певному квантовому стані, другому користувачеві, названому Бобом. Ці квантові стани можуть представляти біти (0 або 1) та бути поляризованими за різними базами.

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

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.

Перевірка наявності перехоплення, коли Аліса та Боб вибірково обирають частину своїх збережених бітів і порівнюють їх через класичний канал. Якщо біти співпадають, то це свідчить про відсутність перехоплення. Інакше, перехоплення намагалося втрутитися в обмін. Формування ключа, коли після перевірки безпеки, вони використовують збережені біти як спільний секретний ключ (DiVincenzo, 2020; Новиков, Полторак, 2023).

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 дає змогу виявити перехоплення з високою точністю (Ekert, 1991);

– E91 – протокол розроблений у 1991 році Артуром Еккертом, що використовує квантове заплутування. Два заплутаних фотони розділяються між Алісою та Бобом, і будь-які спроби перехоплення змінюють кореляції між вимірюваннями (DiVincenzo, 2020).

Перевагами QKD слід зазначити:

– безпека на рівні фізичних принципів. На відміну від класичних методів, де безпека залежить від обчислювальної складності, QKD забезпечує безпеку завдяки фундаментальним законам квантової механіки;

– виявлення перехоплення. Квантові системи автоматично визначають спроби перехоплення, що дає змогу уникнути компрометації ключів.

У випадку виявлення перехоплення викликами є (Broadbent, 2019; Ekert, 1991):

– обмежена дальність передачі даних. Квантові канали поки що обмежені у відстані через втрати у волоконно-оптичних лініях.

– технічні складності. Реалізація квантових систем потребує вартісного обладнання та точного контролю квантових станів.

– інфраструктура. Потрібна спеціалізована інфраструктура, яка б підтримувала квантові канали.

Попри технічні складнощі, QKD вже застосовується в комерційних і наукових цілях (DiVincenzo, 2020; Новиков, Полторак, 2023; Бойко, 2023).

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

Отже, квантова криптографія, особливо через QKD, може стати одним із ключових інструментів для забезпечення безпеки в еру квантових обчислень. Вона відкриває нові можливості для захисту інформації, у тому числі для приховування хоча поки що потребує подальшого розвитку та вдосконалення для широкого впровадження. Так, квантові обчислення дозволяють використовувати квантові канали (наприклад, квантові стани фотонів) для передачі прихованої інформації.

Таким чином, можливості квантової криптографії, зокрема квантовий розподіл ключів (QKD), можуть бути інтегровані з методами стеганографії.

Квантовий розподіл ключів дозволяє двом сторонам обмінюватися криптографічними ключами, використовуючи властивості квантової механіки (наприклад, суперпозиція та заплутаність) (Ekert, 1991).

Інтеграція може відбуватися за допомогою створення квантового ключа, коли QKD генерує абсолютно секретний ключ, який можна

використовувати для шифрування або приховування інформації в стеганографічних системах.

Ще інтеграція може відбутися за допомогою захищеного каналу для передачі даних, коли саме квантовий ключ може використовуватися для забезпечення додаткового рівня безпеки в стеганографічних каналах (Broadbent, 2019; Ekert, 1991).

Крім того, інтеграція може відбуватися за рахунок динамічного оновлення ключів, коли квантова криптографія дозволяє регулярно змінювати ключі, що робить їх недоступними для зловмисників навіть за умов довготривалого спостереження.

Відомо, що квантові системи вразливі до шуму та втрат у каналах зв'язку. Тоді для інтеграції необхідна висока якість комунікаційної інфраструктури та наявність спеціалізованого обладнання, коли потрібні пристрої для генерації, передачі та детектування квантових станів, наприклад квантові генератори випадкових чисел або пристрої для вимірювання фотонів.

Розглянемо з якими основними методами стеганографії можлива інтеграція.

Якщо це цифрова стеганографія, інтеграція здійснюється за допомогою методу приховування в цифрових носіях (зображення, відео, аудіо), коли QKD використовується для шифрування повідомлення перед його приховуванням у цифровому носії. Як приклад: прихування квантово-зашифрованого повідомлення в Least Significant Bit (LSB) пікселів зображення (Новиков, Полторак, 2023).

Якщо це мережева стеганографія, інтеграція здійснюється у вигляді приховування даних у мережевому трафіку, коли QKD забезпечує динамічне шифрування мережевих пакетів, що приховуються, наприклад, у часових інтервалах передачі пакетів або їх розмірах. Як приклад: кожен переданий пакет містить квантово-зашифровану частину даних (DiVincenzo, 2020; Новиков, Полторак, 2023).

Якщо це квантова стеганографія, інтеграція здійснюється як приховування даних у квантових станах. Інтеграція QKD безпосередньо з квантовими каналами для приховування даних у параметрах квантових частинок (наприклад, поляризація фотонів або фаза). Особливість такої інтеграції полягає у тому, що дані можуть бути передані таким чином, що будь-яка спроба виявлення призводить до руйнування квантового стану (принцип невизначеності) (Новиков, Полторак, 2023).

Якщо це фізична стеганографія, здійснюється приховування в реальних об'єктах (наприклад, QR-коди, фізичні властивості матеріалів). Причому QKD використовується для безпечного обміну інформацією, яка потім інтегрується в фізичний носій. Прикладом може бути приховування зашифрованого повідомлення в мікроструктурах матеріалів.

У результаті інтеграції QKD зі стеганографією ми отримуємо такі переваги:

– абсолютна безпека, коли завдяки законам квантової механіки зловмисник не може перехопити ключі без впливу на квантові стани; (Бойко, 2023)

– стійкість до квантових атак, коли навіть із появою потужних квантових комп'ютерів QKD забезпечує довгострокову безпеку;

– невидимість передачі, коли комбінація QKD зі стеганографією робить передачу даних практично непомітною.

Зрозуміло, що існують потенційні виклики, це:

– висока вартість інфраструктури, коли впровадження квантових систем вимагає значних ресурсів;

– чутливість до атак на квантові канали, наприклад, атаки за допомогою ослаблених сигналів або підміни фотонів;

– складність інтеграції з класичними методами, коли необхідна розробка стандартів і протоколів для злагодженої роботи класичних та квантових систем.

Окремим питанням є випадок, коли квантовий розподіл ключів (QKD) стикається зі значними викликами у зашумлених середовищах, таких як атмосферні канали або оптоволоконні лінії. Корекція помилок забезпечує збереження ключа навіть за наявності шуму.

Методи корекції в QKD є:

1. Стабілізатори для виявлення помилок: Наприклад, у фазових зміщеннях стабілізатори $Z_1Z_2Z_{-1}$ $Z_{-2}Z_1Z_2$ забезпечують коректність стану.

2. Перевірка сумісності станів, коли система виконує синдромний аналіз для визначення відхилень стану.

3. Фільтрація пошкоджених станів, коли кубіти, які не відповідають очікуваним підписам, видаляються з ключа.

Приклад стабілізації ключів у шумному середовищі, як метод реалізації квантової корекції на практичних платформах, таких як IBM Qiskit, наведений на рис. 2. Квантова корекція помилок відіграє ключову роль у квантових протоколах, таких як телепортація, BB84 і QKD. Використання стабілізаторів і алгебри підписів дозволяє забезпечувати точність і безпеку квантової інформації навіть у зашумлених середовищах. Ці методи становлять основу для подальшого розвитку квантових комунікаційних

```python
from qiskit import QuantumCircuit, Aer, execute

# Створення заплутаного стану
qc = QuantumCircuit(2)
qc.h(0)
qc.cx(0, 1)

# Внесення шуму
qc.z(1)

# Корекція стану
qc.cx(0, 1)
qc.h(0)

# Симуляція
simulator = Aer.get_backend('statevector_simulator')
result = execute(qc, simulator).result()
statevector = result.get_statevector()
print("Corrected Statevector:", statevector)
```

Рис. 2. Стабілізація ключів у шумному середовищі, як метод реалізації квантової корекції на практичної платформі IBM Qiskit

технологій, у тому числі у напряму інтеграції з стеганографією.

Але, інтеграція QKD і стеганографії є багатообіцяючим напрямком, що може знайти застосування в захищених комунікаціях, зокрема в дипломатії, оборонній сфері та приватних зв'язках.

Поняття стійкості до квантових атак. Стійкість до квантових атак – це здатність криптографічних алгоритмів витримувати атаки з використанням квантових комп'ютерів, що мають значно вищу обчислювальну потужність порівняно з звичайними комп'ютерами. Квантові комп'ютери мають потенціал значно скоротити час розв'язання складних математичних задач, на яких базуються сучасні криптографічні методи (Бойко, 2023).

Вагомий вплив на класичні криптографічні системи мають квантові алгоритми, серед яких найвідоміші – алгоритм Шора та алгоритм Гровера.

Алгоритм Шора розроблений для швидкої факторизації великих чисел і розв'язання задачі дискретного логарифмування.

Вплив на класичні алгоритми, такі як RSA. Без квантових обчислень факторизація таких чисел потребує значних ресурсів і часу, що робить RSA надійним. Однак алгоритм Шора виконує факторизацію за поліноміальний час (Preskill, 2018).

Розглянемо умову $2^{O(Logn)} = poly(n)$, яка суттєво знижує складність алгоритму Шора (рис. 3).

Відомо, що задача дискретного логарифмування є основою алгоритмів на еліптичних

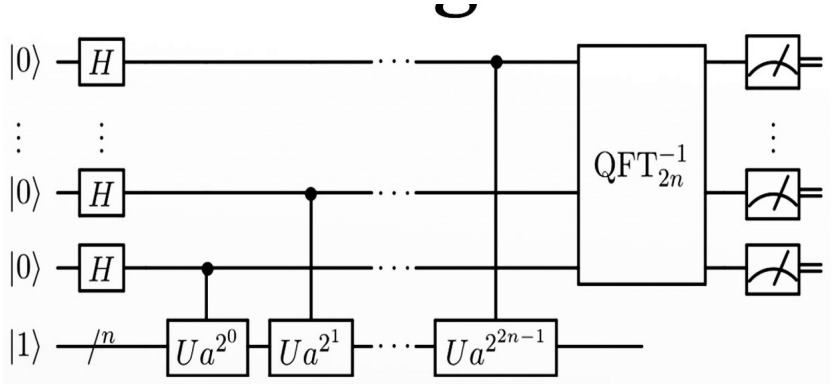

Рис. 3. Структурна схема алгоритму Шора (Gottesman, 2009)

кривих також стає вразливою перед алгоритмом Шора. Але це ставить під загрозу системи, що використовують алгоритми на еліптичні криві для шифрування та підпису (Бойко, Левицький, 2023).

Квантові обчислення впливають на основні методи стеганографії через прискорення аналізу даних, коли квантові алгоритми (наприклад, алгоритм Гровера для пошуку або Шора для факторизації) можуть значно пришвидшити виявлення прихованих даних у великих масивах інформації (Nielsen, Chuang, 2010; Shor, 1995; Steane, 1996; Bennett, Brassard, 1984; Gottesman, 2009; Raussendorf, Harrington, 2007).

Вони впливають також через зміну підходів до приховування – завдяки квантовій криптографії можна розробляти нові протоколи приховування, які будуть інтегровані з квантовими системами.

Квантові обчислення можуть зробити класичну стеганографію менш ефективною через потужні інструменти аналізу, але водночас створюють нові квантові методи, стійкі до класичних атак.

Дослідження цього впливу важливе для майбутнього інформаційної безпеки, адже розвиток квантових обчислень продовжує змінювати обчислювальну парадигму.

Результати дослідження можуть бути використані для розвитку нових підходів до забезпечення інформаційної безпеки та захисту електронної комерції в умовах загроз від квантових обчислень. Це дасть змогу не лише зберегти захищеність даних, але й створити надійні основи для стеганографії в майбутньому.

Висновки й перспективи подальших досліджень. У результаті проведеного дослідження можна зробити кілька важливих висновків щодо впливу квантових обчислень на сучасну стеганографію.

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. Пост-квантова криптографія стає все більш актуальною, оскільки забезпечує безпеку даних у нових умовах, де традиційні алгоритми більше не можуть гарантувати захист. Критерії стійкості до квантових атак містять відсутність відомих квантових атак, збереження стійкості до класичних атак та оптимальну ефективність нових алгоритмів.

По-третє, квантова корекція помилок є ключовим напрямом для успішного розвитку квантових технологій. Алгебра підписів виступає як ефективний інструмент для забезпечення стабільності, безпеки та точності квантових обчислень. Її подальше вивчення та впровадження сприятиме вирішенню викликів, пов'язаних із шумами, масштабуванням і безпекою, відкриваючи нові горизонти для інтеграції квантових досліджень і технологій з стеганографією.

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 мають активізувати зусилля для вивчення та реалізації постквантових криптографічних алгоритмів, щоб забезпечити захист важливих даних у майбутньому.

Інтеграція QKD і стеганографії є багатообіцяючим напрямком, що може знайти застосування в захищених комунікаціях, зокрема в дипломатії, оборонній сфері та приватних зв'язках.

Квантові алгоритми, як-от алгоритм Шора, можуть поставити під загрозу традиційні методи криптографії, які часто використовуються разом зі стеганографією. Це може призвести до необхідності розробки нових методів стеганографії, стійких до квантових атак.

Квантова механіка пропонує високий рівень випадковості, який може бути використаний для підвищення надійності приховування інформації за рахунок переваг квантового випадкового шуму. Це дозволяє створювати більш стійкі до виявлення стеганографічні системи.

Стеганографія в квантових системах стикається з унікальними проблемами, такими як принцип невизначеності, який ускладнює приховування інформації без ризику її викривання.

Напрямками подальших досліджень може бути:

– вивчення інтеграції квантових методів з класичною стеганографією;

– аналіз безпеки стеганографічних методів у постквантовий період;

– розробка квантових протоколів стеганографії;

– оцінка впливу квантового шуму на приховування та виявлення інформації.

Це дослідження може мати значення для підвищення безпеки передачі даних у майбутніх інформаційних системах, в тому числі і в електронній комерції.

ЛІТЕРАТУРА:

1. Nielsen M.A., Chuang I.L. *Quantum Computation and Quantum Information*. Cambridge University Press. 2010. 256 p.
2. Shor P.W. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 1995. 52(4), R2493-R2496. 320 p.
3. Steane A. M. Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 1996. 77(5), P. 793–797.
4. Bennett C. H., Brassard G. Quantum Cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984. 498 p.
5. Gottesman D. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *arXiv preprint quant-ph/0904.2557*. 2009. 420p.
6. Raussendorf R., Harrington J. Fault-tolerant quantum computation with high threshold in two dimensions. *Physical Review Letters*, 2007. 98 (19), 190504, 2007.
7. Preskill J. Quantum Computing in the NISQ era and beyond. *Quantum*, 2018. № 2, P. 79–87.
8. Qiskit Textbook. *IBM Quantum Team*, 2023. URL: https://www.ibm.com/quantum/qiskit
9. Broadbent A., Fitzsimons J., Kashefi E. Universal blind quantum computation. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, 2019. № 3, 400 p.
10. Ekert A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 1991. 67(6), 661–663.
11. DiVincenzo D.P. The Physical Implementation of Quantum Computation. *Fortschritte der Physik*, 2020. 48(9–11), P. 771–783.
12. Новиков Д., Полторак В. Технології пост-квантової криптографії. *Адаптивні автоматичні системи контролю*. 2023. №. 1(42). С.171–183.
13. Бойко Н, Левицький Б. Алгоритми тренування та оцінки моделей машинного навчання для структурованого набору даних. *Information Technology: Computer Science, Software Engineering and Cyber Security*.2023, № 3, С. 3–12.

REFERENCES:

1. Nielsen, M.A., & Chuang, I.L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press. 256 p.
2. Shor, P.W. (1995). Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4), R2493–R2496. 320 p.
3. Steane, A.M. (1996). Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 77(5), P. 793–797.
4. 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*, Bangalore, India, 498 p.
5. Gottesman, D. (2009). An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *arXiv preprint quant-ph/0904.2557*. 420 p.
6. Raussendorf, R., & Harrington, J. (2007). Fault-tolerant quantum computation with high threshold in two dimensions. *Physical Review Letters*, 98 (19), 190504, 2007.
7. Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. *Quantum*, № 2, P. 79–87.
8. Qiskit Textbook. *IBM Quantum Team*, 2023. Retrieved from: https://www.ibm.com/quantum/qiskit
9. Broadbent, A., Fitzsimons, J., & Kashefi, E. (2019). Universal blind quantum computation. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, № 3, 400 p.
10. Ekert, A.K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661–663.
11. DiVincenzo, D.P. (2020). The Physical Implementation of Quantum Computation. *Fortschritte der Physik*, 48(9–11), P. 771–783.
12. Novikov, D., Poltorak, V. (2023). Tekhnolohiyi post-kvantovoyi kryptohrafiyi [Technologies of post-quantum cryptography]. *Adaptive automatic control systems*. №. 1(42). 171–183 [in Ukrainian].
13. Boyko, N, Levyts'kyy, B. (2023). Alhorytmy trenuvannya ta otsinky modeley mashynnoho navchannya dlya strukturovanoho naboru danykh [Algorithms for training and evaluating machine learning models for structured datasets]. *Information Technology: Computer Science, Software Engineering and Cyber Security*. № 3, 3–12 [in Ukrainian].